MH MITCHELL | HAMLINE School of Law

William Mitchell Law Review

Volume 35 | Issue 4 Article 2

2009

Admissibility of E-evidence in Minnesota: New Problems or Evidence as Usual?

Keiko L. Sugisaka

David F. Herr

Follow this and additional works at: http://open.mitchellhamline.edu/wmlr

Recommended Citation

Sugisaka, Keiko L. and Herr, David F. (2009) "Admissibility of E-evidence in Minnesota: New Problems or Evidence as Usual?," *William Mitchell Law Review*: Vol. 35: Iss. 4, Article 2.
Available at: http://open.mitchellhamline.edu/wmlr/vol35/iss4/2

This Article is brought to you for free and open access by the Law Reviews and Journals at Mitchell Hamline Open Access. It has been accepted for inclusion in William Mitchell Law Review by an authorized administrator of Mitchell Hamline Open Access. For more information, please contact sean.felhofer@mitchellhamline.edu.
© Mitchell Hamline School of Law

MH MITCHELL | HAMLINE School of Law OPEN ACCESS
mitchellhamline.edu

ADMISSIBILITY OF E-EVIDENCE IN MINNESOTA: NEW PROBLEMS OR EVIDENCE AS USUAL?

Keiko L. Sugisaka[†] and David F. Herr[††]

I. INTRODUCTION 1454
II. THE UBIQUITY OF ELECTRONIC INFORMATION 1456
III. STANDARDS RELATING TO ADMISSIBILITY OF ELECTRONIC INFORMATION 1457
A. *Basic Evidentiary Status of Electronic Evidence* 1457
B. *Issues Relating to Electronic Evidence* 1457
1. *Relevance* 1458
2. *Authenticity* 1458
3. *Hearsay* 1460
4. *"Original Writing"* 1460
5. *Absence of Undue Prejudice (Rule 403)* 1461
IV. OVERVIEW OF MINNESOTA EVIDENCE LAW 1462
A. *Importance of Federal Evidence Law* 1462
B. *What Does Rule 901 Require for Authentication?* 1464
C. *How Have Minnesota Courts Historically Treated Authentication Issues?* 113
D. *Authentication Issues Raised by ESI* 1467
E. *Rule 901 Authentication Methods for ESI* 1470
F. *Self-Authentication Under Rule 902* 1475
G. *Shortcuts to Authentication of ESI* 1476
H. *Electronic Evidence for Illustrative Purposes* 1477
V. HOW WILL MINNESOTA COURTS TREAT ADMISSIBILITY OF ESI? 1478

† Keiko Sugisaka is a litigator for the Minneapolis law firm of Maslon Edelman Borman & Brand, LLP. She focuses her practice on business and intellectual property litigation. She has litigated complex commercial cases involving a multitude of evidentiary issues, including those surrounding electronic evidence.

†† David F. Herr is a litigator for the Minneapolis law firm of Maslon Edelman Borman & Brand, LLP. He is the co-author of MINNESOTA HANDBOOK OF COURTROOM EVIDENCE (West 2009) and MINNESOTA TRIAL OBJECTIONS (West 2008), is an Elected Member of the American Law Institute, and serves as the current President of the American Academy of Court-Appointed Masters.

Published by Mitchell Hamline Open Access, 2009

I. INTRODUCTION

In recent years electronic discovery has been the media darling of legal writing, at least in the civil procedure arena. The 2006 amendments to the Federal Rules of Civil Procedure were directed in large part to dealing with discovery of electronic information,[1] and they have generated enormous, and some would say undue,[2] attention to the broader subject of electronic evidence in law review articles,[3] as well as in numerous bar journals and other legal

1. *See, e.g.*, Theodore C. Hirt, *The Two-Tier Discovery Provision of Rule 26(b)(2)(B)—A Reasonable Measure for Controlling Electronic Discovery?*, 13 RICH. J.L. & TECH. 12 (2007); Daniel Renwick Hodgman, *A Port in the Storm?: The Problematic and Shallow Safe Harbor for Electronic Discovery*, 101 NW. U. L. REV. 259 (2007); Richard Marcus, *Only Yesterday: Reflections on Rulemaking Responses to E-Discovery*, 73 FORDHAM L. REV. 1 (2004); Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 4 NW. J. TECH. & INTELL. PROP. 171 (2006).

2. For a thoughtful article suggesting that the e-discovery crisis might be a little overblown, see Hon. James M. Rosenbaum, *The Death of E-Discovery*, 54 FED. LAW. 26 (July 2007).

3. *See, e.g.*, Salvatore Joseph Bauccio, Comment, *E-Discovery: Why and How E-mail Is Changing the Way Trials Are Won and Lost*, 45 DUQ. L. REV. 269 (2007); John L. Carroll, *Developments in the Law of Electronic Discovery*, 27 AM. J. TRIAL ADVOC. 357 (2003); Laura E. Ellsworth & Robert Pass, *Cost Shifting in Electronic Discovery*, 5 SEDONA CONF. J. 125 (2004); James M. Evangelista, *Polishing the "Gold Standard" on the E-Discovery Cost-Shifting Analysis:* Zubulake v. UBS Warburg, LLC, 9 J. TECH. L. & POL'Y 1 (2004); Philip J. Favro, *A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata*, 13 B.U.J. SCI. & TECH. L. 1 (2007); Corinne L. Giacobbe, Note, *Allocating Discovery Costs in the Computer Age: Deciding Who Should Bear the Costs of Discovery of Electronically Stored Data*, 57 WASH. & LEE L. REV. 257 (2000); Kindall C. James, *Electronic Discovery: Substantially Increasing the Risk of Inadvertent Disclosure and the Costs of Privilege Review—Do the Proposed Amendments to the Federal Rules of Civil Procedure Help?*, 52 LOY. L. REV. 839 (2006); Lynn Jokela, Comment: *Electronic Discovery Disputes: Will the Eighth Circuit Courts Move Beyond Ad-Hoc Decision Making?*, 30 WM. MITCHELL L. REV. 1031 (2004); Gregory P. Joseph, *Electronic Discovery*, NAT'L L.J., Nov. 24, 2003, at 30; Virginia Llewellyn, *Electronic Discovery Best Practices*, 10 RICH. J.L. & TECH. 51 (2004); Richard L. Marcus, *E-Discovery & Beyond: Toward* Brave New World *or* 1984*?*, 236 F.R.D. 598 (2006); Richard H. Middleton, *The "Complexities" of Electronic Discovery*, 5 SEDONA CONF. J. 105 (2004); Andrew Moerke Mason, *Throwing Out the (Electronic) Trash: True Deletion Would Soothe E-Discovery Woes*, 7 MINN. J.L. SCI. & TECH. 777 (2006); Michael R. Nelson & Mark H. Rosenberg, *A Duty Everlasting: The Perils of Applying Traditional Doctrines of Spoliation to Electronic Discovery*, 12 RICH. J.L. & TECH. 14 (2006); Rebecca Rockwood, Comment, *Shifting Burdens and Concealing Electronic Evidence: Discovery in the Digital Era*, 12 RICH. J.L. & TECH. 16 (2006); Lee H. Rosenthal, *A Few Thoughts on Electronic Discovery After December 1, 2006*, 116 YALE L.J. POCKET PART 167 (2006); Hon. Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule*

publications.[4] Entire treatises have been written on the subject,[5] and a law school casebook focused on electronic discovery has even appeared.[6] Prominent websites are devoted to "e-discovery," as the subject has become known.[7] Even before the 2006 amendments to the federal rules, the Federal Judicial Center's *Manual for Complex Litigation* recommended that any discovery plan address discovery of electronic information.[8] The federal rules now expressly allow judges to require it.[9]

Comparatively little has been written on the myriad issues relating to how electronic evidence, once discovered, is treated when it is offered as proof.[10] Less still is written on how the issues are handled under Minnesota law.[11]

This article addresses the evidence issues presented by electronic evidence, and suggests how these issues should be addressed under Minnesota evidence law. We specifically do not

34 Up to the Task?, 41 B.C. L. REV. 327 (2000); Bahar Shariati, Note, Zubulake v. UBS Warburg: *Evidence that the Federal Rules of Civil Procedure Provide the Means for Determining Cost Allocation in Electronic Discovery Disputes?*, 49 VILL. L. REV. 393 (2004); Withers, *supra* note 1. Not all of the literature on electronic discovery was written in the twenty-first century. Many of the issues have been recognized for decades. *See, e.g.*, Richard M. Long, Comment, *The Discovery and Use of Computerized Information: An Examination of Current Approaches*, 13 PEPP. L. REV. 405 (1986).

