MINNESOTA JUDICIAL TRAINING UPDATE

QUESTION: **During trial, judges are often asked to rule on the admissibility of electronic evidence. This unique form of evidence typically takes the form of:**

1) **Website Data;**
2) **Social Network Communications and Postings;**
3) **Email;**
4) **Text Messages;**
5) **Computer Stored/Generated Documents.**

See attached summary sheets addressing "Authenticity" issues for each of the 5 categories of electronic evidence

What Four-Step legal analysis should the court follow in ruling on the admissibility of Electronic Evidence?

ANSWER AND EXPLANATION OF PROBLEM:

1) Due to the enormous growth in electronic correspondence, electronic writings (also known as e-evidence) are increasingly used in both civil and criminal litigation.
2) E-evidence is subject to the same rules of evidence as paper documents, but 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.
3) Admissibility of electronic evidence is governed by a 4-step analytical framework.
4) The requirement of "Authentication" (step one) is the most difficult and hotly contested hurdle to overcome.
5) See page 2 for a summary of the 4-step analysis for admissibility of e-evidence.
6) Because "Authenticity" is at the heart of most e-evidence disputes, attached to this update are five one-page summary sheets addressing "Authenticity" issues for each of the five categories of electronic evidence listed above.
7) Pre-Trial Best Practice: Admissibility issues involving electronic evidence should always be raised and discussed with the court prior to commencement of trial.

4-STEP ANALYSIS FOR ADMISSIBILITY OF E-EVIDENCE - SUMMARY:

STEP 1: EXHIBIT MUST BE "AUTHENTICATED OR IDENTIFIED"

a. The requirement of authentication or identification as a condition precedent to admissibility is satisfied if the proponent of the exhibit presents sufficient evidence to support a finding that the exhibit in question is what the proponent claims it to be. See Minn. R. Evid. 901(a).
b. The most common method of authentication is the use of testimony by a witness with knowledge that the exhibit is what it is represented to be. Rule 9.01(b)(2) (Listing 9 other methods). Inconsistencies and conflicting inferences regarding authenticity often go to the weight of the evidence, not its admissibility.
c. 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.
d. Attached to this update are five one-page "Authentication Summaries", one for each of the five most common forms of electronic evidence: (1) Website Date; (2) Social Network Communications and Postings; (3) Email; (4) Text Messages; (5) Computer Stored/Generated Documents.

STEP 2: DOES EXHIBIT CONSITUTE "HEARSAY OR NON-HEARSAY"

a. DEFINITION: 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).
b. HEARSAY: 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.
c. NON-HEARSAY: 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 step #3 and 4 below).
d. APPLY THE FOOL-PROOF HEARSAY TEST:
    1) Ask the question 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 this next question:
    3) 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 non-hearsay.

STEP 3: MUST BE "RELEVANT" AND NOT "UNFAIRLY PREJUDICIAL"

a. 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. See Minn. R. Evid. 401 (and comments).
b. UNFAIRLY PREJUDICIAL EVIDENCE: "means although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time or needless presentation of cumulative evidence." Minn. R. Evid. 403.

STEP 4: MUST NOT CONSTITUTE "PRIVILEGED" COMMUNICATION

a. M.S. 595.02 subd 1, identifies various communications which are considered "privileged" and thus, not admissible (e.g. husband-wife; attorney-client; doctor-patient; clergy, etc.) unless deemed waived.

1) AUTHENTICATION - WEBSITE DATA AND 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.

1) GOVERNMENT WEBSITES – SELF-AUTHENTICATING: Pursuant to Minn. Rule of Evid. 902(5) information retrieved from government websites are self-authenticating, subject only to proof that the webpage does exist at the governmental web location. Because of the slight risk of fraud or forgery, extrinsic evidence of authentication is not required.[1] Newspapers and periodicals may also be self-authenticating.[2]

2) PRIVATE OR CORPORATE WEBSITES: Private Websites are not self-authenticating.[3] In order to properly authenticate a non-government website there are three questions that must be answered:

a) What was actually on the website?
b) Does the exhibit or testimony accurately reflect it?
c) If so, is it attributable to the owner of the site? (This step is often hotly contested).

