ELECTRONIC EVIDENCE
HOW TO AVOID GETTING SHOCKED

RICK ROBERTSON

EMILY MISKEL

Koons, Fuller, Vanden Eykel & Robertson, P.C.
5700 W. Plano Pkwy., Suite 2200
Plano, Texas 75093
(972) 769-2727
emily@koonsfuller.com

TABLE OF CONTENTS

I. SCOPE OF ARTICLE.

Increasingly, family lawyers are on the front lines of using modern, electronic evidence. The latest study conducted by the American Academy of Matrimonial Lawyers found that more than 80 percent of divorce attorneys say they have seen an increase in the number of cases using social networking evidence during the past five years. This paper endeavors to provide a practical guide to using and admitting modern evidence. The paper also discusses the laws regarding obtaining and preserving electronic evidence.

II. ELECTRONIC EVIDENCE UNDER EXISTING RULES.

While electronic evidence and online communications feel like a new and unique area in evidence, they are evaluated under the same familiar rules attorneys have always used. State and federal courts have rejected calls to abandon the existing rules of evidence when evaluating electronic evidence. For example, a Pennsylvania court addressed the authentication required to introduce transcripts of instant message conversations:

> 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 [the rules of evidence and 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.[1]

While attorneys are right to be skeptical of electronic evidence, attorneys can forget that the same concerns are present with any type of evidence.

III. AUTHENTICATING ELECTRONIC EVIDENCE.

The requirement of authentication or identification is a condition precedent to admissibility. This requirement is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.[2] Unless the evidence sought to be admitted is self-authenticating under Rule 902, SCRE, extrinsic evidence must be adduced prior to its admission. Rule 901(b) contains a non-exclusive list of illustrations of authentication that comply with the rule. A frequently-cited federal case, *Lorraine v. Markel Am. Insur. Co.*, has become an authority on the application of the rules of evidence to electronically-stored information (ESI).[3] This section quotes extensively from the case, including selections relevant to authenticating ESI:

A. Electronically Stored Information (ESI).

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. 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, the question for the court under Rule 901 is whether the proponent of the evidence has offered a foundation from which the jury could reasonably find that the evidence is what the proponent says it is. The Court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury ultimately might do so.

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. 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. 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.

B. Stored versus Processed Data

In general, electronic documents or records that are merely *stored* in a computer raise no computer-specific authentication issues.[4] If a computer *processes* data rather than merely storing it, authentication issues

[1] *In Re F.P.*, 878 A.2d 91, 95-96 (Pa. Super. Ct. 2005).

[2] Rule 901, SCRE.

[3] *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D.Md. 2007) (memo. op.).

[4] *Lorraine*, 241 F.R.D. at 543 (emph. added).

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 stages 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.

C. Email

There are many ways in which email evidence may be authenticated.[5] 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 email 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. 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.''

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 (Email that qualifies as business record may be 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 email evidence are:

901(b)(1) (witness with knowledge),

901(b)(3) (expert testimony or comparison with authenticated exemplar),

901(b)(4) (distinctive characteristics, including circumstantial evidence), and

902(7) (trade inscriptions).

D. Internet Website Postings.

When determining the admissibility of exhibits containing representations of the contents of website postings of a party, 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.[6] *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?"[7]

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;

[5] *Lorraine*, 241 F.R.D. at 554-55.

[6] *Lorraine*, 241 F.R.D. at 555-56.

[7] 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 21 (9th ed. 2006); *see also* SALTZBURG at § 901.02[12].

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?"[8]

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 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).

South Carolina Case: A court considered evidence of Father's MySpace postings in determining custody.[9]

E. Text Messages and Chat Room Content.

Many of the same foundational issues 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.[10]

One commentator has suggested that the following foundational requirements must be met to authenticate chat room evidence:

(1) evidence that the individual used the screen name in question when participating in chat room conversations (either generally or at the site in question);
(2) evidence that, when a meeting with the person using the screen name was arranged, the individual showed up;
(3) evidence that the person using the screen name identified himself as the person in the chat room conversation;
(4) evidence that the individual had in his possession information given to the person using the screen name; or
(5) evidence from the hard drive of the individual's computer showing use of the same screen name.[11]

Courts also have recognized that exhibits of chat room conversations may be authenticated circumstantially.

For example, in *In re F.P.*,[12] the defendant argued that the testimony of the internet service provider was required, or that of a forensic expert. 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.

Similarly, in *United States v. Simpson*,[13] 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.

Likewise, in *United States v. Tank*,[14] 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. 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.

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 knowledge) and
901(b)(4) (circumstantial evidence of distinctive characteristics).

South Carolina Cases: South Carolina cases that have turned on text message evidence include: *In re Spencer R.*, 387 S.C. 517, 692 S.E.2d 56 (Ct.App. 2010); *Roe v. Reeves*, 392 S.C. 143, 708 S.E.2d 778 (2011); and *Garcia v. Saski*, Opinion No. 2008-MO-044 (Nov. 10, 2008).

South Carolina Cases: The South Carolina Supreme Court upheld the admission of chat room

[8] *Id.* at 22.
[9] *High v. High*, 389 S.C. 226, 697 S.E.2d 690 (Ct.App. 2010).
[10] *Lorraine*, 241 F.R.D. at 556.
[11] SALTZBURG at § 901.02[12].
[12] 878 A.2d at 93–94.
[13] 152 F.3d at 1249.
[14] 200 F.3d at 629–31.

conversations.[15] A recent appellate court case also turned on chat room conversation evidence.[16]

F. 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.[17] 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 of stored digital data to complex computer-generated models performing complicated computations. Each may raise different admissibility issues concerning authentication and other foundational requirements.''

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'' records. 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*,[18] 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. 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.'' *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*,[19] 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. 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.'' 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 files and the time of trial. In other words, the record being proffered must be shown to continue to be an accurate representation of the record that originally was created. Hence, the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created.'' 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.'' 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, viewing electronic records as a form of scientific evidence:

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.

[15] *State v. Gaines*, 380 S.C. 23, 667 S.E.2d 728 (2008).
[16] *State v. Reid*, 383 S.C. 285, 679 S.E.2d 194 (2009).
[17] *Lorraine*, 241 F.R.D. at 556-59.
[18] 263 F.3d at 1180–81.
[19] 336 B.R. 437.