4. *See, e.g.*, Michael C. McCarthy, *Thinking Outside the Box: Recent Developments in Electronic Discovery*, 61 BENCH & B. MINN., Dec. 2004, at 17; Kerry A. Brennan & Mia R. Martin, *Threshold Decisions on Electronic Discovery*, 76 N.Y. ST. B.J., Nov./Dec. 2004, at 23; Stuart Miller & Stephanie Irby Randall, *A Primer on Electronic Discovery for the General Practitioner*, 39 ARK. LAW., Fall 2004, at 16.

5. *See, e.g.*, RONALD J. HEDGES, DISCOVERY OF ELECTRONICALLY STORED INFORMATION (2007); ADAM I. COHEN & DAVID J. LENDER, ELECTRONIC DISCOVERY: LAW AND PRACTICE (2003).

6. SHIRA A. SCHEINDLIN ET AL., ELECTRONIC DISCOVERY AND DIGITAL EVIDENCE: CASES AND MATERIALS (2008).

7. *See, e.g.*, www.ediscoverylaw.com, a particularly helpful site maintained by the Seattle law firm K&L Gates, LLP.

8. *See* MANUAL FOR COMPLEX LITIGATION § 11.446 (J. Stanley Marcus et al. eds., 4th ed. 2004).

9. FED. R. CIV. P. 16(b).

10. "Early" articles addressing these issues include Andrew Jablon, Note, "*God Mail*"*: Authentication and Admissibility of Electronic Mail in Federal Courts*, 34 AM. CRIM. L. REV. 1387 (1997); Anthony J. Dreyer, *When the Postman Beeps Twice: The Admissibility of Electronic Mail Under the Business Records Exception of the Federal Rules of Evidence*, 64 FORDHAM L. REV. 2285 (1996); Christine A. Guilshan, Note, *A Picture Is Worth a Thousand Lies: Electronic Imaging and the Future of the Admissibility of Photographs Into Evidence*, 18 RUTGERS COMPUTER & TECH. L.J. 365 (1992).

11. For one available source, see 11 PETER N. THOMPSON, MINNESOTA PRACTICE: EVIDENCE (3d ed. 2001) (addressing e-discovery in the context of individual rules of evidence and specific case decisions).

intend to contribute to the literature devoted to discovering electronic information. We address the questions of how electronic evidence—whether a party's own information, information obtained by investigation, or obtained from parties or non-parties in formal discovery—can be used in trial proceedings.[12] We conclude that the Minnesota law of evidence is well equipped to deal with admissibility issues relating to electronic evidence. Indeed, it has been doing so successfully for decades.

II. THE UBIQUITY OF ELECTRONIC INFORMATION

If there is one thing every commentator agrees on it is that most information, at least at some point in its life, is stored in electronic form. Many documents or records exist only in electronic form. Experts can only estimate just how large the margin of electronic form of documents is,[13] but there is no room to dispute that the majority of the evidence in many cases and virtually all of it in some cases, is created or used in electronic form.

The ubiquity of electronic evidence is not a "big case" issue, nor is it a "corporate" issue. Discovery of electronic evidence can be encountered in virtually every type of case—personal injury, medical malpractice, marriage dissolution, trust litigation, and every other case type imaginable. Phone records, cell phone

12. "At trial" is really shorthand for any stage of the proceedings where admissibility will be assessed. Evidence used in motion practice must be admissible as well. *See, e.g.*, *In re* Minn. Asbestos Litigation, 552 N.W.2d 242 (Minn. 1996) (holding that exhibits were not authenticated where supported only by conclusory affidavits of counsel); Celotex Corp. v. Catrett, 477 U.S. 317, 322 (1986) (recognizing that for summary judgment, a court may only consider evidence that is admissible). *See generally* 11A PETER N. THOMPSON & DAVID F. HERR, MINNESOTA PRACTICE: COURTROOM HANDBOOK OF MINNESOTA EVIDENCE 487 (West 2009), where the authors state:

> The most important rule to remember is that motions are decided on competent evidence. As a general rule, if evidence would not be admissible at a trial, it should not be probative in a motion hearing. As at trial, where evidence is expressly "offered" into evidence, evidence on a motion should be identified and made part of the record for the motion.

See generally THE SEDONA CONFERENCE COMMENTARY ON ESI EVIDENCE AND ADMISSIBILITY 2 (2008) (noting that summary judgment is the stage in the proceedings where e-evidentiary hurdles are most likely to be encountered).

13. At the Sedona Conference, it was estimated that in 2006, "we created, captured and replicated enough digital information to fill all of the books ever created in the world, 3 million times." *Id.* at 17. By 2011, however, it is estimated that this "digital universe will be 10 times the size it was in 2006." IDC White Paper, *The Diverse and Exploding Digital Universe: An Updated Forecast of Worldwide Information Growth Through 2011,* at 2 (2008).

registers, personal computer information, photographs taken on digital cameras—all can be important evidence in these cases, and many of these "documents" are important in every type of litigated case. E-mail is even more uniformly understood to be encountered and potentially important in every type of case.

III. STANDARDS RELATING TO ADMISSIBILITY OF ELECTRONIC INFORMATION

A. Basic Evidentiary Status of Electronic Evidence

There is no intrinsic barrier in the law of evidence to the admissibility of electronic evidence. For example, e-mail may be admissible, but it also may be excluded from evidence even though relevant to the issues.[14] In general, however, decisions excluding e-mail from evidence do so for reasons other than the intrinsic nature of its electronic form—the evidence may not be relevant, or its receipt in evidence may have unfair prejudicial value that exceeds its probative value, or it may contain hearsay, etc. As e-mail has become a pervasive part of decisions, exclusion of e-mails from evidence merely because they are e-mails is a feature of decisions from the last century.[15]

It is axiomatic that the discovery of information does not give rise to any presumption that it will be admissible at trial. Indeed, just the opposite is so: clearly inadmissible information may well be discoverable. To be discoverable under the rules of civil procedure, information need only be admissible or "reasonably calculated to lead to the discovery of admissible evidence."[16]

B. Issues Relating to Electronic Evidence

The leading case dealing generally with the issues surrounding

14. *Compare* Strauss v. Microsoft Corp., No. 91 Civ. 5928, 1995 WL 326492, at *4–5 (S.D.N.Y. June 1, 1995) (denying motion in limine to exclude e-mail), *with* Monotype Corp. PLC v. Int'l Typeface Corp., 43 F.3d 443, 449 (9th Cir. 1994) (holding that e-mail messages are not business records and thus inadmissible hearsay).

15. *See, e.g.*, *Monotype Corp. PLC*, 43 F.3d at 449 (refusing to recognize e-mail messages as business records).

16. *See* MINN. R. CIV. P. 26.02(a); Ramsey County v. S. M. F., 298 N.W.2d 40 (Minn. 1980). The federal counterpart to this portion of Rule 26.02(a) is identical. *See* FED. R. CIV. P. 26(b)(1). Evidence may be discoverable even if only potentially useful for impeachment. *See, e.g.*, Boldt v. Sanders, 261 Minn. 160, 111 N.W.2d 225 (1961).

admissibility of electronic evidence is *Lorraine v. Markel American Insurance Company*.[17] It is a leading case not because it is the first—electronic evidence has been considered in various forms for years—it is a leading case because it comprehensively and thoughtfully addresses many of the issues. The court in *Lorraine* stated that five evidentiary questions relate to the admission of electronic evidence before it can be found to be admissible: whether the evidence is (1) relevant, (2) authentic, (3) not hearsay or admissible hearsay, (4) the "best evidence," and (5) not unduly prejudicial.[18] In addition to addressing these legal requirements, *Lorraine* is useful precedent because it deals separately with numerous categories of evidence that appear in electronic form.[19] Specifically, the court considered e-mail,[20] Internet web postings,[21] text messages and chat room content,[22] computer-stored records and data,[23] computer animations and computer simulations,[24] and digital photographs.[25] Each of the five evidentiary questions addressed in *Lorraine* has a well-recognized place in the existing law of evidence in Minnesota.

