Making Your Online Evidence Usable in the Courtroom

By

Michael Kaiser, JD.
Kaiser Legal Group
Michael-Kaiser@Kaiser-LegalGroup.com

When you use evidence obtained online, it is not necessary for you to reinvent the wheel anymore than if you were utilizing more "traditional" types of evidence. However, there are issues you will have to finesse.

"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. . . . 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 . . .. Instead of relying on the voodoo information taken from the Internet, Plaintiff must hunt for hard copy back-up documentation in admissible form. . . ." *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, 76 F.Supp.2d 773, 774-75 (S.D. Tex. 1999).

Throughout time, new technology, whether pictures or recordings or anything unfamiliar, has been met with skepticism by the courts. The bar is set higher by society for anything new, and our courtrooms are simply reflections of such, albeit with the law typically evincing even more conservative leanings.

Technology is changing so rapidly that even today's accepted technological truths are often tomorrow's falsehoods. A practitioner is left with

several choices. One is to play it safe and either rely on technological-based evidence as seldom as possible or rely only on using very widely embraced types of online evidence and sources. The other option is to continue to push the envelope and make use of every possible substantive online source in the aid of your client. Over time, I think the winners choose the latter.

This discussion will address verifying the authenticity of your online evidence, examining witnesses on E-Discovery, citing online content properly, presenting your E-Discovery data, avoiding common mistakes made in the courtroom, and certain aspects of social media. All of these are integral components of successful litigation involving on-line evidence.

I. Verifying Authenticity, Honing your Presentation, and Proper Citation.

When addressing authenticity issues in a courtroom, you are working within the parameters of Evidence Rule 901—Requirement of Authentication or Identification, Evidence Rule 902—Self-Authentication, and sometimes Evidence Rule 903 —Subscribing Witness' Testimony Unnecessary. The threshold for authentication is, in a relative sense, low. The only requirement is that the trier-of-fact *could* find the evidence authentic, not that the *gatekeeper* believes it authentic. The fact that online evidence can be altered or misrepresented goes to its weight, not authenticity. *United States v. Safavian*, 435 F.Supp.2d 36, 41 (D.D.C. 2006).

In the seminal case of *Lorraine v. Markel*, 241 F.R.D. 534 (D. Md. 2007), a federal magistrate set out certain parameters regarding the admissibility of electronic evidence. These include that the evidence must: 1) be relevant; 2) be authenticated; 3) not be disallowable hearsay; 4) meet the "best evidence" rule

where applicable; and (5) have probative value that outweighs the risk of unfair prejudice. This framework is widely recognized, and I will touch on various aspects of it throughout this discussion.

A. E-mails

E-mails are taking on an increasingly important evidentiary role. Often times e-mail provides a clear picture regarding state of mind, intent, and motive. E-mails frequently are authenticated in court by the sending and/or receiving parties. Evidence Rule 901(b)(1) provides that evidence can be authenticated by someone with knowledge of the evidence-at-issue. A witness may state that he or she received e-mails in the past from a certain person at the e-mail address-in-question. Testimony also may indicate that the sender regularly uses the language and phraseology employed in the message, and that the sender and/or receiver were among the very few, or the only people, who knew certain details contained in the message. Names, nicknames, and screen names can by used for authentication purposes. Evidence Rule 901(b)(4) states that the authenticity of evidence can be substantiated by the evidence's "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances."

Obviously there are holes in this methodology as it applies to e-mails, but absent undertaking somewhat arduous and, at times, expensive forensic work on a computer or system, and even then it often comes down to a person's believability, personal testimony is a method often employed. As indicated earlier, the fact e-mail can be altered or misrepresented goes to its weight, not authenticity. Still, when one needs to go further in authenticating an e-mail

message, one can print out the entire routing of the message, substantiate through records that every server along the route handled the message, and then verify who had access to the computers-at-issue at the times in question.

B. Websites

Authenticating websites brings different challenges. The challenge often is authenticating that the owner of the website, or a benign party, as opposed to a hacker, is responsible for the content. Still, many courts have stated that testimony from the website's owner is unnecessary to authenticate, but rather that simply a website visitor can authenticate content by stating that at a certain time and date the visitor typed in a web-address, viewed the information-at-issue, and that the evidence being presented reflects what the witness viewed. Furthermore, it generally is accepted that government websites are self-authenticating pursuant to Evidence Rule 902(5). Webpage printouts also generally meet the requirements of the "best evidence rule," although the rule typically only will be at issue in cases involving copyright infringement, fraud, libel, obscenity, and invasion of privacy, or in similar situations in which the case concerns the content of the webpage itself, as opposed to cases concerning what the webpage content presents about issues apart from the webpage itself.

However, separate from the easier authentication examples above, more substantive authentication is often required or expected by either the gatekeeper or the trier-of-fact, especially in high stakes cases. Internet archive websites such as Internet Archive can provide such authentication. Archive websites also help address the fact that websites present very fluid content, and sometimes just a few words or phrases are changed over time, which can confuse even the author. A

personal attestation from someone associated with the archiving firm often is needed also, both to authenticate that what is being presented represents the firm's records and that the methodology behind the record-retention is sound. Evidence Rule 901(b)(9) provides that evidence can be authenticated by "evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result."

