Admissibility of Electronic Evidence: A New Evidentiary Frontier

Posted Oct 14 2013 by Hon. Alan Pendleton in Articles with 0 Comments

Websites, social networks, email, text messaging, computer-generated or stored documents — these new communications technologies challenge evidentiary rules grounded in a more tangible former reality. Authentication of such evidence is perhaps the most difficult challenge as courts seek to determine its admissibility.

Due to the enormous growth in electronic correspondence, electronic writings (also known as e-evidence) have evolved into a fundamental pillar of communication in today's society. Electronic communications have revolutionized how the world does business, learns about and shares news, and instantly engages with friends and family. Ninety one percent of today's online adults use some form of electronic communication regularly in their everyday lives.[1] Not surprisingly, various forms of electronic evidence (*i.e.*, e-evidence) are increasingly being used in both civil and criminal litigation.

During trials, judges are often asked to rule on the admissibility of electronic evidence. How the court rules on questions of admissibility could substantially impact the outcome of a civil lawsuit or determine the difference between conviction or acquittal of a defendant. This unique form of evidence typically falls into one of five distinct categories: 1) Website Data; 2) Social Network Communications and Postings; 3) Email; 4) Text Messages; 5) Computer Stored/Generated Documents.

As courts continue to grapple with this new electronic frontier it is important to stress that electronic evidence is subject to the same rules of evidence as paper documents. However, the unique nature of e-evidence, as well as the ease with which it can be manipulated or falsified, creates hurdles to admissibility not faced with other evidence.

Admissibility of electronic evidence is governed by a four-step analytical framework set forth in the sidebar below. Because e-evidence is subject to manipulation and questions of authorship are often hotly disputed, the requirement to "authenticate" is usually the most difficult to overcome. Each of the five categories of electronic evidence—Website Data, Social Network Communications and

Postings, Email, Text Messages, and Computer Stored/Generated Documents—poses unique problems and challenges for proper authentication and deserves independent consideration.

Analytical Framework

Whenever the admissibility of e-evidence is called into question, the court and attorneys should apply the following four-step analytical framework.

1. **"Authenticate or Identify."** Pursuant to Minn. R. Evid. 901(a), authentication means the party offering the electronic evidence must present sufficient evidence to support a finding that the exhibit in question is what the proponent claims it to be. The most common method of authentication is the use of testimony by a witness with knowledge that the exhibit is what it claims to be. Minn. R. Evid. 9.01(b)(2).
   Inconsistencies and conflicting inferences regarding authenticity often go to the weight of the evidence, not its admissibility. However, because e-evidence is subject to manipulation and questions of authorship are often hotly disputed, the requirement to "authenticate" is usually the most difficult to overcome. *See* "Focus on Authentication" *supra*.
2. **Hearsay or Not?** 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." Minn. R. Evid. 801 (c).
   If the statement is being offered to prove that the assertion is true then the statement is hearsay and is not admissible unless a recognized hearsay exception applies pursuant to statute (M.S. 595.02, subd. 3; 260C.165, etc.) or Rule of Evidence 803, 804, 807. However, if the statement is offered for some other relevant purpose such as to prove knowledge, notice, or the declarant's state of mind, it is not hearsay and is admissible as long as it is "relevant," not "unfairly prejudicial," and is not "privileged." (*See* steps #3 and #4, below).
   One proven method to determine whether a statement constitutes hearsay is to apply what has been referred to as the "Fool-Proof Hearsay Test": 1) Ask whether the relevant purpose for offering the out-of-court statement is its truth; if the answer to that question is "yes," the out-of-court statement is hearsay. 2) If the answer to the question is not clearly "yes," ask "Must the content of the out-of-court statement be believed in order to be relevant?" If yes, the statement is hearsay. If no, the statement is not hearsay.
3. **"Relevant" and Not "Unfairly Prejudicial"?** Under Minn. R. Evid. 401 (and comments) relevant evidence "means evidence having any tendency to make the existence of a fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." Minnesota adopts a liberal approach to relevancy. If the offer has any tendency (even a slight tendency) to make the existence of a fact more probable than it would be without the evidence, it is relevant.
   Even if relevant, evidence may be unfairly prejudicial and may be excluded on that basis. Evidence is "unfairly prejudicial "if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time or needless presentation of cumulative evidence." Minn. R. Evid. 403.
4. **Not "Privileged" Communication?** M.S. 595.02, subd. 1, identifies various communications (*e.g.*, husband-wife; attorney-client; doctor-patient; clergy, etc.) that are considered "privileged" and thus, not admissible unless the privilege is deemed waived.