1. Relevance

All evidence must be relevant in order to be admissible.[26] In that respect, there can be nothing unique to electronic evidence on this front. Relevance is not a unique feature of the evidence itself, but rather, essentially a judgment about its connection to the issues in the case. Evidence is relevant if it "logically tends to prove or disprove a material fact in issue."[27] It is hard to think of a piece of evidence that would be relevant in electronic form but not relevant in paper or some other format.

2. Authenticity

Authenticity is a simple prerequisite to master. This

17. 241 F.R.D. 534 (D. Md. 2007).
18. *Id.* at 538.
19. *Id.* at 554–62.
20. *Id.* at 554–55.
21. *Id.* at 555–56.
22. *Id.* at 556.
23. *Id.* at 556–59.
24. *Id.* at 559–61.
25. *Id.* at 561–62.
26. MINN. R. EVID. 402 ("Evidence which is not relevant is not admissible.").
27. Boland v. Morrill, 270 Minn. 86, 99, 132 N.W.2d 711, 719 (1965).

requirement simply asks: "Is this evidence what it purports to be?"[28] Authenticity is often the central battleground for determining admissibility of electronic evidence, as electronic records may be readily altered and made to appear to be something they are not. It is not at all difficult to create a document that looks like an e-mail sent by one of the parties to the case.[29] As we all know from the spam in our inboxes, it is also possible to create an actual e-mail message sent from a purported author who has never seen, sent, or authorized it.[30]

This was also true in the era of typewriters and carbon paper,[31] when parties would occasionally seek to create a document out of whole cloth or fabricate some detail, such as backdating it.[32] Aside from potentially subjecting its creator to sanctions,[33] the document would not be authentic and therefore not admissible (except possibly in a prosecution of the fabricator). Medical records have long been targets of individuals or organizations seeking to rewrite or at least "polish up" history.[34] Medical records are increasingly found only in electronic form; most medical record systems have, or should have, specific mechanisms to permit the record custodian to verify when an entry was made, by whom, and that it hasn't been altered.

28. *See, e.g.*, FED. R. EVID. 901(a); MINN. R. EVID. 901(a).

29. *See, e.g.*, Jimenez v. Madison Area Technical Coll., 321 F.3d 652, 653–54 (7th Cir. 2003) (involving falsified letters and e-mails in an employment discrimination suit).

30. *See, e.g.*, United States v. Kilbride, 507 F. Supp. 2d 1051, 1055 (D. Ariz. 2007) (discussing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, aimed at preventing spam senders from deceiving intended recipients as to the source or subject matter of the e-mail messages); *see also* Joseph F. Cella III & John Reed Stark, *SEC Enforcement and the Internet: Meeting the Challenge of the Next Millennium*, 52 BUS. LAW. 815, 826 (1997) (detailing what is known as "spoofing," which is the altering or falsifying of e-mails to impersonate a real person or user ID of a real person).

31. "Carbon paper *n.* A lightweight paper coated on one side with a dark waxy pigment, placed between two sheets of blank paper so that the bottom sheet will receive a copy of what is typed or written on the top sheet." THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 280 (4th ed. 2000). Carbon paper was widely used before photocopiers came into widespread use.

32. *See, e.g.*, Herbert L. Packer, *A Tale of Two Typewriters*, 10 STAN. L. REV. 409, 420–21 (1958) (analyzing a typewritten forgery).

33. *See, e.g.*, Derzack v. County of Allegheny, 173 F.R.D. 400, 403 (W.D. Pa. 1996) (imposing dismissal as sanction for fabricating evidence).

34. *See, e.g.*, Pisel v. Stamford Hosp., 430 A.2d 1, 15 (Conn. 1980) (examining the substitution of a falsified document in a patient chart after adverse incident). *See generally* Stanford M. Gage, *Alteration, Falsification, and Fabrication on Records in Medical Malpractice Actions*, 27 MED. TRIAL TECH. Q. 476 (1981).

3. Hearsay

To some degree, most electronic evidence presents a hearsay question. Hearsay is defined to be a statement, other than one made by the witness in court, offered to prove the truth of the matter.[35] Hearsay is generally not admissible in evidence,[36] though the exceptions to that rule are abundant.[37]

The rules include dozens of specific exceptions to the general rule that hearsay is inadmissible.[38] Rule 803 identifies twenty-three categories of hearsay that may still be admissible, without regard to whether the person who made the statement is available to testify.[39] Rule 804 identifies additional exceptions applicable only when the declarant is not available to testify.[40]

4. "Original Writing"

The "original writing" rule is one of the more perplexing rules of evidence. The rule is made more opaque by its misleading sobriquet, the "best evidence" rule. Set forth in Minnesota Rules of Evidence 1002, the rule is simple in text: "To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Legislative Act."[41] As is true for hearsay, the "except" clause is as important as the rule because duplicates are routinely admissible instead of the original.[42] Rule 1004 provides the means of admissibility when an original is not available, Rule 1005 provides special rules for "public records," and Rule 1006 allows for receipt of summaries in lieu of voluminous underlying evidence.

The electronic environment does require analysis of how this requirement is met, and there is not always an obvious parallel to how it is met for paper records.

35. *See* MINN. R. EVID. 801. The statement can be an oral or written assertion, or it can be non-verbal conduct intended to be an assertion. *Id.* at 801(a).

36. *See* MINN. R. EVID. 802 ("Hearsay is not admissible except as provided by these rules or by other rules prescribed by the Supreme Court or by the Legislature.").

37. *See* MINN. R. EVID. 803(2)–(23) (listing the exceptions).

38. *Id.*

39. *Id.*

40. MINN. R. EVID. 804(b).

41. MINN. R. EVID. 1002.

42. *See* MINN. R. EVID. 1003 ("A duplicate is admissible to the same extent as an original . . . .").

5. Absence of Undue Prejudice (Rule 403)

Rule 403 provides that even relevant evidence may be excluded from admission. Although the rule is a relevance rule, it operates to override the general rule that relevant evidence will be admissible.[43] Rule 403 frequently presents challenges for electronic evidence, particularly for documents created by computers, such as animations and other illustrative exhibits.[44]

The five-factor test developed in *Lorraine* is similar in result and somewhat more readily applied than an eleven-factor test advocated in *In re Vinhnee*, an earlier bankruptcy appellate decision.[45] *Vinhnee*'s more arduous eleven-factor test should be borne in mind, however, as it does overcome the potential shortcomings inherent in *Lorraine*'s more cursory analysis of potential admissibility issues. Prudent counsel should be prepared to address any of the eleven *Vinhnee* factors.

43. Specifically, this important rule provides: "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.

44. *See generally* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 559–560 (D. Md. 2007) (discussing the unique authentication issues with computer animation and simulation).

45. *See In re* Vinhnee, 336 B.R. 437, 446–47 (B.A.P. 9th Cir. 2005). The court's eleven-factor test for whether adequate foundation for receipt of electronic evidence was adapted from EDWARD J. IMWINKELRIED, EVIDENTIARY FOUNDATIONS § 4.03[2] (5th ed. 2002), and requires that the proponent of electronic evidence establish that:

1. The business uses a computer.
2. The computer is reliable.
3. The business has developed a procedure for inserting data into the computer.
4. The procedure has built-in safeguards to ensure accuracy and identify errors.
5. The business keeps the computer in a good state of repair.
6. The witness had the computer readout certain data.
7. The witness used the proper procedures to obtain the readout.
8. The computer was in working order at the time the witness obtained the readout.
9. The witness recognizes the exhibit as the readout.
10. The witness explains how he or she recognizes the readout.
11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.

(citation omitted).

IV. OVERVIEW OF MINNESOTA EVIDENCE LAW

Minnesota's evidence law reposes primarily in the Minnesota Rules of Evidence. The rules were adopted in 1977[46] and were modeled on the Federal Rules of Evidence. The major part of evidence law not appearing in the rules is the law of privilege, which remains primarily statutory in Minnesota.[47] The Minnesota judiciary has continued to defer to the legislature's policy judgments on questions of privilege, such as the privilege against adverse spousal testimony.[48]

A. Importance of Federal Evidence Law

The Minnesota Rules of Evidence were substantially identical to their federal counterparts at the time of their adoption,[49] and they continue to be either identical or substantially the same. The status of the rules directly relating to electronic discovery, corresponding generally to the five issues identified in *Lorraine*, are set forth in the following table:

46. *See* PETER N. THOMPSON, 11 MINNESOTA PRACTICE: EVIDENCE § 101.01 (3d ed. 2001) (discussing the overview and history of the Minnesota Rules of Evidence).