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.[20]

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.'').

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, that courts ''should consider the accuracy and reliability of computerized evidence'' in ruling on 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.

[20] EDWARD J. IMWINKELRIED, EVIDENTIARY FOUNDATIONS at § 4.03[2] (LexisNexis 6th ed. 2005).

The methods of authentication most likely to be appropriate for computerized records are:

901(b)(1) (witness with knowledge),
901(b)(3) (expert testimony),
901(b)(4) (distinctive characteristics), and
901(b)(9) (system or process capable of producing a reliable result).

G. Digital Photographs and Videos.

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.[21] 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 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.

Some examples graphically illustrate the authentication issues associated with digital enhancement of photographs: Suppose 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.

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.

1. Original Digital Photograph.

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

[21] *Lorraine*, 241 F.R.D. at 561-62.

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.

Further, even if no witness can testify from personal knowledge that the photo or video accurately depicts the scene, the "silent witness" analysis allows a photo or video to be authenticated by showing a process or system that produces an accurate result.[22]

2. Digitally Converted Images.

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 latter rule implicating expert testimony under Rule 702. Alternatively, if there is a witness familiar with the scene depicted who can testify to the photo produced from the film when it was digitally converted, no testimony would be needed regarding the process of digital conversion.

3. Digitally Enhanced Images.

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. Recently, one state court has given particular scrutiny to how this should be done.

In *State v. Swinton*,[23] the defendant was convicted of murder in part based on evidence of computer enhanced images prepared using the Adobe Photoshop software. 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 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.

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.[24]

The author recognized that this is an extensive foundation, and whether it will be adopted by courts in the future remains to be seen. However, it is probable that courts will require authentication of digitally-enhanced photographs by adequate testimony that a photograph is the product of a system or process that produces accurate and reliable results under Rule 901(b)(9).

South Carolina Case: The South Carolina Supreme Court held that 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. In that case, the animation was authenticated by the testimony of the expert who prepared the underlying data and the computer technician who used that data to create it.[25]

[22] *See* Rule 901(b)(9), SCRE.
[23] 268 Conn. 781, 847 A.2d 921, 950–52 (2004).
[24] Edward J. Imwinkelried, *Can this Photo be Trusted?*, Trial, October 2005 at 54.
[25] *Clark v. Cantrell*, 339 S.C. 369, 529 S.E.2d 528 (2000).

H. Voicemail.

Rule 901(b)(5) provides that a voice recording may be identified by opinion based upon hearing the voice at anytime under circumstances connecting it with the alleged speaker.

South Carolina Case: A tape of a recorded conversation was sufficiently authenticated under 901(b)(6) by the following testimony: the victim who made the call testified that she knew the other party, that she telephoned him from the sheriff's office and knew the conversation was taped, that she listened to the tape, that she recognized the tape from her initials on it, that the tape fairly and accurately represented the phone conversation, and that the tape had not been edited or altered in any way. The court further held that establishing a chain of custody was not necessary since the tape was otherwise authenticated.[26]

I. Conclusion on Authenticating ESI.

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.[27] 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. 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.

An attorney could also ask authenticating questions about ESI during a deposition. An attorney could have the deponent log into various sites during the deposition and testify to the contents. In theory, this would be no different than having a deponent produce a diary and go through it.

IV. BEST EVIDENCE RULE.

The Best Evidence Rule states that, to prove the content of a writing, recording, or photograph, the *original* writing, recording, or photograph is required except as otherwise provided.[28] The purpose of the best evidence rule is to produce the best obtainable evidence, and if a document cannot as a practical matter be produced because of its loss or destruction, then the production of the original is excused.[29]

Under Rule 1001(3), SCRE, 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. An Indiana court, for example, found that internet chat room communications that a party cut and pasted into a word processing document were still originals.[30] In the predicate for introducing a computer printout, asking whether the exhibit reflects the data accurately may help to overcome an objection under the Best Evidence Rule.

V. HEARSAY ISSUES IN ELECTRONIC EVIDENCE.

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.[31] (See "Non-Assertive Statement," below, for a discussion of whether testimony is even a "statement" at all.) Hearsay is inadmissible unless otherwise permitted by the rules or by statute.[32]

Put more simply, any out-of-court statement, whether by the witness or another person, is hearsay and is inadmissible to support the truth of a claim, unless permitted by another rule. If it can be shown that a statement is non-hearsay or that it falls within a hearsay exception, the statement can be admissible as probative evidence.

The twenty-three hearsay exceptions listed in Rule 803 may be roughly categorized into three categories: unreflective statements, reliable documents, and reputation evidence. The rationale for all of the exceptions is that, over time, experience has shown that these types of statements are generally reliable and trustworthy.

A. Unreflective Statements.

Evidence obtained from email, text messaging, or social networking sites, such as Facebook, MySpace, or Twitter, is often relevant in family law cases. The evidence may be non-hearsay to the extent that it is an admission by a party-opponent, but there may be times where statements by others are relevant. Of the hearsay exceptions, 803(1)-(3) can be especially useful in admitting these types of evidence. Those are the exceptions for present sense impression, excited utterance, and then-existing condition. Electronic communication is particularly prone to candid statements of the declarant's state of mind, feelings,

---

[26] *State v. Aragon*, 354 S.C. 334, 336-37, 579 S.E.2d 626 (Ct.App. 2003).
[27] *Lorraine*, 241 F.R.D. at 562.
[28] Rule 1002, SCRE (emph. added).
[29] Rule 1004(1), SCRE.
[30] *Laughner v. State*, 769 N.E.2d 1147, 1159 (Ind. Ct. App. 2002).
[31] Rule 801(c), SCRE.
[32] Rule 802, SCRE; *see* Rules 801(d), 803, 804.

emotions, and motives.[33] Further, such messages are often sent while events are unfolding. The logic of the existing exceptions can be applied to admit even new forms of communication.

Prior to South Carolina's adoption of the Rules of Evidence, there was a common-law *res gestae* hearsay exception.[34] The previous *res gestae* exception combined both 803(1) and (2), but, under the Rules of Evidence, those exceptions are different.

