Chapter 5

NON-TECHNICAL MANIPULATION OF DIGITAL DATA

Legal, Ethical and Social Issues

Michael Losavio

Abstract This paper investigates basic issues related to the use of digital evidence in courts. In particular, it analyzes the basic legal test of authenticity of evidence with respect to an e-mail tool that can be used to manipulate evidence. The paper also examines the experiences and perceptions of U.S. state judicial officers regarding digital evidence, and reviews case law on how such evidence might be tested in the courts. Finally, it considers ethical and social issues raised by digital evidence and the mitigation of problems related to digital evidence.

Keywords: Digital evidence, e-mail evidence, authenticity

1. Introduction

Digital forensics bridges the science of computing and the judicial process. Both disciplines seek the truth, but their methods are distinct and their ends different. Every aspect of digital evidence, even the seemingly trivial, is tested during the judicial process. For example, issues related to the authenticity and integrity of e-mail messages are addressed during the administration of justice. Addressing these issues involves varying contributions by digital forensics with varying results.

This paper examines basic issues related to the use of digital evidence in courts and how digital forensics links computing to the judicial process. The growing use of digital evidence in judicial proceedings is discussed, focusing on the use of e-mail evidence in U.S. District Courts. The mutability and evanescence of electronic data raises issues concerning its authenticity that may lead courts to question its reliability as

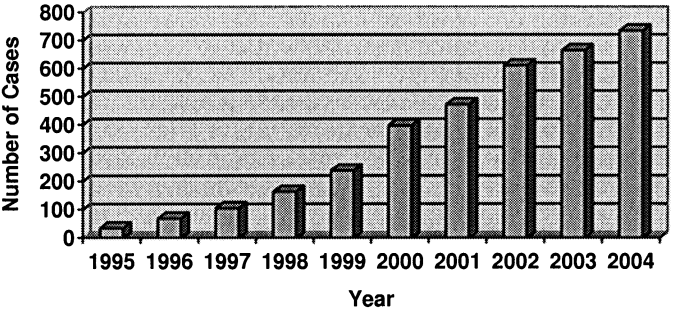

Figure 1. U.S. District Court cases referencing e-mail.

evidence. This issue of authenticity is investigated with respect to an e-mail tool that can be used to manipulate evidence.

The paper also examines the experiences and perceptions of U.S. state judicial officers regarding digital evidence, and reviews case law on how such evidence might be tested in the courts. Finally, it considers ethical and social issues raised by digital evidence and the mitigation of potential problems related to digital evidence.

2. Digital Evidence

Society's dependence on computers and networks assures the presentation of digital evidence in courts [11]. Electronic mail has become the very fabric of commercial litigation [20]. It creates a wealth of possible evidence and a growing "cottage industry" to assist litigators in discovering such evidence, with the legal commentary to explain it.

A keyword analysis of trial-level U.S. District Court opinions referencing e-mail shows a significant increasing trend over a ten-year period (Figure 1). The bulk of all cases in the United States, including most criminal cases and all domestic relations cases, are resolved by state courts whose opinions are not reported in legal databases. Nevertheless, anecdotal information suggests that the increasing trend in the use of e-mail evidence is common throughout the judicial system.

3. Relevance and Authenticity

Relevance and authenticity are two significant considerations that judicial officers must take into consideration before deciding whether or not to admit any evidence into court. Relevance is the truth or falsehood of a fact or issue in question; a test of relevance must not involve any undue prejudice against the opposing party. Authenticity, in its legal sense, means that something is what it is claimed to be. One of the

Table 1. Case data from a U.S. state court system.

Year	2001	2002	2003	2004
General jurisdiction cases terminated (by fiscal year (July 1–June 30))	115,800	117,900	129,600	138,500
Reported appellate opinions involving digital evidence (by calendar year)	2	3	3	3
Subset of reported appellate opinions involving challenges to admissibility	0	0	0	0

measures of authenticity is how evidence is demonstrated to be reliable. The legal testing of the authenticity of digital evidence has received less attention than techniques for digital forensic investigation and discovery [20]. In 2004, of about 163 reported U.S. federal appellate cases referencing e-mail, none addressed authenticity issues. Furthermore, of about 760 federal trial cases referencing e-mail, only four involved issues of authenticity of e-mail messages.