3) MOST COMMON METHOD OF AUTHENTICATING WEBSITE DATA: Minn. R. Evid. 9.01(B)(1)

a) Witness testifies 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.[4]

b) This is no different than that required to authenticate a photograph or other demonstrative exhibit.[5] The witness may be lying or mistaken, but that is true of all testimony and a principal reason for cross-examination.

c) Unless the opponent of the evidence raises a genuine issue as to trustworthiness, it is reasonable to indulge a presumption that material on a web site was placed there by the owner of the site.[6] Once properly authenticated, inconsistencies or conflicting inferences regarding authenticity go to the weight of the evidence, not admissibility.

d) 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.[7]

4) TOTALITY OF THE CIRCUMSTANCES: 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 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).[8]

5) CAUTION: Because of the increased risk of hacking or other manipulation of content, many courts are reluctant to attribute documents obtained from a website to the organization or individual who maintains the site.[9] Private website postings are not self-authenticating and therefore require additional proof of the source of the posting or the process by which it was generated.[10] 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.[11]

2) AUTHENTICATION - SOCIAL NETWORK MESSAGES & POSTINGS

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 fourteen.[13]

1) HEAVY BURDEN OF AUTHENTICATION: Despite the novelty of social network-generated documents, courts have applied traditional concepts of authentication under existing Rules of Evidence. [14] See Minn. R. Evid. 9.01(B)(1). 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]

2) SOCIAL NETWORK MESSAGING: 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.[16] 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.[17] 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, content known only to the participants, or retrieval of messages from a specific computer.[18]

@ Most Common Method of Authenticating a Social Network Message: 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 access by hackers.[20]

3) SOCIAL NETWORK PROFILE AND POSTINGS: 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[23] based on content and context.[24]

@ Three Methods of Authenticating a Social Network Profile or Posting: (a) the first method is to ask the purported creator if he created the profile and also if he added the posting in question; (b) 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; (c) 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.[25]

3) AUTHENTICATION – EMAIL MESSAGES

Like internet evidence, email evidence 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.

1) AUTHENTICITY RULE: 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."

2) MOST COMMON METHOD OF AUTHENTICATING EMAIL: 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.[26] Testimony from a witness with knowledge that the emails were exchanged with another person comprises prima facie evidence of authenticity.[27]

3) DISTINCTIVE CHARACTERISTICS AND THE LIKE: 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.[28]

4) RISK OF MANIPULATION: However, because of the risk of manipulation of e-mail headers, evidence that defendant's name is written as the author of an e-mail or that the electronic communication originates from an e-mail (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 e-mails.[29]

5) REPLY EMAIL DOCTRINE: Evidence that the e-mail to be authenticated (e.g. purportedly sent by defendant) is a timely response to an earlier e-mail message that was sent to defendant's email address has been held sufficient to authenticate the source and genuineness of defendant's e-mail response.[30]

6) ADDITIONAL CIRCUMSTANTIAL EVIDENCE OF AUTHENTICATION: Circumstantial indicia that may suffice to establish that email was sent by a specific person include evidence that:

a. Email bore the customary format of an email, including the addresses of the sender and recipient.[31]
b. Address of recipient is consistent with the email address on other emails sent by the same sender.[32]
c. The email contained the typewritten name or nickname of the recipient (and, perhaps, the sender) in the body of the email.[33]
d. The email contained the electronic signature of the sender.[34]
e. The email recited 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).[35]
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.[36]

7) TECHNICAL TRACING OF EMAILS: There are a variety of technical means by which email transmissions may be traced,[37] such as identifying the email coded internet protocol IP address. The IP address allows the recipient of an email to identify the sender by contacting the service provider. 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.[38]

4) AUTHENTICATION – TEXT MESSAGES

Like emails, text message evidence raise novel authentication issues. The general principles of admissibility are essentially the same since text messages, like email evidence, are both distinctive types of electronic evidence - namely, the use of a cell phone or the internet to send personalized electronic communications.