Data & Postings

Information appearing on private, corporate and government websites is often proffered as evidence in litigation. Printouts of web pages must be authenticated as accurately reflecting the content and image of a specific web page on the computer.

Pursuant to Minn. R. Evid. 902(5) information retrieved from government websites is self-authenticating, subject only to proof that the webpage does exist at the governmental web location. Because of the difficulty and inconvenience that would result if formal authentication was required and the slight risk of fraud or forgery, extrinsic evidence of authentication is not required.[2] However, Rule 902(5) does not preclude the opposing party from attacking the genuineness of the evidence to detract from the weight to be given it by the trier of fact.[3] Newspapers and periodicals may also be self-authenticating.[4]

On the other hand, private websites are not self-authenticating and therefore require additional proof of the source of the posting or the process by which it was generated.[5] For example, in assessing the authenticity of website data, important evidence is normally available from the person(s) managing the website ("webmaster"). A webmaster can establish that a particular file, of identifiable content, was placed on the website at a specific time. This may be done through direct testimony or through documentation, which may be generated automatically by the software of the web server.[6]

The most common method of authenticating website data is having a competent witness testify that he typed in the URL of the website; that he logged onto the site and viewed what was there; and that the exhibit (printout) fairly and accurately reflects what the witness saw.[7] This is no different than that required to authenticate a photograph or other demonstrative exhibit.[8] The witness may be lying or mistaken, but that is true of all testimony and a principal reason for cross-examination. Unless the opponent of the evidence raises a genuine issue as to trustworthiness, it is reasonable to indulge a presumption that material on a website was placed there by the owner of the site.[9] Once material is properly authenticated, inconsistencies or conflicting inferences regarding authenticity go to the weight of the evidence, not admissibility. However, the opponent of the evidence must, in fairness, be free to challenge that presumption by adducing facts showing that the proffered exhibit does not accurately reflect the contents of the website, or that those contents are not attributable to the owner of the site.[10]

In considering whether the opponent has raised a genuine issue as to trustworthiness, and whether the proponent has satisfied it, the courts will look at the "totality of the circumstances," including, for example: (1) length of time the data was posted on the site; (2) whether others report having seen it; (3) whether it remains on the website for the court to verify; (4) whether data is of a type ordinarily posted on same or similar websites (*e.g.*, financial information from corporations); (5) whether the owner of the site (or others) have published the same data elsewhere; (6) whether the data has been republished by others who identify the source of the data as the website in question; (7) whether there is a reasonable risk of hacking or manipulation (*e.g.*, proponent of exhibit was a skilled computer user).[11]

Social Network Messages

Many new types of writings, potentially relevant as evidence in civil and criminal trials, are retrieved from internet sites known as "social networks." Social networking websites permit their members to share information with others. Members create their own individual web pages (their profiles) on which they post personal information, photographs, and videos and from which they can send and receive messages to and from others whom they have approved as their "friends."[12] Anyone can

create a Facebook or MySpace profile at no cost, as long as they have an email address and claim to be over the age of 14[13]

Despite the novelty of social network-generated documents, courts have applied traditional concepts of authentication under existing rules of evidence.[14] The key issue is typically one of authorship: Who authored/posted the proffered document in question? Because of the increased dangers of falsehood and fraud with this new type of medium, courts have imposed a heavier burden of authentication on social network messages and postings.[15]