47. *See* MINN. R. EVID. 501 ("Nothing in these rules shall be deemed to modify, or supersede existing law relating to the privilege of a witness, person, government, state or political subdivision.").

48. *See* State v. Gianakos, 644 N.W.2d 409, 420 (Minn. 2002) (stating the preference to "defer a policy determination of this nature to the legislature").

49. *See* THOMPSON, *supra* note 46, § 101.01.

Minnesota Evidence Rule[50]	Federal Counterpart
Rule 402—Relevance	Substantially identical
Rule 901—Authentication and Identification	Identical
Rule 902—Self-Authentication	Substantially identical, although Minnesota has not adopted Rules 902(11) and (12) relating to certification of business records to facilitate authentication
Rule 801—Hearsay Definitions	Rules 801(a)–(c) are identical; Rule 801(d) (prior statements) is substantially different
Rule 802—Hearsay Rule	Substantially identical
Rule 803—Hearsay Exceptions where availability of declarant is immaterial	Many subdivisions are identical; business records exception (Rule 803(6) uses different language but is substantially the equivalent)
Rule 804—Hearsay Exceptions where declarant is not available	Many subdivisions are identical; rules are substantially similar in purpose and interpretation
Rules 1001 to 1008—Contents of Writings (also known as "Original Writings Rule" or, less helpfully, the "Best Evidence Rule")	Each rule is identical
Rule 403—Relevant evidence may be excluded if probative value outweighed by unfair prejudice or confusion	Identical

The similarity of the rules is important to Minnesota evidence law, for where state and federal rules are substantially similar, the Minnesota courts expressly favor using federal precedent to guide Minnesota case decision-making.[51] The federal cases are especially

50. The comparisons in this table are drawn from 11A PETER N. THOMPSON & DAVID F. HERR, MINNESOTA PRACTICE: COURTROOM HANDBOOK OF MINNESOTA EVIDENCE (West 2008) (comparing each state and federal rule in Chapter 1: Minnesota Rules of Evidence with Commentary).

51. The Minnesota Supreme Court has regularly recognized the value in state court practice of federal court interpretations of the federal rules. *See, e.g.*, Patterson v. Wu Family Corp., 608 N.W.2d 863, 867 n.4 (Minn. 2000) ("Where our

valuable because many important procedural and evidentiary questions are infrequently encountered and are likely not to have been addressed by the Minnesota Supreme Court. The federal decisions therefore provide the only useful decisions to guide Minnesota courts.

B. What Does Rule 901 Require for Authentication?

Authentication, while traditionally not presented as one of the more problematic evidence issues, remains a prerequisite for the potential admission of any piece of evidence.[52] The concept of authentication itself is at once both straightforward and lacking in precise parameters.[53] As Rule 901(a) states, authentication is simply accomplished with "evidence sufficient to support a finding that the matter in question is what its proponent claims."[54] In other words, the proponent of the evidence need only make a prima facie showing that the evidence is what the proponent claims it to be. This is not a particularly high threshold since the court need not find that the evidence is what it claims to be; there only need be sufficient evidence for a jury to reach such a conclusion.[55]

rules of procedure parallel the federal rules, 'federal cases interpreting the federal rule are helpful and instructive but not necessarily controlling' on our interpretation of the state counterpart." (quoting Johnson v. Soo Line R.R. Co., 463 N.W.2d 894, 899 n.7 (Minn. 1990))). *See also* State v. Deal, 740 N.W.2d 755, 761 (Minn. 2007).

52. *See* MINN. R. EVID. 901(a) (identifying "authentication or identification as a condition precedent to admissibility"); *see also id.* committee's cmt. (1977) ("The general rule treats authentication in terms of a condition precedent to admissibility."). Under MINN. R. EVID. 104(a) and 104(b), it is the court and not the fact-finder that makes the admissibility determination. Rule 104(a) governs admissibility matters concerning whether an expert is qualified and if the expert's opinions are admissible, the applicability of any privileges, whether evidence is hearsay, and if any exception applies. *See* MINN. R. EVID. 104(a). Rule 104(b) simply addresses whether the evidence has sufficient probative value for a reasonable jury to find that the evidence is what the proponent claims it to be. *See* MINN. R. EVID. 104(b) committee's cmt. (1977). In doing so, the fact-finder makes the final determination of whether the evidence is authentic. *Id.*

53. MINN. R. EVID. 901(a) committee's cmt. (1977) ("The concept is frequently easy in application but most difficult to define.").

54. MINN. R. EVID. 901(a).

55. PETER N. THOMPSON & DAVID F. HERR, 11A MINNESOTA PRACTICE: COURTROOM HANDBOOK OF MINNESOTA EVIDENCE 272 (West 2008).

C. How Have Minnesota Courts Historically Treated Authentication Issues?

With this standard in mind, Minnesota appellate courts generally have not mandated specific requirements for proper authentication.[56] As noted by the Minnesota Supreme Court in 1927 in *Lundgren v. Union Indemnity Co.*:

> It is difficult, if not impossible, to formulate a standard of admissibility at once definite and dependable. But it occurs to us that any relevant writing may be admitted when from its contents and other circumstances in evidence it is reasonably inferable that the author is the person sought to be charged or another lawfully acting for him. "Evidence which, if uncontradicted, would satisfy a reasonable mind" is sufficient.[57]

Thus, as a result of the common law and the general standard under Rule 901(a), Minnesota courts have experienced little difficulty in deciding authentication issues for a variety of documentary and tangible evidence such as telegrams,[58] business records,[59] letters,[60] photographs,[61] videotapes,[62] audiotapes,[63] public

56. PETER N. THOMPSON, 11 MINNESOTA PRACTICE: EVIDENCE § 901.01 (3d ed. 2001) ("Very few appellate decisions set out specific rules to be applied by the trial judge in making rulings on authentication and identification."). *But see* Furlev Sales & Assocs., Inc. v. N. Am. Auto. Warehouse, Inc., 325 N.W.2d 20, 27 n.9 (Minn. 1982) (describing a seven-step process for authenticating audiotapes).

57. 171 Minn. 122, 125, 213 N.W. 553, 555 (1927).

58. *See, e.g.*, *id.* at 126–27, 213 N.W. at 555 (holding that a telegram is not authenticated when there is no evidence offered to support authentication); Halstead v. Minn. Tribune Co., 147 Minn. 294, 297–98, 180 N.W. 556, 557–58 (1920) (explaining that subsequent correspondence, conduct, and acknowledgment of receipt successfully authenticated the telegram).

59. *See, e.g.*, Lund v. Vill. of Princeton, 250 Minn. 472, 484, 85 N.W.2d 197, 206 (1957) (authenticating business records and noting that "it is not required that every person who took part in the compilations of business records should testify as to their accuracy"); Watson v. Gardner, 183 Minn. 233, 234, 236 N.W. 213, 214 (1931) (receiving bank and mortgage company books and records into evidence); Johnson v. Burmeister, 182 Minn. 385, 386–87, 234 N.W. 590, 590–91 (1931) (allowing corporate minutes to be authenticated by corporation's former auditor and director); State v. Johnson, 179 Minn. 217, 221, 228 N.W. 926, 927–28 (1930) (affirming the admittance of bank books and records); State v. Thornton, 174 Minn. 323, 326, 219 N.W. 176, 177 (1928) (affirming the admittance of bank books and records). Unlike the federal rules, the Minnesota Rules of Evidence do not provide for a specific authentication rule for business records. *Compare* FED. R. EVID. 902(11) (providing for the authentication of business records), *with* MINN. R. EVID. 902 (providing rules for other self-authenticating documents). The authentication requirement for business records in Minnesota is instead found in Rule 803(6) as a hearsay exception. *See* MINN. R. EVID. 803(6).

records,[64] and other types of documentary information.[65] Circumstantial evidence of authentication will commonly suffice when a document's accuracy is in question because the Minnesota

60. *See, e.g.*, State v. Pippitt, 645 N.W.2d 87, 95 (Minn. 2002) (explaining that a letter was not authenticated when the witness denied writing the letter and no other evidence was offered to authenticate it).