1. Present Sense Impression.

A statement describing or explaining an event made *while* the declarant was perceiving the event or *immediately* thereafter.[35] Unlike the excited-utterance exception, the rationale for this exception stems from the statement's contemporaneity, not its spontaneity. The present sense impression exception to the hearsay rule is based upon the premise that the contemporaneity of the event and the declaration ensures reliability of the statement.[36] The rationale underlying the present sense impression is that the statement is safe from any error of the defect of memory of the declarant because of its contemporaneous nature; there is little or no time for a calculated misstatement; and the statement will usually be made to another (the witness who reports it) who would have an equal opportunity to observe and therefore check a misstatement. The rule is predicated on the notion that the utterance is a reflex product of immediate sensual impressions, unaided by retrospective mental processes. It is instinctive, rather than deliberate. If the declarant has had time to reflect upon the event and the conditions he observed, this lack of contemporaneity diminishes the reliability of the statements and renders them inadmissible under the rule. Once reflective narratives, calculated statements, deliberate opinions, conclusions, or conscious thinking-it-through statements enter the picture, the present sense impression exception no longer allows their admission. Thinking about it destroys the unreflective nature required of a present sense impression.

2. Excited Utterance.

A statement relating to a startling event or condition made while the declarant was under the stress of excitement caused by event or condition.[37] The excited-utterance exception is broader than the present-sense-impression exception. While a present-sense-impression statement must be made while the declarant was perceiving the event or condition, or immediately thereafter, under the excited-utterance exception, the startling event may trigger a spontaneous statement that relates to a much earlier incident. The elements of the excited-utterance exception are: (1) a startling occasion, (2) a statement relating to the circumstances of the startling occasion, (3) a declarant who appears to have had opportunity to observe personally the events, and (4) a statement made before there has been time to reflect and fabricate.[38] The critical factor in determining when a statement is an excited utterance under Rule 803(2) is whether the declarant was still dominated by the emotions, excitement, fear, or pain of the event. The time elapsed between the occurrence of the event and the utterance is only one factor considered in determining the admissibility of the hearsay statement.

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.[39] The type of statement contemplated by this rule includes a statement that on its face expresses or exemplifies the declarant's state of mind—such as fear, hate, love, and pain. However, a statement is inadmissible if it is a statement of memory or belief offered to prove the fact remembered or believed.[40] One federal court offers the following explanation of Rule 803(3)'s "exception to the exception": Case law makes it clear that a witness may testify to a declarant saying "I am scared," but not "I am scared because the defendant threatened me." The first statement indicates an actual state of mind or condition, while the second statement expresses belief about why the declarant is frightened. The phrase "because the defendant threatened me" is expressly outside the state-of-mind exception because the explanation for the fear expresses a belief different from the state of mind of being afraid.[41]

B. Reliable Documents.

The second category of hearsay exceptions, reliable documents, can also include a variety of computer- or internet-stored data. Anything from online flight schedules, to personal financial records, to emails could potentially be admitted under these existing hearsay exceptions.

---

[33] *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 570 (D.Md. 2007) (memo. op.).

[34] *See State v. Burroughs*, 328 S.C. 489, 492 S.E.2d 408 (1997).

[35] Rule 803(1), SCRE (emph. added).

[36] *Miller v. Keating*, 754 F.2d 507, 511-12 (3d Cir. 1985).

[37] Rule 803(2), SCRE.

[38] *Miller v. Keating*, 754 F.2d 507, 511-12 (3d Cir. 1985).

[39] Rule 803(3), SCRE.

[40] Rule 803(3), SCRE.

[41] *United States v. Ledford*, 443 F.3d 702, 709 (10th Cir. 2005).

1. Recorded Recollection.

A memorandum or record concerning a matter about which a witness once had knowledge but now has insufficient recollection to enable the witness to testify fully and accurately, shown to have been made or adopted by the witness when the matter was fresh in the witness' memory and to reflect that knowledge correctly, unless the circumstances of preparation cast doubt on the document's trustworthiness. If admitted, the memorandum or record may be read into evidence but may not itself be received as an exhibit unless offered by an adverse party.[42] For a statement to be admissible under Rule 803(5), the witness must have had firsthand knowledge of the event, the statement must be an original memorandum made at or near the time of the event while the witness had a clear and accurate memory of it, the witness must lack a present recollection of the event, and the witness must vouch for the accuracy of the written memorandum. To meet the fourth element, the witness may testify that she presently remembers recording the fact correctly or remembers recognizing the writing as accurate when she read it at an earlier time. But if her present memory is less effective, it is sufficient if the witness testifies that she knows the memorandum is correct because of a habit or practice to record matters accurately or to check them for accuracy.

2. 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 activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness; provided, however, that subjective opinions and judgments found in business records are not admissible. The term "business" as used in this subsection includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.[43]

For example, if a spouse keeps financial records as part of a regularly organized activity, the records can be admitted under this exception with the spouse as the sponsoring witness, without a business records affidavit. Courts have admitted check registers in this way.[44] The predicate for admissibility under the business records exception is established if the party offering the evidence establishes that the records were generated pursuant to a course of regularly conducted business activity and that the records were created by or from information transmitted by a person with knowledge, at or near the time of the event.

3. 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.[45] Where it is proven that publications of market prices or statistical compilations are generally recognized as reliable and regularly used in a trade or specialized activity by persons so engaged, such publications are admissible for the truth of the matter published. A variety of potentially-relevant commercial data published online can be admissible under this exception.

C. Statements That Are Not Hearsay.

Evidence constitutes hearsay only if it is (1) an assertive statement (2) by an out-of-court declarant (3) offered to prove the truth of the assertion.[46]

1. Computer Generated "Statements."

"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.'"[47]

While there may be authentication issues relating to computer-generated text or computer-processed data, several federal cases have held that such information is not hearsay:

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'");

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

[42] Rule 803(5), SCRE.
[43] Rule 803(6), SCRE.
[44] *See Sabatino v. Curtiss Nat'l Bank*, 415 F.2d 632, 634 (5th Cir. 1969).
[45] Rule 803(17), SCRE.
[46] Edward J. Imwinkelreid, *Evidentiary Foundations*, 7th ed., §10.01, p. 407 (2008).
[47] *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 564-65 (D.Md. 2007) (memo. op.).

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 records 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.").