C. Photographs

Online photographs also may present authentication issues. Many photographs have been altered or "enhanced." Someone may be able to authenticate the methodology behind an alteration, but no one then can authenticate that the picture fairly represents the scene at the time of the picture. On the other hand, enhanced photos, where, for example, a portion is enlarged to bring greater clarity, are easier to authenticate as representing what the photographer saw at the time of the picture. Regardless, one must take special care when preparing to authenticate online photographs, and it is arguable that the less one uses them the better.

D. Computer Generated Records

Authentication of computer-generated records often times rests with whether the computer and software were functioning properly at the time the records were generated. Other issues of concern are what procedures were followed to generate the records, and the qualifications of the computer operators. Furthermore, the data inputted and the computer program used also are relevant.

E. Miscellaneous Note

A recent United States Supreme Court decision has arguably placed an additional burden on the use of affidavits for authentication purposes. In *Melendez-Diaz v. Massachusetts*, 129 S.Ct. 2527 (2009), the Court found that it was a violation of the Sixth Amendment's Confrontation Clause for a chemical drug test to be admitted without testimony from the technician who conducted the test. The contours of how this ruling will apply to cases involving online evidence—which often also is filtered through a technician—is still evolving, but it would be safe to have your technician, or anyone who has proffered an affidavit regarding your online evidence, ready to testify if necessary.

II. Examining Witnesses on E-Discovery (20 Questions)

The following are appropriate questions to ask a witness under various circumstances involving E-Discovery:

1. Did trained technicians transfer the evidence?
2. Was a litigation hold placed on the evidence?
3. How thorough was the search for available evidence?
4. Are individual directories purged at any time?

5. Do the paper records accurately reflect the computer-stored records?
6. What steps were taken to ensure compliance with the discovery request or court order?
7. What precautions are, and were, taken to avoid accidental destruction of evidence?
8. Explain the chain of custody?
9. What outside vendors have had access to the data?
10. Explain the data retention policy?
11. Who has access normally to the computers-at-issue?
12. Has software been altered?
13. Has any hardware-at-issue recently been altered?
14. Explain the computer and both the internal and the external (eg. network, server, etc.) system under which it operates?
15. Is data regularly automatically deleted, including by any utility programs?
16. Is data backed up?
17. Were any backup procedures changed in light of this case?
18. Do other parties on a network have access to the evidence?
19. How is the data secured?
20. Is the data encrypted?

III. Tips to Avoid Making Common Courtroom Mistakes

Let opposing counsel know in advance what technology you plan to use. Surprised opponents cause problems for everyone.

Make sure the court knows what you plan to do and that the court is comfortable and has a working knowledge of your technology. Take the time to educate the court in advance if necessary.

Ensure that the courtroom has the infrastructure necessary for you to make use of your online evidence and technology. Test your equipment in the courtroom before the hearing.

Hire an online-evidence professional if you are not on top of the case's online evidence. The worst thing you can do is come across in court as not understanding the evidence, especially if it is your own. There also is a good chance there will be people on your jury who were born, so to speak, with a computer in their hand, and they can be quick, at times, to dismiss someone out-of-hand who is not tech-savvy.

IV. Social Media

Social networking sites often contain the most unadulterated snapshot of a party. Still, frequently issues of relevancy can get in the way of using this information in court. Furthermore, Evidence Rule 403, which can exclude relevant but prejudicial evidence, also often comes into play. Information obtained from social media sites certainly can be embarrassing or prejudicial to a party. Furthermore, if submitted simply to tar a party, it can turn off a trier-of-fact. People who use social media know they have posted things they would not want the whole world to know. Thus, both for legal and logistical reasons, the party introducing such evidence must do so delicately and in a manner that makes clear the evidence's relevance.

Hearsay is another evidentiary hurdle that can arise. Evidence Rule 801 defines a statement as an oral or written assertion. The contents of social media clearly meet this test. However, Evidence Rule 803 provides exceptions to the hearsay rule, and several of the exceptions may apply under certain circumstances. Evidence Rule 803(1)—Present Sense Impressions—allows for the introduction of a statement describing an event or condition, made while or immediately after the declarant perceived it. Clearly, people often post on social networks their thoughts or feelings about events that are unfolding or just have unfolded. That is a major component of the medium. Evidence Rule 803(2)—Excited Utterances—also at times tracks some of the same factors. As would Evidence Rule 803(3)—Then-Existing Mental, Emotional, or Physical Condition. The very nature of social media can implicate Evidence Rule 803(5)—Recorded Recollections. Lastly, comments on someone's social media page could be admissible under Evidence Rule 801(21)—Reputation Concerning Character.

Chat rooms are another type of social media that present similar foundational issues. However, there are several unique aspects to chat rooms. Parties regularly use fake identities in chat rooms. Furthermore, because so much of the content in chat rooms is posted by the users, the web site owner cannot be assumed to have knowledge of what was on the site at any particular time. The transcript of a chat room discussion, as with e-mail, is often authenticated under Evidence Rule 901(b)(4) using circumstantial evidence or other means. In *Ford v. State*, 617 S.E.2d 262 (Ga. Ct. App. 2005), the Georgia Court of Appeals permitted a participant in a chat room conversation to authenticate a transcript. However, evidence from the hard drive of a computer, or independent evidence that a particular individual used, or uses, a particular screen name, may at other times be necessary.