61. *See, e.g.*, State v. Daniels, 361 N.W.2d 819, 828 (Minn. 1985) (explaining that there was no authentication of photographs of a crime scene taken fourteen months after event); LaCombe v. Minneapolis St. Ry. Co., 236 Minn. 86, 93, 51 N.W.2d 839, 844 (1952) (admitting photographs as authenticated after "ample testimony" was offered, establishing that the photos "accurately depicted conditions which were the same as those prevailing at the time of the accident"). The "conventional method for authenticating photos is referred to as the 'pictorial witness theory' because the photograph is thought to be a pictorial representation of what the witness observed." *In re* Welfare of S.A.M., 570 N.W.2d 162, 164 (Minn. Ct. App. 1997).

62. *See, e.g.*, State v. Brown, 739 N.W.2d 716, 721–22 (Minn. 2007) (allowing a digitized copy of a VHS videotape to be authenticated by establishing chain of custody and description of process for digitizing tape); State v. Williams, 337 N.W.2d 689, 690–91 (Minn. 1983) (involving authentication by a video recorder operator who observed events depicted on videotape); *S.A.M.*, 570 N.W.2d at 166 (authenticating videotape by testimony describing the reliability of the process or system that created the tape, as well as by testimony from an observer that videotape accurately portrayed the event); Scott v. State, 390 N.W.2d 889, 892–93 (Minn. Ct. App. 1986) (allowing authentication by a witness who observed events depicted on videotape and technician who produced the tape and did not alter it).

63. *See, e.g.*, Furlev Sales & Assocs., Inc. v. N. Am. Auto. Warehouse, Inc., 325 N.W.2d 20, 27 n.9 (Minn. 1982) (describing a seven-step process for authenticating audiotapes); *see also* Turnage v. State, 708 N.W.2d 535, 542 (Minn. 2006) (allowing a digital database of phone calls at a workhouse to be authenticated using *Furlev* elements); State v. Washington, 725 N.W.2d 125, 136–37 (Minn. Ct. App. 2006) (authenticating a 911 tape based on police testimony); *In re* Gonzalez, 456 N.W.2d 724, 728 (Minn. Ct. App. 1990) (involving an answering machine recording that was authenticated by a witness who identified the voice on a recording).

64. *See, e.g.*, Hennepin County v. Shasky, 289 Minn. 44, 49–50, 182 N.W.2d 431, 435 (1970) (allowing authentication of a map by an expert familiar with the property on the map); State v. Northway, 588 N.W.2d 180, 182 (Minn. Ct. App. 1999) (holding that a price report was not authenticated under MINN. R. EVID. 901(b)(7), 902 or MINN. STAT. § 600.13 (2008) when no evidence substantiated that the price report came from the U.S. Department of Agriculture; the price report did not contain a seal, certification, authorized signature, or other such marking; and no evidence or authority indicated it was an official publication under MINN. R. EVID. 902(5)).

65. *See, e.g.*, Gopher Oil Co. v. Am. Hardware Mut. Ins. Co., 588 N.W.2d 756, 765 (Minn. Ct. App. 1999) (involving an insurance declaration and endorsement authenticated under MINN. R. EVID. 901(b)(1)); Minneapolis Pub. Hous. Auth. v. Greene, 463 N.W.2d 558, 561 (Minn. Ct. App. 1990) (allowing a chemist's report to be authenticated by a chemist's certification on the report and by chain of custody testimony by the police officer who provided the tested substance to the chemist).

Supreme Court has long recognized relevant circumstantial evidence as bearing on authentication.[66] For example, in *State v. Johnson*, where the issue involved whether entries in a bank's general ledger had been falsified, an examination of the ledger records of a separate bank in which the bank kept a deposit account satisfied the court that the general ledger records were authentic.[67] The proponent of the evidence did not present any direct testimony that the signatures on the bank's remittance documents to the deposit bank were signatures of bank officers; instead, comparison of the documents to an "untainted" third party—the depository bank—demonstrated their authenticity.[68] The Minnesota Supreme Court was satisfied by evidence showing that the two banks engaged in regular, daily transactions for remittances, and withdrawals from which a comparison could be made for the accuracy of the bank's records and identification of the falsified entries.[69]

This application of circumstantial evidence to establish authentication will continue to play an important role for electronically stored information ("ESI"). Given the wide range of forms ESI can take, the heightened potential for its intentional or unintentional manipulation, and the relative impossibility of eliminating all possibility of such manipulation, circumstantial evidence may be a party's best and perhaps only method to satisfy authentication requirements.

D. Authentication Issues Raised by ESI

Although satisfying authentication requirements provides a sufficient basis for finding that evidence is what it purports to be, authentication is not intended or presumed to be completely foolproof.[70] At best, authentication requirements simply present

66. *See* Lundgren v. Union Indem. Co., 171 Minn. 122, 125, 213 N.W. 553, 555 (1927) ("Upon the preliminary issue of admissibility, any evidence which promises relevancy should be received, at least tentatively, for decision will frequently depend upon many circumstances, some of which if isolatedly considered would seem irrelevant.").

67. 179 Minn. 217, 218–20, 228 N.W. 926, 927 (1930).

68. *Id.* at 220, 228 N.W. at 927.

69. *Id. See also* Katzmarek v. Weber Brokerage Co., 214 Minn. 580, 583, 8 N.W.2d 822, 824 (1943) (allowing admission of telephone call when identity of person called could be "established with reasonable certainty by means of the surrounding facts and circumstances").

70. In order to authenticate evidence, a proponent need not negate "all

obstacles to mistakes or manipulation. While the opportunity for mistake or manipulation is heightened when ESI is involved, the requirements for authenticating ESI have not necessarily been heightened by Minnesota courts in response.[71] To date, no Minnesota state court decisions have specifically addressed authentication of ESI or any requirements for ESI beyond that specified by Minnesota Rule of Evidence 901(a) or 902.[72] The absence of additional guidance may be alarming to some given that electronic evidence may involve issues of improper entry, retrieval, conversion, or storage of data that can compromise the data's integrity.[73] Although the potential for inaccuracy or manipulation exists on a larger scale than for paper records, these problems are not necessarily unique to ESI. In fact, the authentication of ESI need not necessarily be more time consuming, expensive, or problematic than the authentication of traditional writings or

possibility of tampering or substitution." State v. Johnson, 307 Minn. 501, 505, 239 N.W.2d 239, 242 (1976). "Contrary speculation may well affect the weight of the evidence . . . but does not affect its admissibility." *Id.*

71. Elsewhere, courts and commentators have been critical of the accuracy of ESI and call for more stringent showings of authentication. *See generally* United States v. Scholle, 553 F.2d 1109, 1125 (8th Cir. 1977) (noting that "the complex nature of computer storage calls for a more comprehensive foundation[,]" but admitting a printout of compiled electronic data as a business record); Rudolph J. Peritz, *Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence*, 80 NW. U. L. REV. 956 (1986).

72. This is true even though Minnesota courts have recognized the potential for inaccuracy in digital evidence. *See* State v. Brown, 739 N.W.2d 716, 723 (Minn. 2007) (recognizing that "[d]espite the requirement that the duplicate be produced by a technique designed to accurately reproduce the original, we understand that there is the risk of manipulation or distortion, particularly with digitization, and 'commentators have properly urged courts to exercise greater care for photographic evidence.'") (quoting CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, FEDERAL EVIDENCE § 9:23, at 509 (3d ed. 2007)). Other commentators have noted that "[n]o additional authenticating evidence is required just because the records are in computerized form rather than pen or pencil and paper." 5 JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 901.08[1] (2d ed. 2009); *see also* United States v. Koontz, 143 F.3d 408, 412 (8th Cir. 1998) (finding "no reason" to reject a booking report "simply because it was computer-generated"); MANUAL FOR COMPLEX LITIGATION (FOURTH) § 11.446 (2004) ("In general, the Federal Rules of Evidence apply to computerized data as they do to other types of evidence.").