2. Metadata

Metadata is the computer-generated data about a file, including date, time, past saves, edit information, etc. It would likely be considered a non-statement under the above logic, and therefore non-hearsay. It remains important to properly satisfy authentication requirements. A higher authentication standard may apply, since it is computer-processed data, rather than merely computer-stored data.

However, since metadata is normally hidden and usually not intended to be reviewed, several states have issued ethics opinions concluding that it is unethical to mine inadvertently-produced metadata.[48] A few ethics opinions have held that mining metadata is not unethical.[49] The American Bar Association has published a state-by-state chart comparing positions on metadata.[50] South Carolina does not yet have an ethics opinion directly on point.

3. Admissions by a Party-Opponent.

The statement is offered against a party and is (A) the party's own statement in either an individual or a representative capacity, or (B) a statement of which the party has manifested an adoption or belief in its truth, or (C) a statement by a person authorized by the party to make a statement concerning the subject, or (D) a statement by the party's agent or servant concerning a matter within the scope of the agency or employment, made during the existence of the relationship, or (E) a statement by a coconspirator of a party during the course and in furtherance of the conspiracy.[51]

The Rules of Evidence allow liberal introduction of a party's admissions and define them as non-hearsay, because of the incongruity of the party objecting to his own statement on the ground that he was not subject to cross-examination by himself at the time. For this reason, the Rules of Evidence omit any provision allowing introduction of admissions made by predecessors in interest or those in privity to a party, as considerations of privity and joint interest neither furnish criteria of credibility nor aid in the evaluation of testimony.[52]

The exemption for admissions by a party-opponent is extremely useful in overcoming a hearsay objection to texts, emails, Facebook wall posts, etc.

VI. WITNESSES.

Online evidence can also be useful in managing a witness.

A. Writing Used to Refresh Memory.

Social networking or other electronic communications can be a useful record of events or a witness's thoughts. If a witness's memory fails, a writing, including an electronic communication, may be used to refresh the witness's memory.

---

[48] NY. Comm. On Prof'l Ethics, Op. 749 (1002); Prof'l Ethics of the Fla. Bar, Op. 06-2 (2006); Ala. State Bar office of the Gen. Counsel, Op. No. 2007-02 (2007); D.C. Bar, Op. 341.

[49] Md. State Bar Ass'n, Comm. on Ethics, Op. 2007-092 (2006); ABA Formal Op. 06-442.

[50] *Available at*: http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html

[51] Rule 801(d)(2), SCRE.

[52] *See Eldridge v. Greenwood*, 331 S.C. 398, 432 n.17, 503 S.E.2d 191 (1998).

There is often confusion about the difference between a recorded recollection under the hearsay exception of Rule 803(5) and a writing used to refresh memory under Rule 613. The *Welch*[53] case offers a helpful explanation of the differences: A witness testifies from present recollection what he remembers presently about the facts in the case. When that present recollection fails, the witness may refresh his memory by reviewing a memorandum made when his memory was fresh. After reviewing the memorandum, the witness must testify either his memory is refreshed or his memory is not refreshed. If his memory is refreshed, the witness continues to testify and the memorandum is not received as evidence. However, if the witness states that his memory is not refreshed, but has identified the memorandum and guarantees the correctness, then the memorandum is admitted as past recollection recorded. Where the memorandum, statement or writing is used to refresh the present recollection of the witness and it does, then the memorandum does not become part of the evidence, for it is not the paper that is evidence, but the recollection of the witness.

An adverse party is entitled to have the writing produced at the hearing, to inspect it, to cross-examine the witness thereon, and to introduce in evidence those portions which relate to the testimony of the witness.[54] Use of an otherwise privileged writing to refresh a party's memory will constitute a waiver of that privilege.

B. Impeachment.

Electronic communications can be some of the most useful tools for impeachment. Impeachment evidence is generally hearsay and does not have probative value. Prior inconsistent statements offered to impeach the witness's credibility do not constitute hearsay because they are not offered for the truth of the matter asserted. If the impeachment evidence meets a hearsay exception or exemption, however, it may be admitted as probative evidence.

The *Michael*[55] case gives an excellent summary of the means of impeachment: There are five major forms of impeachment: two are specific, and three are nonspecific. Specific impeachment is an attack on the accuracy of the specific testimony (i.e., the witness may normally be a truthteller, but she is wrong about X), while non-specific impeachment is an attack on the witness generally (the witness is a liar, therefore she is wrong about X). The two specific forms of impeachment are impeachment by prior inconsistent statements and impeachment by another witness. The three non-specific forms of impeachment are impeachment through bias or motive or interest, impeachment by highlighting testimonial defects, and impeachment by general credibility or lack of truthfulness. Electronic evidence can be useful for providing specific impeachment (previous statements by the witness) as well as non-specific impeachment (photos of the witness in situations that reflect poorly on the witness's credibility).

1. Prior Inconsistent Statement.

Extrinsic evidence of a prior inconsistent statement by a witness is not admissible unless the witness is advised of the substance of the statement, the time and place it was allegedly made, and the person to whom it was made, and is given the opportunity to explain or deny the statement. If a witness does not admit that he has made the prior inconsistent statement, extrinsic evidence of such statement is admissible. However, if a witness admits making the prior statement, extrinsic evidence that the prior statement was made is inadmissible. This provision does not apply to admissions of a party-opponent as defined in Rule 801(d)(2).[56]

If a proper predicate is not laid, the inconsistent statement may be excluded and further cross-examination on the subject blocked. However, if the witness is the opposing party, no confrontation is required, and no opportunity to explain need be given.

2. Impeaching Hearsay Statements

The credibility of hearsay statements can be impeached just as if the statements were uttered by a witness. If an opponent successfully uses online communications from a third party, an attorney can put on evidence to impeach the credibility of the out-of-court declarant. Rule 806, SCRE, provides that when a hearsay statement, or a non-hearsay statement defined by Rule 801(d), has been admitted in evidence, the credibility of the out-of-court declarant may be attacked. Evidence of a statement or conduct by the declarant at any time may be offered to impeach the out-of-court declarant. There is no requirement that the declarant be afforded an opportunity to deny or explain. If the credibility of the out-of-court declarant is attacked, it may be supported by any evidence which would be admissible if the declarant had testified as a witness. If the party against whom a hearsay statement has been admitted then calls the declarant as a witness, the party is entitled to examine the declarant on the statement as if under cross-examination.