1) TREATED SAME AS EMAILS: Accordingly, text messages sent between cell phone users[39] are treated the same as e-mails for purposes of authentication. Typically such messages are admitted on the basis of identifying the author who texted the proffered message. Mere ownership of the phone that originated the message is not sufficient.[40] Like 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.[41]

2) TOTALITY OF THE CIRCUMSTANCES: Like email and social media, text messages have certain seemingly self-authentication 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.[42] As a result, these features are generally considered circumstantial evidence of authenticity to be considered, along with other circumstantial evidence, in the totality of the circumstances.[43]

3) DISTINCTIVE CHARACTERISTICS TO CONSIDER: Characteristics to consider in determining whether text message evidence has been properly authenticated include: (a) consistency with the text message number in another text message sent by the alleged author; (b) the author's awareness, shown through the text message, of details of the alleged author's conduct; (c) the text message inclusion of similar requests that the alleged author had 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.[44]

4) BEST EVIDENCE RULE: Text messages are effectively emails sent by cell phone but they present unique problems because they are transitory. 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. Generally, testimony of accurate transcription, together with whatever other corroboration may be available, is sufficient *prima facie* evidence of authenticity.[45] In addition, such transcriptions of text messages have been held not to violate the best evidence rule[46] if the proponent satisfies Fed.R.Evid1004(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."[47]

5) AUTHENTICATION - COMPUTER STORED/GENERATED DOCUMENTS

1. WHEN COMPUTER IS USED AS A TYPWRITER OR FOR STORAGE: When a computer is simply used as a typewriter, computer-stored documents may be authenticated by a percipient witness or by distinctive characteristics that establishes 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.[48]

2. COMPUTER-GENERATED MATERIAL: 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.

3. CREATION OF DATA COMPLILATION: 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.[49] A more elaborate foundation may be required to satisfy Federal Rule 901(b)(9) or Minn. R. Evid. 901(b)(9)[50] if the computer is performing more complex manipulations. Testimony about the computer equipment, the hardware and software, the competency of the operators, the procedures for inputting data and retrieving the output may be necessary, particularly if these elements are challenged.[51]

4. ACCURACY OF THE PROCESS: 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 how and who prepares the printouts, and how the system records and retrieves information.[52]

5. PARTY ADMISSIONS: 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.[53]

6. BASIC BUSINESS COMPUTER OPERATIONS: Basic computer operations relied on in the ordinary course of business are admitted without an elaborate showing of accuracy.[54] 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.[55]

7. HEARSAY: COMPUTER-STORED v. COMPUTER-GENERATED: Computer-stored documents are entirely statements by persons and, if offered to prove their truth, can be considered hearsay. However, computer-generated materials are not statements by persons, they cannot fit the definition of 'hearsay" in Minnesota Rule of Evidence 801(c).[56]

8. COMPUTERIZED ANIMATIONS: The standard for the admissibility of demonstrative evidence and visual aids is whether the evidence is relevant and accurate and assists the jury in understanding the testimony of a witness. Demonstrative evidence must be an accurate representation of the evidence in the record to which it relates. This same standard is also applicable to computerized animations.[57]

ENDNOTES

[1] *See, e.g. Weingartner Lumber & Supply Co. v. Kadant Composites, LLC,* 2010 U.S. Dist. LEXIS 24918 (E.D. Ky. Mar. 10, 2010) (printout of official records from website of Securities and Exchange Commission are self-authenticating); *Scurmont LLC v. Firehouse Restaurant Grp.,* 2011 U.S. Dist. LEXIS 75715 (D. S.C. July 8, 2011) ("Records from government websites are generally considered admissible and self-authenticating.").

[2] Minn. R. Evid. 9.01 (6); Federal Rule of Evidence 902(6) provides for self-authentication of "printed material." Fed. Rule of Evidence 101(b)(6), effective December 1, 2011, expands "printed" to include the purely electronic, by providing that: "[A] reference to any kind of written material or any other medium includes electronically stored information." Therefore, Rule 902(6)'s reference to "printed material" extends to information that never reaches hard copy but exists only in cyber space.

[3] C. McCormick, Evidence §227 page 105 (7th ed., 2013).

[4] *Miriam Osborn Mem. Home Ass'n v Rye,* 800 N.Y.S.2d 909 (Sup. Crt. Westchester County 2005) (plaintiff "testified at trial as to the manner in which she downloaded, printed and copied the electronic record of the [government website]. In so doing, it was taken from its electronic from and turned into a tangible exhibit…. [T]his Court concludes that 'the exhibit is a true and accurate representation of such electronic record;'").

[5] *State v. Jackson*, 770 N.W.2d 470, 483 (Minn. 2009) (holding that the test for website authentication is the same as authentication for photographs); *See, e.g.,Actonet, Ltd. v. Allou Health & Beauty Care,* 219 F.3d 836, 848 (8th Cir. 2000) ("HTML codes may present visual depictions of evidence. We conclude, therefore, that HTML codes are similar enough to photographs to apply the criteria for admission of photographs to the admission of HTML codes").