The general lack of security for this medium raises an issue as to whether a third party may have sent a message via another user's account. Standing alone, the fact that an email communication is sent on a social network and bears a person's name is insufficient to authenticate the communication as having been authored or sent by that person. Generally, there must be confirming circumstances sufficient to permit the inference that the purported sender was in fact the author.[16] As with email, the electronic signature on a document must be corroborated with additional proof of the identity of the sender, such as application of the reply letter doctrine,[17] content known only to the participants, or retrieval of messages from a specific computer.[18]

Generally, electronic conversations on social networking sites (instant messaging) can be authenticated under Rule 9.01(B)(1) by testimony from a participant in the conversation that (a) he or she knows the user name on the social networking site of the person in question, (b) that printouts of the conversation appear to be accurate records of his or her electronic conversation with the person, and (c) a portion of the contents of the communications are known only to the person or a group of people of whom the person in question is one.[19] In the absence of significant corroboration courts have excluded social network messages, stating their concerns with the website's security and the potential for access by hackers.[20]

Profile pages on social network sites raise authentication issues analogous to those raised by website data. In assessing authenticity, it is important to bear in mind that essentially anyone is free to create a profile page using whatever name they choose, so the mere existence of a profile page in someone's name does not necessarily reflect that the purported creator had anything to do with its creation.[21] Such postings do not require a unique user name and password.[22] However, if the characteristics of the proffered e-evidence are "genuinely distinctive," courts are likely to allow circumstantial authentication based on content and context.[23]

There are three common methods of authenticating a social network profile or posting: (1) The first method is to ask the purported creator if he created the profile and also if he added the posting in question; (2) The second option is to search the computer of the person who allegedly created the profile and posting and examine the computer's internet history and hard drive to determine whether that computer was used to originate the social networking profile and posting in question; (3) A third method is to obtain information directly from the social networking website that links the establishment of the profile to the person who allegedly created it and also links the posting sought to be introduced to the person who initiated it.[24]

Email Messages

Like internet evidence, email evidence also raises novel authentication issues. The general principles of admissibility are essentially the same since email is simply a distinctive type of internet evidence; namely, the use of the internet to send personalized communications.

The authenticity of email evidence is governed by Minn. R. Evid 9.01 (a), which requires only "evidence sufficient to support a finding that the matter in question is what its proponent claims." Authenticity is often established by testimony of a witness who sent or received the emails, in essence, that the emails are the personal correspondence of the witness.[25] Testimony from a witness with knowledge that the emails were exchanged with another person constitutes prima facie evidence of authenticity.[26]

Even in the absence of testimony from a direct participant in the communication, under Minn. R. Evid. 9.01(b)(4)
email may be authenticated by reference to its appearance, contents, substance, internal patterns, or other distinctive characteristics taken in conjunction with circumstances.[27] However, because of the risk of manipulation of email headers, evidence that defendant's name is written as the author of an email or that the electronic communication originates from an email (account) that bears the defendant's name is not sufficient alone to authenticate the electronic communication as having been authored or sent by the defendant. There must be some "confirming circumstances" sufficient for a reasonable jury to find by a preponderance of the evidence that the defendant authored the emails.[28] For example, under the "Reply Email Doctrine," evidence that the email to be authenticated (*e.g.*, purportedly sent by defendant) is a timely response to an earlier email message that was sent to defendant's email address has been held sufficient to authenticate the source and genuineness of defendant's email response.[29]

Additional circumstantial indicia that may suffice to establish that email was sent by a specific person includes evidence that: (a) the email in question bears the customary format of an email, including the addresses of the sender and recipient;[30] (b) the address of the recipient is consistent with the email address on other emails sent by the same sender;[31] (c) the email contains the typewritten name or nickname of the recipient (and, perhaps, the sender) in the body of the email;[32] (d) the email contains the electronic signature of the sender;[33] (e) the email recites matters that would normally be known only to the individual who is alleged to have sent it (or to a discrete number of persons including this individual);[34] (f) following receipt of the email, the recipient had a discussion with the individual who purportedly sent it and the conversation reflected this individual's knowledge of the contents of the email.[35]