[53] *Welch v. State*, 576 S.W.2d 638, 641 (Tex.Crim.App. 1979).
[54] Rule 612, SCRE.
[55] *Michael v. State*, 235 S.W.3d 723, 726 (Tex.Crim.App. 2007).
[56] Rule 613(b), SCRE.

C. Character Evidence.

Social networking evidence can be especially useful for providing character evidence or evidence of a party's prior conduct.

Evidence about prior instances of conduct used to show that a person acted in conformity on a particular occasion is generally inadmissible. However, under 404(b), such evidence may be admissible for other purposes, such as showing proof of motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake or accident. Further, evidence of the habit of a person or of the routine practice of an organization, whether corroborated or not and regardless of the presence of eyewitnesses, is relevant to prove that the conduct of the person or organization on a particular occasion was in conformity with the habit or routine practice.[57]

Although evidence of specific acts is limited, character evidence can be admissible.[58] If reputation or opinion testimony is admitted, evidence of specific instances of conduct is permitted on cross-examination.

VII. UNFAIR PREJUDICE.

If an attorney trying to keep a piece of evidence out has failed to block the evidence based on relevance, authenticity, hearsay, or the original writing rule, the final step is the requirement to balance evidence's probative value against the potential for unfair prejudice, or other harm, under Rule 403. 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, or needless presentation of cumulative evidence.

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:

Offensive language. When the evidence would contain offensive or highly derogatory language that may provoke an emotional response.

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.").

Computer Animations. 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 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).

Summaries. When considering the admissibility of summaries of voluminous electronic writings, recordings or photographs under Rule 1006.

Weinstein[59] ("Summary evidence is subject to the balancing test under Rule 403 that weighs the probative value of evidence against its prejudicial effect.").

Reliability and Accuracy. 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).

VIII. EXPERT TESTIMONY AND OPINIONS.

A. Basis of Expert Testimony and Opinions.

Increasingly, parties are bringing electronic evidence directly to experts, including Facebook posts, Twitter "tweets," online photo albums, and other relevant social networking posts. For example, social study evaluators are being handed printouts of a spouse's online activity. To determine how this

[57] Rule 406, SCRE.

[58] Rules 404-405, SCRE.

[59] JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 1006.08[3] (Joseph M. McLaughlin ed., Matthew Bender 2d ed. 1997).

evidence affects an expert's work, attorneys should look back at the rules regarding expert testimony.

B. Factors Relied Upon.

The general rule is that, once properly qualified, an expert can base his or her opinion on just about anything remotely relevant to the issue he or she is called to testify about—including evidence of online activity. Rule 703, SCRE, permits an expert to rely on the following to base his opinion:

Personal Knowledge. This would include such observations as statements made by the parties, testing results, etc.

Facts/Data Made Known to the Expert at or Before the Hearing. Many mental health professional rely and may rely on other evidence presented by others, deposition testimony and reports of other experts.

Inadmissible Evidence, if Relied on by Others. The reliance on tests, trade journals, other medical reports, etc. has not created much controversy in regard to expert opinions. However, a problem may arise when the expert begins to recount a hearsay conversation he has had with another. Rule 703 implies that this type of testimony is permissible, but the case law indicates that there are limits.[60] Rule 703 permits an expert giving an opinion to rely on facts or data that are not admitted in evidence or even admissible into evidence. The rule, however, does not allow for the unqualified admission of hearsay evidence merely because an expert has used it in forming an opinion. The expert may testify to evidence even though it is inadmissible under the hearsay rule, but allowing the evidence to be received for this purpose does not mean it is admitted for its truth. It is received only for the limited purpose of informing the jury of the basis of the expert's opinion and therefore does not constitute a true hearsay exception.

IX. DISCOVERY OF ELECTRONIC EVIDENCE

South Carolina amended its rules of civil procedure this year to explicitly address ESI. The amendments to Rules 16, 26, 33, 34, 37 and 45 of the South Carolina Rules of Civil Procedure concerning electronic discovery are substantially similar to the corresponding provisions in the Federal Rules of Civil Procedure.[61] Federal Rule of Civil Procedure 34, for example, governs the production of documents and electronically stored information. The Committee Notes on the 2006 amendment to FRCP 34 detail some of the issues courts have had to face in applying traditional discovery rules to include electronic evidence:

"As originally adopted, Rule 34 focused on discovery of 'documents' and 'things.' In 1970, Rule 34(a) was amended to include discovery of data compilations, anticipating that the use of computerized information would increase. Since then, the growth in electronically stored information and in the variety of systems for creating and storing such information has been dramatic. Lawyers and judges interpreted the term 'documents' to include electronically stored information because it was obviously improper to allow a party to evade discovery obligations on the basis that the label had not kept pace with changes in information technology. But it has become increasingly difficult to say that all forms of electronically stored information, many dynamic in nature, fit within the traditional concept of a 'document.' Electronically stored information may exist in dynamic databases and other forms far different from fixed expression on paper. Rule 34(a) is amended to confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents. The change clarifies that Rule 34 applies to information that is fixed in a tangible form and to information that is stored in a medium from which it can be retrieved and examined. At the same time, a Rule 34 request for production of 'documents' should be understood to encompass, and the response should include, electronically stored information unless discovery in the action has clearly distinguished between electronically stored information and 'documents.'

Discoverable information often exists in both paper and electronic form, and the same or similar information might exist in both. The items listed in Rule 34(a) show different ways in which information may be recorded or stored. Images, for example, might be hard-copy documents or electronically stored information. The wide variety of computer systems currently in use, and the rapidity of technological change, counsel against a limiting or precise definition of electronically stored information. Rule 34(a)(1) is expansive and includes any type of information that is stored electronically. A common example often sought in discovery is electronic communications, such as e-mail. The rule covers—either as documents or as electronically stored information—information 'stored in any medium,' to encompass future developments in computer technology. Rule 34(a)(1) is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments.

References elsewhere in the rules to 'electronically stored information' should be understood to invoke this expansive approach. A companion change is made to Rule 33(d), making it explicit that parties choosing to respond to an interrogatory by permitting access to responsive

[60] *Jones v. Doe*, 372 S.C. 53, 63, 640 S.E.2d 514 (Ct.App. 2006).