[6] Joseph, Modern Visual Evidence § 15.02[1][a], at 15-4 (2012) ("it is reasonable to indulge a presumption that material on a website….was placed there by the owner of the site.").

[7] *See, e.g., Boim v. Holy Land Found.,* 511 F.3d 707 (7th Cir. 2007) (plaintiff's expert relied in part on Internet website postings in which the terrorist organization Hamas took credit for the murder of plaintiffs' decedent; held, the expert failed sufficiently to elucidate the basis for his conclusion that the website statements were attributable to Hamas and, therefore, the statements were insufficiently authenticated).

[8] Internet and E-Mail Evidence: Admissibility Issues, by Gregory Joseph, ALI-CLE, Page 5, August 22, 2012.

[9] *In re Block,* 727 N.W.2d 166, 177 (Minn.App.2007) (excluding website evidence that had not been authenticated, cautioning that information on websites is subject to being altered at will by site operators. Also holding web pages are not "learned treatises" and are thus subject to stricter scrutiny); C. McCormick, Evidence §227 page 105 (7th ed., 2013); *St. Clair v. Johnny's Oyster & Shrimp, Inc.,* 76 F. Supp. 2d 773, 775 (S.D. Tex. 1999) ("Anyone can put anything on the Internet…the Court holds no illusions that hackers can[not] adulterate the content on any web-site from any location at any time.").

[10] C. McCormick, Evidence §227 page 105 (7th ed., 2013); *In re Homestore.com, Inc. Securities Litigation,* 247 F. Supp. 2d 769, 782-83 (C.D. Cal. 2004) ("To be authenticated, some statement or affidavit from someone with knowledge is required; for example, Homestore's web master or someone else with personal knowledge would be sufficient."). *But see* Joseph, Modern Visual Evidence § 15.02[1][a], at 15-4 (2012) ("It is reasonable to indulge a presumption that material on a website…was placed there by the owner of the site.").

[11] Supra, "Internet and E-Mail Evidence: Admissibility Issues", endnote #8.

[12] C. McCormick, Evidence §227 page 107 (7th ed., 2013); *See United States v. Meregildo*, 883 F.Supp2d 523, S.D. New York (2012) Government did not violate 4th Amendment when it accessed the defendant's Facebook account through a cooperative witness who was "friended" by the defendant.

[13] C. McCormick, Evidence §227 page 107 (7th ed., 2013); See Griffin v. State, 19 A.3d 415, 420 (2011)("Anyone can create a MySpace profile at no cost, as long as that person has an email address and claims to be over the age of fourteen….).

[14] C. McCormick, Evidence §227 page 108 (7th ed., 2013).

[15] C. McCormick, Evidence §227 page 109 (7th ed., 2013).

[16] C. McCormick, Evidence §227 page 108 (7th ed., 2013); *See, e.g., State v. Eleck,* 23 A.3d 818, 821 (Conn.App.2011) (message "could be generated by someone other than the named sender. This is true even with respect to accounts requiring a unique user name and password, given that account holders frequently remain logged in to their accounts while leaving their computers and cell phones unattended. Additionally, passwords and website security are subject to compromise by hacker.").

[17] *See, e.g., Commonwealth v Purdy,* 945 N.E.2d 372 (Mass.2011) ("Evidence that the defendant's name is written as the author of an e-mail or that the electronic communication originates from an e-mail or a social networking Web site such as Facebook or MySpace 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 e-mails." Held, sufficient circumstantial evidence was presented: "in addition to the e-mails having originated from an account bearing the defendant's name and acknowledged to be used by the defendant, the e-mails were found on the hard drive of the computer that the defendant acknowledged he owned, and to which he supplied all necessary passwords. In the absence of persuasive evidence of fraud, tampering, or 'hacking,' this was sufficient to authenticate the e-mails.

[18] C. McCormick, Evidence §227 page 108 (7th ed., 2013); See endnote #30.