73. *See* MANUAL FOR COMPLEX LITIGATION (FOURTH) § 11.446 (2004) ("Accuracy may be impaired by incomplete data entry, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions. The integrity of data may also be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling.").

evidence.[74]

Nonetheless, Minnesota evidence law has recognized the need to address issues involving potential manipulation of evidence. In *Furlev Sales & Associates, Inc. v. North American Automotive Warehouse, Inc.*, the Minnesota Supreme Court set forth seven foundational elements for admission of a tape recording:

> (1) a showing that the recording device was capable of taking testimony; (2) a showing that the operator of the device was competent; (3) establishment of the authenticity and correctness of the recording; (4) a showing that changes, additions and deletions have not been made; (5) a showing of the manner of the preservation of the recording; (6) identification of the speakers; and (7) a showing that the testimony elicited was voluntarily made without any kind of inducement.[75]

While the *Furlev* requirements have not always been followed for admitting tape recordings,[76] several of these factors have the potential to apply to ESI. The requirements of establishing that the data is authentic and correct and that "changes, additions and deletions have not been made" is a challenge for all forms of ESI given the ease in which it can be altered. In addition, the competency of a recording device and its operator has potential application to computer-stored or computer-processed data.[77]

In addition, establishing chain of custody may come into play for ESI. This is a traditional method of demonstrating, through testimony or evidence establishing the continuous whereabouts of the item at issue, that evidence has not been contaminated or altered.[78] Indeed, chain of custody has been an essential element for many forms of physical evidence that are not otherwise unique

74. Indeed, the greater time and expense involved in satisfying "fail-safe" standards for authenticating ESI likely outweighs the likelihood of the existence of mistake or fraud.

75. 325 N.W.2d 20, 27 n.9 (Minn. 1982). In *Furlev*, the tape recording at issue was admitted without meeting these seven foundational requirements but the court determined that such error was harmless. *Id.* at 27–28.

76. *Compare* Turnage v. State, 708 N.W.2d 535, 542 (Minn. 2006) (finding digital database of phone calls at workhouse authenticated under *Furlev* elements) *with* State v. Washington, 725 N.W.2d 125, 136–37 (Minn. Ct. App. 2006) (authenticating 911 tape based on police testimony) *and In re* Gonzalez, 456 N.W.2d 724, 728 (Minn. Ct. App. 1990) (allowing authentication of answering machine recording by witness who identified the voice on a recording).

77. These requirements are more fully discussed *infra* with regard to MINN. R. EVID. 901(b)(9) addressing authentication of a process or system.

78. *See* State v. Johnson, 307 Minn. 501, 504, 239 N.W.2d 239, 242 (1976).

and inherently identifiable by their appearance.[79] Establishing chain of custody does not require eliminating all possibility of alteration or manipulation.[80] But "the more susceptible the item is to alteration, substitution, or change of condition, the greater the need to negate such possibilities."[81] This is particularly true of ESI given that it can exist in multiple locations with varying degrees of access and can be readily altered.

E. Rule 901 Authentication Methods for ESI

Rule 901(b) provides ten non-exhaustive illustrations of authentication methods, including direct testimony, circumstantial evidence, and proof of custody. The following authentication methods would most commonly apply to different types of ESI:

> (1) *Testimony of witness with knowledge.* Testimony that a matter is what it is claimed to be.[82]

The simplest and most common form of direct proof to authenticate is the production of a witness with personal knowledge who testifies that the item is what it purports to be, whether through authorship, source, substance, accuracy, or otherwise. The witness may authenticate the document by demonstrating proof of authorship or other connection, including by witnessing authorship or receipt of the document.[83] This rule encompasses a variety of ESI, including e-mail, instant messages, text messages, chat rooms, and web pages.[84]

79. *See, e.g.*, State v. Bellikka, 490 N.W.2d 660, 663 (Minn. Ct. App. 1992) (establishing that a chain of custody is required for common items such as controlled substances and bodily fluids).

80. State v. Hager, 325 N.W.2d 43, 44 (Minn. 1982) (quoting M. Graham, *Evidence and Trial Advocacy Workshop: Relevance and Exclusion of Relevant Evidence—Real Evidence*, 18 CRIM. L. BULL. 241, 243–47 (1982)).

81. *Id.*

82. MINN. R. EVID. 901(b)(1).

83. *See id.*

84. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 554–56 (D. Md. 2007); United States v. Safavian, 435 F. Supp. 2d 36, 40 n.2 (D.D.C. 2006) (holding that authentication of e-mail may occur by a witness with personal knowledge of e-mail); United States v. Tank, 200 F.3d 627, 630–31 (9th Cir. 2000) (holding that authentication of chat rooms may occur by a person who participated in the chat room, can identify chat room users, and can testify that the chat room log is an accurate representation). For a web page, the party could offer a witness who visited the website at a particular URL address—whether it be a website administrator or third party—reviewed its content and testified that the printout or other exhibit accurately reflected what was at the URL address. *Accord* St. Luke's Cataract & Laser Inst., P.A. v. Sanderson, No. 8:06-CV-223-T-MSS, 2006 WL

> (3) *Comparison by Trier or Expert Witness.* Comparison by the trier of fact or by expert witnesses with specimens that have been authenticated.[85]

Authentication may occur via comparison by the factfinder or expert witness with previously authenticated examples.[86] Such a comparison by the fact finder, however, is subject to limitations recognized by the rule drafters.[87] Clearly, the more sophisticated the evidence is or the more specialized knowledge is needed to interpret it, the less likely jurors will be allowed to authenticate such evidence. This may implicate certain types of ESI, such as technical computer data or metadata that may require analysis by expert witnesses. On the other hand, more common and easily identified forms of ESI, such as e-mail, can be authenticated under this Rule by jurors.[88]

> (4) *Distinctive Characteristics and the Like.* Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.[89]

The presence of distinctive characteristics, including circumstantial evidence, that show that the evidence is what it purports to be provides sufficient authentication under Minnesota Rule of Evidence 901(b)(4).[90] Circumstantial proof of authenticity has long been recognized as an acceptable method of

1320242, at *1–2 (M.D. Fla. May 12, 2006) (requiring testimony from person with personal knowledge of a website, such as a webmaster, to authenticate printouts from a website); Telewizja Polska USA, Inc. v. Echostar Satellite Corp., No. 02 C 3293, 2004 WL 2367740, at *6 (N.D. Ill. Oct. 15, 2004) (finding that an Internet archive is a form of evidence). Other courts, however, appear to require more stringent standards for website authentication. *See* United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000) (finding no authentication of website postings because proponent needed to show that website postings were actually posted by particular group and not proponent herself), *cert. denied*, 531 U.S. 973 (2000).

85. MINN. R. EVID. 901(b)(3).

86. *Id.* at committee's cmt. (1977) ("The practice of allowing jurors to determine the authenticity of a writing has been approved in Minnesota.") (citing State v. Houston, 278 Minn. 41, 44, 153 N.W.2d 267, 269 (1967)).

87. *Id.* ("The rule should not be read as a statement that jurors can authenticate other matters by comparison techniques without the benefit of expert testimony, *e.g.*, ballistics or fingerprints. These questions must be resolved on a case by case basis.").

88. *See Safavian*, 435 F. Supp. 2d at 40 (allowing jurors to compare e-mails with authenticated e-mails from same purported sender in order to authenticate them under Federal Rule of Evidence 901(b)(3)).

89. MINN. R. EVID. 901(b)(4).

90. *Id.* at committee's cmt. (1977) ("This illustration indicates that an offer of evidence can be authenticated by circumstantial evidence.").

authentication.[91] For example, letters, telegrams, and telephone conversations were commonly authenticated by the "reply doctrine."[92] The reply doctrine recognizes that distinctive content or substance in a communication can demonstrate the source, author, or other authenticity.[93] This same doctrine can apply to e-mail, text, and instant messages[94] with the recipient's use of the reply function. Other distinct characteristics of e-mail that may provide sufficient circumstantial evidence include the sender's e-mail address and contents of the e-mail that may reveal details only known to the sender and the person receiving the message.[95] These "distinctive characteristics," however, are still subject to the risk that someone other than the named sender sent the message. Thus, a court may still require a witness with personal knowledge under Rule 901(b)(1) to attest to the accuracy of the contents or other information related to the message, such as its transmission date or time.[96]

Another method for authentication under Rule 901(b)(4) for ESI is the use of hash values.[97] A hash value is "[a] unique

91. *Id.* *But see* Monotype Corp. PLC v. Int'l Typeface Corp., 43 F.3d 443, 449 (9th Cir. 1994).

92. MINN. R. EVID. 901(b)(4) committee's cmt. (1977); Merchants' Nat'l Bank v. State Bank of Worthington, 172 Minn. 24, 30, 214 N.W. 750, 753 (1927) (concluding telephone conversation authenticated that affirmed previous agreement kate – I'm not sure what this parenthetical is trying to say); Halstead v. Minn. Tribune Co., 147 Minn. 294, 297–99, 180 N.W. 556, 557–58 (1920) (determining reply telegraph authenticated same comment); Hoxsie v. Empire Lumber Co., 41 Minn. 548, 550, 43 N.W. 476, 477 (1889) (determining reply letter authenticated same).