[61] *See* S.C. R. Civ. P. Note to 2011 Amendment.

records may do so by providing access to electronically stored information. More generally, the term used in Rule 34(a)(1) appears in a number of other amendments, such as those to Rules 26(a)(1), 26(b)(2), 26(b)(5)(B), 26(f), 34(b), 37(f), and 45. In each of these rules, electronically stored information has the same broad meaning it has under Rule 34(a)(1). References to 'documents' appear in discovery rules that are not amended, including Rules 30(f), 36(a), and 37(c)(2). These references should be interpreted to include electronically stored information as circumstances warrant.

The term 'electronically stored information' is broad, but whether material that falls within this term should be produced, and in what form, are separate questions that must be addressed under Rules 26(b), 26(c), and 34(b)….

Rule 34(a)(1) is also amended to make clear that parties may request an opportunity to test or sample materials sought under the rule in addition to inspecting and copying them. That opportunity may be important for both electronically stored information and hard-copy materials. The current rule is not clear that such testing or sampling is authorized; the amendment expressly permits it. As with any other form of discovery, issues of burden and intrusiveness raised by requests to test or sample can be addressed under Rules 26(b)(2) and 26(c). Inspection or testing of certain types of electronically stored information or of a responding party's electronic information system may raise issues of confidentiality or privacy. The addition of testing and sampling to Rule 34(a) with regard to documents and electronically stored information is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems….

Subdivision (b). Rule 34(b) provides that a party must produce documents as they are kept in the usual course of business or must organize and label them to correspond with the categories in the discovery request. The production of electronically stored information should be subject to comparable requirements to protect against deliberate or inadvertent production in ways that raise unnecessary obstacles for the requesting party. Rule 34(b) is amended to ensure similar protection for electronically stored information.

The amendment to Rule 34(b) permits the requesting party to designate the form or forms in which it wants electronically stored information produced. The form of production is more important to the exchange of electronically stored information than of hard-copy materials, although a party might specify hard copy as the requested form. Specification of the desired form or forms may facilitate the orderly, efficient, and cost-effective discovery of electronically stored information. The rule recognizes that different forms of production may be appropriate for different types of electronically stored information. Using current technology, for example, a party might be called upon to produce word processing documents, e-mail messages, electronic spreadsheets, different image or sound files, and material from databases. Requiring that such diverse types of electronically stored information all be produced in the same form could prove impossible, and even if possible could increase the cost and burdens of producing and using the information. The rule therefore provides that the requesting party may ask for different forms of production for different types of electronically stored information.

The rule does not require that the requesting party choose a form or forms of production. The requesting party may not have a preference. In some cases, the requesting party may not know what form the producing party uses to maintain its electronically stored information, although Rule 26(f)(3) is amended to call for discussion of the form of production in the parties' prediscovery conference.

The responding party also is involved in determining the form of production. In the written response to the production request that Rule 34 requires, the responding party must state the form it intends to use for producing electronically stored information if the requesting party does not specify a form or if the responding party objects to a form that the requesting party specifies. Stating the intended form before the production occurs may permit the parties to identify and seek to resolve disputes before the expense and work of the production occurs. A party that responds to a discovery request by simply producing electronically stored information in a form of its choice, without identifying that form in advance of the production in the response required by Rule 34(b), runs a risk that the requesting party can show that the produced form is not reasonably usable and that it is entitled to production of some or all of the information in an additional form. Additional time might be required to permit a responding party to assess the appropriate form or forms of production.

If the requesting party is not satisfied with the form stated by the responding party, or if the responding party has objected to the form specified by the requesting party, the parties must meet and confer under Rule 37(a)(2)(B) in an effort to resolve the matter before the requesting party can file a motion to compel. If they cannot agree and the court resolves the dispute, the court is not limited to the forms initially chosen by the requesting party, stated by the

responding party, or specified in this rule for situations in which there is no court order or party agreement.

If the form of production is not specified by party agreement or court order, the responding party must produce electronically stored information either in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable. Rule 34(a) requires that, if necessary, a responding party "translate" information it produces into a "reasonably usable" form. Under some circumstances, the responding party may need to provide some reasonable amount of technical support, information on application software, or other reasonable assistance to enable the requesting party to use the information. The rule does not require a party to produce electronically stored information in the form it [sic] which it is ordinarily maintained, as long as it is produced in a reasonably usable form. But the option to produce in a reasonably usable form does not mean that a responding party is free to convert electronically stored information from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information efficiently in the litigation. If the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature.

Some electronically stored information may be ordinarily maintained in a form that is not reasonably usable by any party. One example is "legacy" data that can be used only by superseded systems. The questions whether a producing party should be required to convert such information to a more usable form, or should be required to produce it at all, should be addressed under Rule 26(b)(2)(B).

Whether or not the requesting party specified the form of production, Rule 34(b) provides that the same electronically stored information ordinarily be produced in only one form."[62]

The National Center for State Courts Conference of Chief Justices approved GUIDELINES FOR STATE TRIAL COURTS REGARDING DISCOVERY OF ELECTRONICALLY STORED INFORMATION in 2006.[63] The document is intended to help reduce the uncertainty in state court litigation by assisting trial judges in identifying the issues and determining the decision-making factors to be applied. If you have a case that you know will be particularly focused on electronic evidence, it may be useful to circulate the guide at pretrial discovery hearings to provide guidance on some of the more complex electronic discovery issues.

X. ILLEGALLY OBTAINING ELECTRONIC EVIDENCE

Many clients have questions about whether they can record phone calls, hide a camera to catch a cheating spouse in the act, or access a spouse's emails. Attorneys wonder whether such evidence may be used at trial.

Electronic evidence can be a trap for both client and attorney, exposing them to extensive civil and even criminal liability. A confusing mix of state and federal laws on wiretapping and computer security can have significant effects on divorcing spouses. Further, a spouse can be subject to private suits and common-law tort liability. This article will address the most common types of surreptitious electronic evidence and the pitfalls associated with each.

A. Wiretap Laws

The federal Wiretap Act, 18 U.S.C. §§ 2510-2522, regulates electronic surveillance of oral communications, whether those conversations are in person, by telephone, or by cell phone. Under the federal act, civil remedies include liquidated damages of $10,000, punitive damages, and attorney's fees. Criminal penalties can include imprisonment of up to five years.