[19] Compare, *Ohio v. Bell,* 2009 Ohio App. LEXIS 2112 (Ohio Cr. App. 8th Dist. May 18, 2009), *app. denied,* 914 N.E.2D 1064 (2009) (affirming authentication through alleged victim's testimony that (1) he had knowledge of the defendant's MySpace user name, (2) the printouts appeared to be accurate records of his electronic conversations with defendant, and (3) the communications contained code words known only to defendant and his alleged victims); But compare, *People v. Goins,* No. 289039, 2010 WL 199602, at *1-2 (Mich. App. Jan. 21, 2010) ("Defendant argues that the trial court's decision to exclude the contents of the Myspace entry deprived him of the right to present a defense…. Here, provided in what certainly appears to be Bradley's MySpace page are descriptive details of the assault that fit within what a reasonable person would consider to be 'distinctive content' not generally known to anyone other than Bradley….. The jury reasonably could have found that Bradley authored the content in the MySpace account…. The trial court should have found that the evidence was properly authenticated….").

[20] C. McCormick, Evidence §227 page 108 (7th ed., 2013); *See, e.g., State v. Eleck,* 23 A.3d at 822-824 (Conn.App.2011) (fact that purported author held and managed the account did not provide a sufficient foundation for admitting the printout; content of message did not reflect specific interpersonal conflict, did not reflect distinct information only purported author could have known, nor were the contents corroborated by events nor authorship by a forensic examination); *People v. Al-Shimary,* 2010 WL 5373826 (Mich. Ct. App. 2010) (message on witness's Facebook page offered by defense; witness denied writing the message and defendant made no further offer of proof; no error in trial court's excluding the document as not properly authenticated).

[21] *Griffin v. State,* 19 A.3d 415, 427-28 (2011) ("[A]nyone can create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username and password…. The potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user leads to our conclusion that a printout of an image from such a site requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site in order to reflect that [the depicted person] was its creator and the author of the [relevant] language [on the profile page].").

[22] C. McCormick, Evidence §227 page 109; *Griffin v. State,* 19 A.3d 415, 420-421 (Md. 2011) at issue was a threatening message posted on the purported MySpace page of defendant's girlfriend. The prosecution sought to use this message against defendant to prove that his girlfriend had made the posted threat against a State witness. The Court of Appeals of Maryland was concerned that the page may not have been created by the girlfriend and she may not have posted the threatening message. The court found the prosecution had not presented sufficient corroborating evidence of the girlfriend's ownership of the page, or authorship of the message, to properly authenticate either.

[23] Circumstantial Authentication. When a witness is unavailable or uncooperative, proving that social media content was indeed authored by the user can be a difficult task. Rule 901(b) (4) provides that circumstantial evidence, including "appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances," can help to authenticate evidence. Social networking sites can include a wealth of information, such as profile pages, posts, photographs, and video, as well as several types of metadata, some of which are not publicly visible.

Different types of social media evidence will require different indicia of reliability, for example, profile pages and posts may require sufficiently distinctive data, such as references about which only the author would have known.

[24] In *Griffin v. State*, 19 A.3d 415 (Md. 2011) the prosecution in a murder trial introduced printouts from a MySpace page in an effort to impeach a defense witness. On appeal, the court held that the witness' picture, birth date, and location were not sufficiently distinctive characteristics on a MySpace profile page to authenticate the printout. Because the trial court had given "short shrift" to the concerns that someone other than the putative author could have accessed the account and had "failed to acknowledge the possibility or likelihood that another user could have created the profile in issue," admitting this evidence was held to be reversible error. *Id.* at 423. By contrast, in *Tienda v. State*, 358 S.W.3d 633 (Tex. Crim. App. 2012) the prosecution in another murder trial successfully introduced evidence from *Tienda's* MySpace page that tended to implicate *Tienda* in the shooting death of the victim. There, the circumstantial evidence consisted of relevant metadata fields including *Tienda's* username – which consistent with his commonly known nickname, his stated location, his user ID number, an email address registered to the account, and several photos of *Tienda* with date and time stamps. The court stated this was "ample circumstantial evidence…..to support a finding that the MySpace pages belonged to the Appellant and that he created and maintained them. Id. at 645. Taken together, *Griffin* and *Tienda* demonstrate that if the characteristics of the communication proffered as evidence are genuinely distinctive, courts are likely to allow circumstantial authentication based on content and context. By contrast, if the characteristics are general, courts may require additional corroborating evidence.

[25] *Griffin v. State,* 19 A.3d 415, 427-28 (Md. 2011) ("The first, and perhaps most obvious method [of authentication] would be to ask the purported creator if she indeed created the profile and also if she added the posting in question…. The second option may be to search the computer of the person who allegedly created the profile and posting and examine the computer's internet history and hard drive to determine whether that computer was used to originate the social networking profile and posting in question….A third method may be to obtain information directly from the social networking website that links the establishment of the profile to the person who allegedly created it and also links the posting sought to be introduced to the person who initiated it).