93. 11 PETER N. THOMPSON, MINNESOTA PRACTICE SERIES: EVIDENCE § 901.05 (3d ed. 2001).

94. An in-depth analysis of authentication of instant messages has been addressed elsewhere. *See e.g.*, Andrew M. Grossman, *No, Don't IM Me—Instant Messaging Authentication, and the Best Evidence Rule*, 13 GEO. MASON L. REV. 1309 (2006).

95. *See, e.g.*, United States v. Siddiqui, 235 F.3d 1318, 1322–23 (11th Cir. 2000); United States v. Safavian, 435 F. Supp. 2d 36, 39–41 (D.D.C. 2006). Instant messages have also been authenticated under rules similar to 901(b)(4). *In re* F.P., 878 A.2d 91, 94 (Pa. Super. Ct. 2005).

96. WEINSTEIN'S FEDERAL EVIDENCE, *supra* note 72, § 900.73[3][c].

97. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 546–47 (D. Md. 2007) ("Hash values can be inserted into original electronic documents when they are created to provide them with distinctive characteristics that will permit their authentication under [Fed.] Rule 901(b)(4)."). *See also* Federal Evidence Review, Using "Hash" Values in Handling Electronic Evidence, http://federalevidence.com/blog/2008/september/using-%E2%80%9Chash%E2%80%9D-values-handling-electronic-evidence (Sept. 18, 2008) (discussing additional uses for hash values for electronic evidence during

numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set."[98] The likelihood of data sets having the same hash values "is less than one in a billion."[99] Thus, the hash value "is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production."[100] Therefore, one can fairly determine that a copy of an electronic file has not been altered if its hash value is identical to the hash value of the original.

Metadata may also provide sufficient distinctive characteristics for authentication of electronic information under Rule 901(b)(4).[101] Metadata is essentially data about data, which "describes how, when, and by whom the data set or document was collected, created, accessed, or modified; its size; and how it is formatted."[102] Although this type of information is useful for attempting authentication under Rule 901(b)(4), it does not appear to have the same accuracy as hash values and may require additional authentication methods such as witnesses with personal knowledge or expert testimony.[103]

> (9) *Process or System.* Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.[104]

This illustration in the Rule's commentary is the only one specifically contemplating computer-related evidence in the Minnesota Rules:

> The admissibility of evidence based on X-rays, computer printouts, voice-prints, public opinion polls, etc., all depend upon a showing that the process or system used does produce an accurate result. The degree of accuracy required might vary with the purposes for which the evidence is being offered, the state of the art, and the type

litigation).

98. BARBARA J. ROTHSTEIN ET AL., FED. JUDICIAL CTR., MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES 24 (2007).

99. *Id.*

100. *Id.*

101. *Lorraine*, 241 F.R.D. at 547.

102. ROTHSTEIN ET AL., *supra* note 98, at 24–25.

103. *See* Fennell v. First Step Designs, Ltd., 83 F.3d 526, 530 (1st Cir. 1996) (noting that metadata may be changed by saving electronic files in different locations).

104. MINN. R. EVID. 901(b)(9).

of method or process involved.[105]

Rule 901(b)(9) may be useful for ESI resulting from a computer program designed to produce a result, *i.e.*, computer-generated information, as opposed to information or data that is simply stored on a computer.[106] Thus, computational software, graphs, tables, animations, and spreadsheets could all fall into this authentication category. Although no Minnesota courts have addressed any specific requirements for Rule 901(b)(9), a party would be well advised to be able to show, at a minimum, that the computer process or system at issue is reliable and provides accurate results, explain the procedure or protocol for providing data to the computer process or system, and show that such procedure or protocol was followed in the producing the results at issue.[107]

> (10) *Methods provided by statute or rule.* Any method of authentication or identification provided by Legislative Act or by other rules prescribed by the Supreme Court pursuant to statutory authority.[108]

This rule was "intended to make it clear that rule 901 does not limit or supersede other forms of authentication."[109] For example, Minnesota passed the Electronic Authentication Act in 1997.[110] The Act provides for the authentication of certified digital signatures, although the Act is still subject to court evidentiary requirements.[111]

105. *Id.* at committee's cmt. (1977).

106. Information that is simply stored in electronic form may be adequately authenticated under Minnesota Rule 901(b)(1). "In general, electronic documents are records that are merely stored on a computer and raise no computer-specific authentication issues." JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 900.06[3] (Joseph M. McLaughlin ed., Matthew Bender 2d ed. 1997).

107. A far more demanding showing, consisting of an eleven-step test, has been delineated by the Ninth Circuit Bankruptcy Panel for authentication under Federal Rule 901(b)(9). *See In re* Vinhnee, 336 B.R. 437, 446 (B.A.P. 9th Cir. 2005).

108. MINN. R. EVID. 901(b)(10).

109. *Id.* at committee's cmt. (1977).

110. MINN. STAT. §§ 325K.01–.28 (2008).

111. The defined purposes of the Act are to facilitate commerce by means of reliable electronic messages, minimize the incidence of forged digital signatures and fraud in electronic commerce, implement international standards created to ensure reliability and authenticity of electronic messages, and establish uniform rules with other states in this area. § 325K.02. The Act, however, specifically acknowledges that it does not supersede court rules "governing the use of electronic messages and documents." *Id.* § 325K.27.

F. Self-Authentication Under Rule 902

In addition to the authentication methods illustrated under Rule 901, Rule 902 provides for self-authentication methods that do not need the extrinsic evidence of a witness providing foundational testimony.[112] In other words, Rule 902 simply obviates the need for preliminary authentication by the proponent but does not preclude other evidentiary challenges.[113] Two 902 rules stand out as being potentially applicable to ESI.

> (5) *Official Publications.* Books, pamphlets, or other publications purporting to be issued by public authority.[114]

The identification of "publications" under this rule may apply to the website of a public authority, such as the government.[115] Some courts, however, still find websites, even from public authorities, inherently suspect given the potential for third parties to infiltrate such sites and alter the content.[116] Nonetheless, given the increasing number of government agencies with websites and the posting of official publications on their websites, Rule 902(5) will likely be increasingly offered as a basis for authentication. Elsewhere, courts have found printed government websites to be

112. As a result, any challenge to such evidence is relevant only to the weight, and not admissibility, of the evidence. The admissibility, however, may still be challenged under other exclusionary rules such as Rules 402, 403, 501, 702, 802, or 1002. THOMPSON & HERR, *supra* note 12, at 279.

113. As noted by Minnesota courts, "[s]elf-authenticating, however, does not mean that no authentication is required." State v. Northway, 588 N.W.2d 180, 182 (Minn. Ct. App. 1999).

114. MINN. R. EVID. 902(5).

115. *See, e.g.*, U.S. E.E.O.C. v. E.I. DuPont de Nemours & Co., No. Civ.A. 03-1605, 2004 WL 2347556 (E.D. La. Oct. 18, 2004) (finding webpage printouts from the U.S. Census Bureau website self-authenticating under FED. R. EVID. 902(5)); Sannes v. Jeff Wyler Chevrolet, Inc., 1999 U.S. Dist. LEXIS 21748, at *10 n.3 (S.D. Ohio, Mar. 31, 1999) (holding FTC press releases from FTC website were self-authenticating official publications under FED. R. EVID. 902(5)).

116. *See, e.g.*, St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 744, 775 (S.D. Tex. 1999) (finding information about boat's ownership from U.S. Coast Guard Vessel Database website inadmissible because Internet information was "inherently untrustworthy" due to possibility of hackers); State v. Davis, 10 P.3d 977, 1010 (Wash. 2000) (rejecting state population statistics from official state website because "an unauthenticated printout obtained from the Internet does not . . . qualify as a self-authenticating document" under Washington's counterpart Rule 902(e)). Even Minnesota courts have required some type of additional authenticating testimony from "self-authenticating" documents. *See Northway*, 588 N.W.2d at 182 (price report from U.S. Department of Agriculture was not authenticated absent testimony from an authorized person, seal, certificate, or other indication of genuineness).

self-authenticating if the offering party can show specific identifying information for the website.[117]

> (7) *Trade inscriptions and the like.* Inscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin.