The federal wiretapping laws are "one-party consent" laws, meaning you may record any conversation you are a part of without the consent of the other party. However, planting a bug to record conversations between others would be a violation, as would installing an application on someone else's cell phone to record his or her calls with others. Courts have found a limited "vicarious consent" exception allowing a parent to record his or her child's conversations with others if there is a good faith, reasonable basis that it is necessary for the welfare of the child.

While South Carolina does not have an explicit statute on point, caselaw holds that only one party's consent is required, similar to federal law.[64]

B. Electronic Data Laws

The federal Stored Communications Act, 18 U.S.C. §§ 2701-2712, regulates access to electronic communications including e-mail, faxes, and

[62] FED. R. CIV. P. 34, Committee Notes on Rules—2006 Amendment.

[63] *Available at:* http://www.ncsconline.org/images/EDiscCCJGuidelinesFinal.pdf

[64] *See Mays v. Mays*, 229 S.E.2d 725, 726-27 (S.C. 1976) (finding that 18 U.S.C. §2511(2)(d) "makes it clear that one party to a telephone conversation may lawfully tape the conversation without the other's knowledge or permission and subsequently disclose [the conversation]."); *Thompson v. State*, 479 S.E.2d 808, 810-11 (S.C. Ct. App. 1996) (finding that taped telephone conversations between defendant and confidential informant did not violate 18 U.S.C. §2511 and the defendants right to privacy).

voicemail. Despite the use of the term "stored," the Act regulates the access of communications during electronic transmission. Interestingly, this means that accessing emails saved to the hard drive of a shared computer is permitted, but accessing emails through a spouse's webmail account without consent is a violation. Penalties include fines and imprisonment for up to five years.

Using evidence obtained from Facebook, MySpace, blogs, and other online sites is a growing trend in family law. It is a violation to log in to a spouse's online account without consent, however, the stored communications laws do not contain the same strict exclusionary rule as the wiretap laws. This means that even illegally-intercepted internet communications may be used at trial.

South Carolina Case: A South Carolina Court recently applied the Stored Communications Act in a divorce case.[65]

C. Torts

Many invasion-of-privacy torts can apply to wiretapping or illegally obtaining electronic evidence. Victims of wiretapping, videotaping, and intercepted emails can sue for (a) intrusion upon seclusion, (b) public disclosure of private facts, (c) appropriation of name or likeness for defendant's advantage, and even (d) intentional infliction of emotional distress, depending on the facts. Liability does not always depend on whether the private matters were ever publicized. Hiding a camera in a master bedroom can give rise to an invasion of privacy claim.

In tort, a plaintiff can recover actual and punitive damages. A divorcing spouse would not have to file a separate lawsuit, because a court can consider tort claims in making a disproportionate division of a marital estate.

D. Consequences for Attorneys

An attorney's *use* or *disclosure* of intercepted communications violates the wiretap laws, even if the attorney did not direct a client to make the recording. This means that attorneys can face criminal and civil penalties for using evidence that a client obtained in violation of the wiretap laws. If an attorney has reason to believe that recordings were illegally obtained, the attorney should immediately cease reviewing the recordings and should not use or disclose the communications in any way.

Although it is very tempting for clients to try to obtain smoking-gun evidence, attorneys must be aware of the serious consequences that can flow from violating electronic evidence laws.

[65] *Jennings v. Jennings*, 389 S.C. 190, 697 S.E.2d 671 (Ct.App. 2010).

XI. SPOLIATION OF ELECTRONIC EVIDENCE

Over the past few years, case and statutory law have begun to outline the duties and obligations of parties to litigation with respect to electronic discovery and evidence. Though fiduciary litigation, outside of closely held corporations, will largely be confined in discovery requests to the business data and hardware, do not automatically exclude the possibility of extraneous sources of electronic data, such as texts, facebook pages, blogs, or websites. The ever-developing case and statutory law provides important guidelines for any litigator to keep in mind when dealing with electronic evidence and discovery.

A. Zubulake

In a series of opinions culminating in what is commonly referred to as *Zubulake V*, Judge Schendlin of the Southern District of New York announced what have now become significant protocols for counsel's responsibilities surrounding electronic discovery and evidence.[66] One of the primary obligations the *Zubulake* opinions address is the duty to preserve electronic evidence when a party reasonably anticipates litigation.[67] *Zubulake V* provides three steps counsel should take to ensure compliance with a party's preservation obligation:

> 1) Counsel must issue a "litigation hold" at the beginning of litigation or whenever litigation is reasonably anticipated. The hold should be re-issued periodically so that new employees are aware of it and all employees are reminded of their duties.
>
> 2) Counsel should communicate directly with "key players" in the litigation (*i.e.* people identified in a party's initial disclosure and any supplemented disclosure).
>
> 3) Counsel should instruct all employees to produce electronic copies of their relevant active files and make sure that all backup media which the party has a duty retain is identified and stores in a safe place.[68]

A litigation hold notice should describe the matter at issue, provide specific examples of the types of information at issue, identify potential sources of

[66] *Zubulake v. UBS Warburg, LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004); Losey, 53.

[67] *See Zubulake V*, 228 F.R.D. 422; *The Sedona Conference Commentary on Legal Holds: The Trigger and The Process*, 1, (Conor R. Crowley et al. eds, The Sedona Conference 2007).