[26] *State v. Bohlman,* No. A05-207, 2008 WL 915765 (Minn.App.Dec.23, 2008)(authentication of e-mails can be done through testimony of a witness "with knowledge" who verifies that the e-mails shown are what they purport to be and that they are sent from the person in question); *Read v. Teton Springs Golf & Casting Club, LLC,* 2010 U.S. Dist. LEXIS 134621 (d. Idaho Dec. 14, 2010) (testimony from recipient of email sufficient to authenticated it); *In re Second Chance Body Armor, Inc.,* 434 B.R. 502, 504 (Bankr. W.D. Mich. 2010) (discussing Fed.R.Evid. 901: "[w]hen the document involved is an e-mail communication, a 'participant in, or recipient of, that communication' will generally be able to authenticate the communication, so long as the person 'was able to perceive who communicated what.'"); *EEOC v. Olsten Staffing Servs. Corp.,* 657 F.Supp.2d 1029 (W.D. Wis. 2009) ("Testimony from someone who personally retrieved the e-mail from the computer to which the e-mail was allegedly sent is sufficient for the purpose").

[27] *State v. Bohlman,* No. A05-207, 2008 WL 915765 (Minn.App.Dec.23, 2008); *Ussery v. State,* 2008 Tex. App. LEXIS 741 (Tex. App. Austin 2008) (approving admission where the victim 'testified, identifying the e-mail communications as fair and accurate copies of actual e-mails she exchanged with appellant. She thus provided testimony authenticating the e-mails.")' *United States v. Gagliardi,* 506 F.3d 140 (2d Cir. 2007) ("[T]he standard for authentications one of 'reasonable likelihood'… and is 'minimal'…. both the informant and Agent Berlas testified that the exhibits were in fact accurate records of [defendant's] conversations with Lorie and Julie. Based on their testimony, a reasonable juror could have found that the exhibits did represent those conversations, notwithstanding that the e-mails and online chats were editable").

[28] *See generally United States v. Siddiqui,* 235 F.3d 1318, 1322 (11th Cir. 2000); *See State v. Reed*, 2009 WL 5088751 (Minn.App.2009) Court did not require handwriting comparison to admit handwritten letter purportedly written by defendant. Because letter referenced defendant's mother, a prior traffic stop, and how defendant felt like he was in a movie with guns in his closet, there were sufficient distinctive characteristics to authenticate the letter.

[29] C. McCormick, Evidence §227 page 103 (7th ed., 2013); *Com. v. Purdy,* 945 N.E.2d 372 381 (2011) Supra fn17*; Lorraine v. Markel American Ins. Co.,* 241 F.R.D. 534, 555 (D. Md. 2007) (noting while there are many ways to authenticate an email, the "most frequent" are 901(b)(1) (person with personal knowledge), 901(b)(3) (expert testimony or comparison with authenticated exemplar), 901(b)(4) (distinctive characteristics, including circumstantial evidence), 902(7) (trade inscriptions), and 902(7) (trade inscriptions), and 902(11) (certified copies of business record)).

[30] C. McCormick, Evidence §224 page 94 and 227 page 108 (7th ed., 2013); *State v. Pullens,* 800 N.W.2d 202 (Neb. Sup. Ct. 2011) (Evidence that an email is a timely response to an earlier message addressed to the purported sender is proper foundation analogous to the reply letter doctrine); *Manuel v. State,* 357 S.W.3d 66, 75-82 (Tex. App. Tyler 2011) (trial court did not abuse its discretion by admitting multiple electronic exhibits, including emails, text messages, Facebook posts, and MySpace posts, based in part on the reply-letter doctrine). *See also, State v. Robinson,* 2003 WL 347592 (Minn.App.2003) When defendant calls an officer back, identifies himself by name, and volunteers the "true owner" of the gun found in his room, circumstances sufficient to authenticate caller's identity. *See also* Goode, The Admissibility of Electronic Evidence, 29 Rev. Litig. 1,25 (2009) (discussing authentication of e-mail, including reply evidence).

[31] *Ecology Servs. v. GranTurk Equip., Inc.,* 443 F.Supp.2d 756, 762 n.1 (D.Md. 2006) (excluding purported email which was not accompanied by an authenticating affidavit and which did not "bear the customary formatting of a printed e-mail message, indicating the sender, recipient, date, and subject").