In the absence of circumstantial evidence of authenticity, there are a variety of technical means by which email transmissions may be traced,[36] such as identifying the encoded internet protocol (IP) address from which or to which the email was sent. Knowing the IP address enables one to contact the service provider who can identify the sender or recipient. Therefore, if serious authentication issues arise, a technical witness may be of assistance. This may become important in cases where a person or entity denies sending an email, or denies receipt of an email, and there is no circumstantial evidence of the sending or receipt of the email or other electronic communication.[37]

Text Messages

Like email, text message evidence also raises novel authentication issues. The general principles of admissibility are essentially the same since text messages are a distinctive type of electronic evidence, namely, the use of a cell phone to send personalized electronic communications. Text messages sent between cell phone users[38] are treated the same as email for purposes of authentication. Typically such messages are admitted on the basis of identifying the author who texted the proffered message. However, mere ownership of the phone that originated the message is

not sufficient.[39] As in authentication of email, authorship can be determined by the circumstances surrounding the exchange of messages; their contents; who had the background knowledge to send the message; and whether the parties conventionally communicated by text message.[40]

Like email and social media, text messages have certain seemingly self-authenticating features. For example, email messages are marked with the sender's email address, text messages are marked with the sender's cell phone number, and Facebook messages are marked with a user name and profile picture. Nonetheless, given that such messages could be generated by a third party under the guise of the named sender, the majority of jurisdictions have not equated evidence of these account user names or numbers with self-authentication. For example, even though text messages are somewhat different than email in that they are intrinsic to the cell phones in which they are stored, as with email accounts, cellular telephones are not always exclusively used by the person to whom the phone number is assigned.[41] As a result, those factors are generally considered circumstantial evidence of authenticity to be considered, along with other circumstantial evidence, in the totality of the circumstances.[42]

Characteristics to consider in determining whether text message evidence has been properly authenticated include: (a) sequential consistency with another text message sent by the alleged author (based on the text message number); (b) the author's awareness, shown through the text message, of details of the alleged author's conduct; (c) inclusion in the text message of similar requests that the alleged author made by phone, email, or other media during the time period; and (d) the text message's reference to the author by the alleged author's nickname.[43]

What about the "Best Evidence Rule"?[44] A recurring factual scenario involves one party transcribing or copying text messages only to realize thereafter that the texts have been purged by the carrier. Thus transcripts made by law enforcement at the time the cell phone is seized are often proffered as evidence of the messages and must be authenticated as an accurate transcription. Such transcriptions of text messages have been held not to violate the Best Evidence Rule if the proponent satisfies Fed. R. Evid. 1004(a) or Minn. R. Evid. 1004(1), which provides that an original is not required when "all originals are lost or have been destroyed, unless the proponent lost or destroyed them in bad faith."[45]

Computer-Stored Documents

When a computer is simply used as a typewriter, computer-stored documents may be authenticated by a percipient witness or by distinctive characteristics that establish a connection to a particular person. The mere presence of a document in a computer file will constitute some indication of a connection with the person or persons having ordinary access to that file. However, much will depend on the surrounding facts and circumstances, and it is reasonable to require that these include some additional evidence of authenticity.[46]

Computer-generated material is the product of the machine itself (not a person) operating according to a program. Pursuant to Minn. R. Evid. 901(b)(9) the process of authentication is two-fold: (1) a description of the system or process to produce a particular result, and (2) evidence showing that the process or system produces an accurate result. For example, when a computer is used to create a data compilation, how much information will be required about data input and processing to authenticate the output will depend on the nature and completeness of the data, the complexity of the manipulation, the routineness of the operation, and verifiability of the result.[47] If the computer is performing more complex manipulations a more elaborate foundation may be required to satisfy Fed. R. Evid. 901(b)(9) or Minn. R. Evid. 901(b)(9).[48] Testimony about the computer equipment, the hardware and software, the competency of the operators, and the procedures for inputting data and

retrieving the output may be necessary, particularly if these elements are challenged.[49] Authenticity may also depend on the accuracy of the process that generates the computer documents. To lay this foundation a qualified witness should have general knowledge of who prepares the printouts and how, and how the system records and retrieves information.[50] If the records are preexisting and identified as belonging to a party-opponent and are thus admissible as party admissions regardless of their accuracy, the information about their retrieval from the parties' computer will suffice.[51]