The rule commentary acknowledges that this rule is "based on the unlikelihood of forgery of a trade inscription."[118] As applied to ESI, this rule could provide authentication for an e-mail containing a tag identifying the company-employer and the origin of the e-mail.[119] Many business e-mails include signature blocks, provide such information as the sender's name, company, job title, physical address, telephone number, and e-mail address. Of course, authentication of e-mails under Rule 902(7) are subject to the same problems as authentication of e-mails under Rule 901(b)(4) because the e-mail may have been sent from someone other than the identified sender. In that event, a party may still be required to authenticate the e-mail by a witness with personal knowledge under Rule 901(b)(1).

G. Shortcuts to Authentication of ESI

In searching for the least burdensome, but most reliable, method of authenticating ESI, parties should not forget other methods available to them under the Minnesota Rules of Civil Procedure. Much of the authentication gymnastics for ESI, as well as for any other types of evidence, can be avoided by judicious use of available pretrial and discovery rules.[120] For example, Rule

117. Williams v. Long, 585 F. Supp. 2d 679, 689 (D. Md. 2008) ("A proponent of ESI could use the URL, date, and/or official title on a printed webpage to show that the information was from a public authority's website, and therefore, self-authenticating. Similarly, the public authority's selection of the posted information for publication on its website will act as the necessary 'seal of approval' needed to establish that the information came from a public authority for purposes of [Federal] Rule 902(5).").

118. MINN. R. EVID. 902(7) committee's cmt. (1989).

119. JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 900.07[3][c][i] (Joseph M. McLaughlin ed., Matthew Bender 2d ed. 1997) (noting that an e-mail signature block "alone may be sufficient to authenticate an e-mail under Rule 902(7)"). *See also* Superhighway Consulting, Inc. v. Techwave, Inc., No. 98 CV 5502, 1999 WL 1044870, at *4–5 (N.D. Ill. Nov. 16, 1999) (authenticating e-mail based on signature block, among other factors).

120. Indeed, the writers of the *Manual for Complex Litigation* recommend that "[i]ssues concerning accuracy and reliability of computerized evidence, including any necessary discovery, should be addressed during pretrial proceedings and not raised for the first time at trial." MANUAL FOR COMPLEX LITIGATION, *supra* note 8, §

16.03(c) specifically contemplates obtaining stipulations regarding the authenticity of documents as well as seeking advance rulings on the admissibility of evidence.[121] Alternatively, a party could use requests to admit the authenticity of particular documents, including ESI, under Rule 36.01.[122] Finally, some courts have found that a party who produces ESI during discovery implicitly admits its authenticity by doing so and is thus barred from later objecting to its admission by the opposing party on authentication grounds.[123]

H. Electronic Evidence for Illustrative Purposes

Some "evidence" is not really substantive, but is allowed to be considered by the fact-finder as "illustrative."[124] Illustrative evidence may be allowed, but is subject to the same limitations whether created or stored in an electronic format or in India ink on vellum.[125] It is not substantive evidence in the case—it does not help a party carry a burden of proof and is not considered in reviewing the sufficiency of evidence to support a claim. An illustrative exhibit that is misleading or not fairly produced can be excluded, usually under Rule 403.[126]

The presentation of evidence may be objectionable even if the exhibit itself is otherwise admissible. For example, in a failure-to-diagnose medical malpractice case, the x-rays of the patient would invariably be admissible. But the court might very well exclude magnified portions of those x-ray films.[127] This result would

21.446.

121. MINN. R. CIV. P. 16.03(c).

122. MINN. R. CIV. P. 36.01.

123. *See* Sprinkle v. Lowe's Home Centers, Inc., No. 04-CV-4116-JPG, 2006 WL 2038580, at *2 (S.D. Ill. July 19, 2006); *Superhighway Consulting, Inc.*, 1999 WL 1044870, at *4–5; and Indianapolis Minority Contractors Ass'n, Inc. v. Wiley, No. IP 94-1175-C-T/G, 1998 WL 1988826, at *6 (S.D. Ind. May 13, 1998).

124. *See, e.g.*, Strasser v. Stabeck, 112 Minn. 90, 92, 127 N.W. 384, 385 (1910) (holding that the admissibility of illustrative evidence is "admitted, when properly verified, to illustrate or express the testimony of a competent witness, but [is] not original evidence").

125. Verification and authentication of such evidence may be made by having a knowledgeable witness testify that the exhibit is a substantially correct representation of what that witness independently observed. MINN. R. EVID. 901(b)(1).

126. *See, e.g.*, Racz v. R.T. Merryman Trucking, Inc., No. 92-3404, 1994 WL 124857 (E.D. Pa. Apr. 4, 1994) (excluding computerized accident reconstruction due to a distorted data presentation).

127. *See, e.g.*, Rodd v. Raritan Radiologic Assocs., P.A., 860 A.2d 1003 (N.J.

presumably be reached regardless of whether the x-rays were digital images stored in a computer or traditional films stored in manila sleeves with the patient's chart.

V. HOW WILL MINNESOTA COURTS TREAT ADMISSIBILITY OF ESI?

Given the court's considerable discretion to admit evidence and the variety of authentication methods available under the Minnesota Rules of Evidence, courts have not been inclined to deviate from the existing rules of evidence for authenticating evidence that involves computers or electronic technology.[128] Over eighty years ago, the Minnesota Supreme Court recognized the ability of basic evidentiary rules to evolve and apply to future technologies:

> It may be one of those things with respect to which the common law of evidence should demonstrate its ability to adapt its concepts of admissibility to the current and universal practices of business. The need will remain however to bring forward the best evidence which the case sensibly permits. That done, the writing should be admitted if from the evidence there can be drawn the necessary inference of authorship.[129]

Not only should traditional evidentiary rules apply equally to future technologies, but the discretion and common sense of the court similarly provides a mechanism for dealing with new technologies

Super. Ct. App. Div. 2004) (excluding x-rays that were enlarged 30 to 150 times and projected on a six by eight-foot screen, showing detail not discernable on original x-rays). The result in this case might well have been the opposite if the 150-times enlargement was shown to be the standard medical practice for reading these films.

128. *See, e.g.*, State v. Brown, 739 N.W.2d 716, 723 (Minn. 2007) (authenticating digital photographs). *See also In re* Vinhnee, 336 B.R. 437, 444 (B.A.P. 9th Cir. 2005) ("Authenticating a paperless electronic record, in principle, poses the same issue as for a paper record, the only difference being the format in which the record is maintained . . . ."); MANUAL FOR COMPLEX LITIGATION, *supra* note 8, § 11.446 ("In general, the Federal Rules of Evidence apply to computerized data as they do to other types of evidence."). *Vinhnee* has been viewed as establishing a stricter standard for admission of electronic evidence. *See, e.g.*, Cooper Offenbecher, *Admitting Computer Record Evidence After In re Vinhnee: A Stricter Standard for the Future?*, 4 SHIDLER J. L. COM. & TECH. 6 (2007). However, this stricter standard appears not to have been widely followed. *Id.*

129. Lundgren v. Union Indem. Co., 171 Minn. 122, 125, 213 N.W. 553, 555 (1927).

under "old" rules.[130] In addition, courts should continue to rely on the parties to make challenges to proffered evidence and point out potential pitfalls and inadequacies to authentication of current technologies.[131]

The starting point—and often the end point—of the analysis should often be to ignore the format of the proffered evidence. If it is admissible in a nineteenth-century format, it probably should be admitted in the twenty-first century, at least in the absence of a serious challenge to its authenticity. Because of the potential for electronic records to be manipulated, however, courts should be open to considering good faith challenges to the authenticity of evidence, and hold proponents of questionable evidence to their burdens of establishing admissibility.

130. *See* Johnson v. Burmeister, 182 Minn. 385, 387, 234 N.W. 590, 591 (1931) ("The discretion of the trial judge as to how much and what foundation to require for the introduction of documentary evidence is not so limited as to prevent his exercise of common sense.").

131. *See* State v. Hagar, 325 N.W.2d 43, 44–45 (Minn.1982) ("If, upon consideration of the evidence as a whole, the court determines that the evidence is sufficient to support a finding by a reasonable juror that the matter in question is what its proponent claims, the evidence will be admitted. The party against whom the evidence has been received may . . . offer contradictory evidence . . . or challenge the credibility of the supporting proof . . . . The trier of fact renders the ultimate decision as to whether the item of real evidence . . . is as it is purported to be.").