[32] *Shea v. State,* 167 S.W.3d 98, 105 (Tex. App. 2005).

[33] *Interest of F.P.,* 878 A.2d 91 (Pa. Super. 2005) ("He referred to himself by his first name"); *Commonwealth v. Capece,* 2010 Pa. Dist. & Cnty. Dec. LEXIS 506 (Ct. Common Pl. Oct. 18, 2010).

[34] *See, e.g., Sea-Land Serv., Inc. v. Lozen Int'l, LLC,* 285 F.3d 808, 821 (9th Cir. 2002) (email of one employee forwarded to party opponent by a fellow employee – containing the electronic signature of the latter – constitutes an admission of a party opponent).

[35] *Manuel v. State,* 357 S.W.3d 66, 75-82 (Tex.App. Tyler 2011).

[36] *See generally United States v. Siddiqui,* 235 F.3d 1318, 1322-23 (11th Cir. 2000). See also United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006).

[37] *See, e.g., Clement v. California Dep't of Corrections,* 220 F.Supp.2d 1095, 1111 (N.D. Cal. Sept. 9, 2002) (major email providers include a coded Internet Protocol address (IP address) in the header of every email….The IP address allows the recipient of an email to identify the sender by contacting the service provider).

[38] *See, e.g., Hood-O'Hara v. Wills,* 873 A.2d 757, 760 & n.6 (Pa. Super. 2005) (authenticity not established where person to whom email name belonged denied sending email and testified that problems in the past has required her to modify her email account on at least one prior occasion).

[39] C. McCormick, Evidence §227 (7th ed., 2013); Text messaging, or texting, is the act of typing and sending a brief, electronic message between two or more mobile phones or fixed or portable devices over a phone network. *In re F.P.,* 2005 Pa Super 220, 878 A.2d 91, 93 n.2 (2005). ("'Instant messaging differs from email in that conversations happen in realtime.' http://en.wikipediea.org. 'Generally, both parties in the conversation see each line of text right after it is typed (line-by-line), thus making it more like a telephone conversation than exchanging letters.' Id.").

[40] C. McCormick, Evidence §227 page 104 (7th ed., 2013).

[41] *State v. Haines*, No. 07-1743, 2008 WL 5333357, *4 (Minn.App. Dec. 23, 2008)(method for authenticating text messages is similar to that of authenticating e-mails, and can be done through testimony of a witness "with knowledge", evidence of distinctive characteristics such as appearance, contents, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances. The State must also show that it is reasonably probable that tampering did not occur).

[42] *Commonwealth v. Koch,* 39 A.3d 996 (Pa Super. 2011).

[43] *See, E.g., State v. Eleck.,* 23 A.3d 818, 821 n.4 (2011), *appeal granted,* 302 Conn. 945, 30 A.3d 2 (2011) ("Typically, electronic messages do have self-identifying features. For example, e-mail messages are marked with the sender's e-mail address, test 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, opinions from other jurisdictions have not equated evidence of these account user names or numbers with self-authentication. Rather, user names have been treated as circumstantial evidence of authenticity that nay be considered in conjunction with other circumstantial evidence);

[44] *Manuel v. State,* 357 S.W.3d 66, 74-75 (Tex.App.-Tyler 2011) "an e-mail is properly authenticated if its appearance, contents, substance, or other distinctive characteristics, taken in conjunction with circumstances, support a finding that the

document is what its proponent claims…. Characteristics to consider……include (1) consistency with the e-mail address in another e-mail sent by the alleged author; (2) the author's awareness, shown through the e-mail, of the details of the alleged author's conduct; (3) the e-mail's inclusion of similar requests that the alleged author had made by phone during the time period; and (4) the e-mail's reference to the author by the alleged author's nickname…. Text messages can be authenticated by applying the same factors." *Accord State v. Thompson,* 777 N.W.2d 617 (N.D. Sup. Ct. 2010) (relying on email authentication case law to analyze admissibility of text messages).