[68] *See Zubulake V*, 229 F.R.D 422; *The Sedona Conference Commentary on Legal Holds*, 12.

information, and inform recipients of their legal obligations.[69] Case law is clear that a party does not have to preserve information that is not relevant.[70]

B. Sedona Guidelines

The Sedona Conference, a working group composed of lawyers, consultants, academics, and jurists, has also published a series of articles on the management of and best practices regarding electronic evidence. Primarily aimed at organizations, the Sedona Conference published the following guidelines for managing electronic information and records:

- An organization should have reasonable policies and procedures for managing its information and records.
- An organization's information and records management policies and procedures should be realistic, practical and tailored to the circumstances of the organization.
- An organization need not retain all electronic information ever generated or received.
- An organization adopting an information and records management policy should also develop procedures that address the creation, identification, retention, retrieval and ultimate disposition or destruction of information and records.
- An organization's policies and procedures must mandate the suspension of ordinary destruction practices and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, government investigation or audit.[71]

The Sedona Conference has also devised the following guidelines to determine when litigation is reasonably anticipated and when a duty to take affirmative steps to preserve relevant information has arisen:

- Reasonable anticipation of litigation arises when an organization is on notice of a credible threat it will become involved in litigation or anticipates taking action to initiate litigation.
- The adoption and consistent compliance with a policy defining a preservation decision-making process is one factor that demonstrates reasonableness and good faith in meeting preservation obligations.
- The adoption of a process for the reporting a threat of litigation to a responsible decision maker is a factor that demonstrates reasonableness and good faith.
- The determination of whether litigation is reasonably anticipated should be based on good faith and reasonable evaluation of relevant facts and circumstances.
- Judicial evaluation of an organization's legal hold decision should be based on the good faith and reasonableness of the decision (including whether a legal hold is necessary and how the legal hold should be executed) at the time it was made.[72]

C. Federal Rules of Civil Procedure

The Federal Rules of Civil Procedures were amended on December 1, 2006 to address the discovery of electronically stored information. Among the changes:

- Amended Rule 26(b)(2)(B) states that a party does not need to provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.
- Amended Rule 34 includes "electronically stored information" as a category for which any party may request any other party in an interrogatory to produce and inspect, copy, test or sample.
- Amended Rule 37(f) provides that, absent exceptional circumstances, a court may not impose sanctions on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.

D. Other Rules involving Electronic Information

In August of 2007 the Uniform Law Commissioners adopted the Uniform Rules Relating to Discovery of Electronically Stored Information for use

[69] *The Sedona Conference Commentary of Legal Holds*, 12.

[70] *See Zubulake v. UBS Warburg (Zubulake IV)*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003)(stating, "Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every e-mail or electronic documents, and every backup tape? The answer is clearly, 'no.' Such a rule would cripple large corporations.")

[71] *The Sedona Guidelines: Best Practice Guidelines and Commentary for Managing Information and Records in the Electronic Age, iv-v* (Charles R. Ragan et al. eds, The Sedona Conference 2005).

[72] *The Sedona Conference Commentary on Legal Holds*, 3.

by state courts. A copy of these model rules can be found in the Appendix to this paper.

E. Recent Case law on Spoliation and Sanctions

Courts have indicated that there may be serious consequences for parties and their counsel for failing to preserve electronic evidence and to comply with the duties set forth in *Zubulake.* Possible sanctions include fines, attorney's fees and costs, as well as adverse-inference jury instructions. Additionally, in one new, important case regarding sanctions for willful spoliation, the judge threatened jail time for the actions of one party. Here are some recent examples:

In *Victor Stanley v. Creative Pipe*, 2010 WL 3530097 (D. MD. Sept. 9, 2010), already known as Victor Stanley II, the aptly named Judge Grimm of Maryland threatened jail time if the party who willfully destroyed evidence did not pay for the opposing party's fees and costs. While extreme in conduct and punishment, the most lasting takeaway from Victor Stanley II is Judge Grimm's 12 page circuit break down of spoliation criteria, caselaw, and sanctions, attached as Appendix A. Judge Grimm's sanctions and national survey of the caselaw were not done to further ESI sanctions, but rather to grasp the state of the law in order to stabilize it. As the judge stated in his opinion:

> "the Court could be excused for simply acknowledging Defendants' concessions and applying the applicable law of the Fourth Circuit without considering the broader legal context in which preservation/spoliation issues are playing out in litigation across the country. While justified, such a narrow analysis would be of little use to lawyers and their clients who are forced, on a daily basis, to make important decisions in their cases regarding preservation/spoliation issues, and for whom a more expansive examination of the broader issue might be of some assistance. Accordingly, I will attempt to synthesize not only the law of this District and Circuit, but also to put it within the context of the state of the law in other circuits as well. I hope that this analysis will provide counsel with an analytical framework that may enable them to resolve preservation/ spoliation issues with a greater level of comfort that their actions will not expose them to disproportionate costs or unpredictable outcomes of spoliation motions."

In *Phoenix Four, Inc. V. Strategic Resources Corp*., a law firm and it clients were sanctioned $45,162 for the attorneys' failure to personally investigate and understand that two of its client's computer serves had hidden partitions containing discoverable electronic information.[73]

The Southern District Court of New York in *Qualcomm Inc. v. Broadcom Corp*. found Qualcomm in violation of its discovery obligation for failing to produce over 200,000 pages of relevant e-mails, memoranda, and other company documents until four months after trial.[74] The court issued a show cause order which stated:

> "this Court is inclined to consider the imposition of any and all appropriate sanctions on Qualcomm's attorneys, including but not limited to, monetary sanctions, continuing legal education, referral to the California State Bar for appropriate investigation and possible sanctions, and counsel's formal disclosure of this Court's findings to all current clients and any courts in which counsel is admitted or has litigation currently pending."[75]

In *Teague v. Target Corp*., the Western District Court of North Carolina found that plaintiff had a duty to preserve evidence, even though the suit had not been filed, because she had retained counsel and filed EEOC charges.[76] Thus, plaintiff failed to comply with her duty to preserve relevant information when she threw away her computer, which contained information relevant to the lawsuit.[77] As sanctions, the court issued an adverse inference jury instruction.[78]

XII. CONCLUSION

Although using modern evidence can feel like a new puzzle, attorneys are still working with the same familiar rules of evidence. Do not be intimidated just because evidence is electronic in nature. An attorney who is well-prepared to argue how the rules of evidence apply to electronic evidence can successfully use even the newest technologies.

---

[73] No. 05-CIV-4837, 2006 WL 1409413 (S.D.N.Y. May 22, 2006); Losey 58.

[74] No. 05-CV-1958-B(BLM) Doc. 593 (S.D. Cal. Aug. 6, 2007); Losey 114.

[75] *Qualcomm*,No. 05-CIV-4837, 2006 WL 1409413 (S.D.N.Y. May 22, 2006); Losey 116.

[76] 2007 WL 1041191 (W.D. N.C. April 4, 2007); Losey 150.

[77] 2007 WL 1041191 (W.D. N.C. April 4, 2007); Losey 150.

[78] 2007 WL 1041191 (W.D. N.C. April 4, 2007); Losey 151.