Basic computer operations relied on in the ordinary course of business are admitted without an elaborate showing of accuracy.[52] The accuracy of the individual computer will not be scrutinized unless specifically challenged and even perceived errors in the output are said to go to the weight of the evidence, not its admissibility.[53]

What about hearsay? Even after properly authenticating an e-evidence exhibit, is there a difference between computer-stored and computer-generated documents/statements? Computer-stored documents are entirely statements by persons and, if offered to prove their truth, can be considered hearsay. However, because computer-generated materials are not statements by persons, but rather are the product of the machine itself operating according to a program, they do not fit the definition of "hearsay."[54]

Conclusion

Electronic communications will continue to revolutionize how the world does business and how individuals instantly engage with friends and family. E-evidence is undeniably a critical new evidentiary frontier which has left both judges and attorneys struggling to understand how the admissibility of this new information fits into existing legal paradigms. Despite this uncertainty, one thing is clear: the use of e-evidence will continue to play an ever-increasing critical role in both civil and criminal litigation. Because e-evidence can have a substantial impact at trial, it is vitally important for attorneys and the court to stay in touch with ongoing legal and technological developments. It is strongly recommended that admissibility issues involving electronic evidence be raised and discussed with the court prior to commencement of trial.

Judge Alan F. Pendleton has served as a judge of the 10th Judicial District since 1999. He is actively involved in attorney and judicial training programs, serves on the Supreme Court Judicial Faculty Development Team, and has offered instruction at several local universities and law schools as well as the National Institute of Trial Advocacy and the National Judicial College in Reno, NV. He currently authors the "Minnesota Judicial Training Updates" which are distributed biweekly throughout the state. Judge Pendleton was awarded the Minnesota District Judges Association's 2012 Outstanding Judge Award.

Notes

Tags: *Courts* **Category:** Articles

Related Posts

-  So You Want to Be a Judge
December 13, 2013

-  Offspring of Camelot's Demise: The Legal Legacy of JFK's Assassination
December 13, 2013
-  Judicial Discretion: Melding Messy Facts and Pristine Law
November 11, 2013

Leave a Reply

Name *

Email *

Website

Submit Comment

Search For...

In All Categories Search

Articles by Issue

Select Month

Articles by Subject

ADR (6)

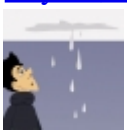
Popular Posts

Recent Comments

- mike on Are Your Clients Making You Crazy? How to Avoid Drama with Maddening Clients
- Yuri on Issues in Joint Custody & Shared Parenting: Lessons from Australia
- jeannie w. bowers on Summary of Public Discipline

- Jon on Debating Voter ID: A Means to Increase Confidence in Elections
- August 2012 - Minnesota Ethics Update | Minnesota Lawyering on Summary of Admonitions

Recent Posts

-  MSBA President 2014-15: Richard Kyle
  July 16, 2014
-  Corporate Liability Under the FCPA: Identifying Defense Opportunities
  July 16, 2014
-  Rental Repairs in Minnesota: The Case for Repair and Deduct
  July 16, 2014

Opportunity Market

Submit a Classified Ad
Subscribe by Email

MSBA Online

- MSBA Home

B&B Online

- Digital Edition
- Directory
- RSS Articles

Advertising

- Classified Ads
- Display Ads
- RSS Classifieds

Contact Us

- Contact the Editor
- Submit an Announcement
- Submit Tips & Traps

- Site Map