[45] *United States v. Culberson,* 2007 U.S. Dist. LEXIS 31044 (E.D. Mich. April 27, 2007), a drug conspiracy prosecution, the DEA agent found text messages on the defendant's phone. He accurately transcribed all texts verbatim but did not immediately print out the texts. Two weeks later he realized the contents were no longer stored on the phone and that the carrier had purged the texts from its system as well. The defense objected to admission of the transcripts because it did not have an opportunity to review the original emails. The Court held that, under the liberal standards of Fed.R.Evid. 9-01(a), the transcription was held sufficiently authenticated by the testimony of (i) the agent, and (ii) one of the co-conspirators.

[46] Minn. R. Evid. 1002

[47] *See United States v. Culberson,* Supra, endnote 45 (holding that defendant failed to carry his burden of establishing bad faith and that the DEA agent's testimony that the emails were unavailable, and that they could not be obtained from cell phone carriers, was sufficient to establish unavailability);

[48] C. McCormick, Evidence §227 page 110, §222 page 85 and §224 page 92 (7th ed., 2013); *Compare Stafford v. Stafford*, 641 A.2d 348 (1993) (testimony of wife that she obtained list of husband's extramarital sexual encounters from family computer held sufficient to authenticate) with *People v. Slusher,* 844 P.2d 1222 (Colo.App.1992) (where date of document's creation critical to relevancy, testimony of witness that he retrieved document dated by computer's internal clock by using defendant's password held not sufficient to authenticate; defendant was a computer programmer, and testimony showed that sophisticated person could tamper with internal clock.

[49] *Turnage v. State,* 708 N.W.2d, 542 (Minn. 2006) (holding that tape recording stored in a digital database re subject to the same test for authenticity as standard tape recordings and duplicates. 'A duplicate [recording] is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original."); C. McCormick, Evidence §227 page 112 (7th ed., 2013); Joseph, Modern Visual Evidence §7.01 [3][b] (2012).

[50] Minn. R. Evid. 901(b)(9) Process or System – "Evidence describing process or system used to produce a result and showing that the process or system produces an accurate result."

[51] C. McCormick, Evidence §227 page 112 (7th ed., 2013); *See generally,* Joseph, Modern Visual Evidence §7.03 [c] (2012) (use of a program in business world or scientific/technical community is taken as evidence of the accuracy of its process).

[52] *State v. Brown,* 739 N.W.2d 716, 722-23 (Minn. 2007) (Unless there is a genuine question as to the authenticity of the original videotaped recording or unfairness in the admission of the digital copy that qualifies as a duplicate, the properly authenticated digital copy is generally admissible. However, recognizing that there is a risk of manipulation or distortion, particularly with digitization….."Commentators have properly urged courts to exercise greater care***for photographic evidence***," Meuller & Kifkpatrick, Federal Evidence § 10:15, at 717 (3d ed.2007); *Turnage v. State,* Supra, endnote 49; C. McCormick, Evidence §227 page 111 (7th ed., 2013); Joseph, Modern Visual Evidence §7.03[2][b] (2012).

[53] C. McCormick, Evidence §227 page 111 (7th ed., 2013).

[54] *Id;* U.S. Salgado, 250 F.3d 438 (6th Cir. 2001) (government not required to present expert testimony on mechanical accuracy when it was shown that the company relied on its system. The authentication of computerized business records is typically satisfied by applying the requirements of the hearsay exception for such records, Federal Rule 803(6)).

[55] C. McCormick, Evidence §227 page 111 (7th ed., 2013); *U.S. v. Catabran,* 836 F.2d 453 (9th Cir. 1988); See 5 Weinstein's Federal Evidence, 900.06 [3](McLaughlin ed. 2012).

[56] Rulings on Evidence, by Judge Gordon Shumaker (Ret.), Chapter 17, page 186, Minn. CLE. 2013.

[57] *State v. Stewart*, 643 N.W.2d 281, 293 (Minn. 2002) the admissibility of a computer-generated animation used to assist a witness in testifying in a criminal case is a question of first impression in Minnesota. The Court found inadequate foundation

for the animation because Roe had no personal knowledge of most of the facts which the animation depicted and had no basis for authenticating any parts of the animated sequences which preceded the actual entry of the bullet into Basta's body, including the actual time in which the events took place, the distance of the gun from Basta at the time the shot was fired, and where appellant was looking when he pulled the trigger. Animation is a new and powerful evidentiary tool, but must be used with great care. Because of its dramatic power, proposed animations must be carefully scrutinized for proper foundation, relevancy, accuracy, and the potential for undue prejudice. The court should issue a cautionary instruction relating to the animation before playing the animation to the jury and in final instructions to help insure its proper use.