The ability to fabricate digital data makes authenticity a vital issue, even where some courts assert that digital mutability alone does not impact reliability [16, 25]. But this situation may change if authenticity challenges begin to exclude digital evidence from court proceedings. Robins [20] questions whether the computerized nature of digital evidence makes fabrication and/or errors more likely and, therefore, less reliable for decision-making.

Table 1 presents case closure statistics for trial courts, published appellate opinions involving digital evidence, and the admissibility of digital evidence for one U.S. state court system. Interestingly, from among more than 100,000 trial-level cases during each 12-month period, there were no more than three reported appeals in each period mentioning digital evidence, and not one case addressed admissibility or reliability. This may explain why there is so little case law guidance for individuals working in the discipline of digital forensics.

3.1 Legal Tests for Authenticity

In U.S. courts of law, the Rules of Evidence seek to assure the integrity and authenticity of evidence as a precondition for admissibility, to the end that the truth may be ascertained and proceedings justly determined [21, 24, 27, 28, 31, 32, 34–36]. In particular, *Federal Rule of Evidence*

901: Requirement of Authentication and Identification [34] and its state progeny provide as to any evidence, digital or otherwise:

> The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

This flexible rule permits authentication by direct testimony or analysis of contents, internal patterns or other distinctive characteristics. Digital evidence gets special treatment in this rule. In particular, the rule states that where "data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original." Thus, a printout or other output of digital data may be used as the evidence [31]. Testimony pertaining to such a duplicate or copy of digital evidence is considered to be as reliable as the original (or "best evidence"). Evidence rules pertaining to hearsay also address reliability. In particular, out-of-court statements of third parties are not admissible absent showing such second-hand evidence is authentic and reliable, and need not withstand direct testing via cross-examination.

Robins [20] and Givens [11] suggest that these evidentiary rules might be liberally construed in a way that admits digital evidence with less rigor than non digital evidence. Givens [11] notes that some courts give greater credence to digital evidence because a computer is deemed less subject to error and manipulation than a human agent. However, several non-technical tools are available for manipulating digital information such as e-mail messages. As discussed below, these tools significantly increase the potential that digital evidence may be fabricated.

3.2 Fabrication of E-Mail Messages

A popular e-mail program was used to investigate the ease with which digital evidence could be fabricated. Although the fabrication may be obvious to experts, it may not be obvious to many individuals in the judicial system, including jurors, counsel and judges.

A digital forensics expert who reports on the fabrication or authenticity of digital evidence must be prepared to address what may be "obvious" to him/her in a clear, credible and non-condescending manner. Clarity and credibility may depend on truthful testimony that the expert has tested the "obvious" and has made hard findings. Speculation – even if it is scientifically grounded – may not be enough. The expert's answer to the question: *Have you ever tested this?* may be important to a judge or jury in accepting the expert's conclusions. In any case, testing is good scientific method.

Three tests were conducted using a popular e-mail program. The tests were used to create digital evidence, including potentially admissible printouts of e-mail messages.

Fabrication Test 1

The first test simply edits an existing e-mail message and prints out the edited version.

1 An existing e-mail message is opened using an e-mail program.

2 The e-mail message is edited by adding or deleting text.

3 The e-mail message is printed.

Examination of the printout of the fabricated e-mail message reveals that the edited version is indistinguishable on its face from the original.

Fabrication Test 2

Assuming a challenge to the paper "original," the e-mail program is used to fabricate the electronic copy of the e-mail message itself. In other words, the "best evidence" of the e-mail message is modified.

1 An existing e-mail message is opened using an e-mail program.

2 The e-mail message is edited by adding or deleting text.

3 The edited e-mail message is saved.

4 The e-mail program is closed.

5 The edited e-mail message is re-opened using the e-mail program, showing the edited text as part of the e-mail message.

The forged e-mail message is saved in digital form as the document itself. The content of the document cannot be demonstrated to be unreliable.

Fabrication Test 3

The `Properties` option in the e-mail program permits the review of the time an e-mail message was sent, received and last modified. This timestamp information may indicate tampering, raising questions about the authenticity and integrity of the "best evidence."

1 The system date and time are reset.

2 An existing e-mail message is opened using an e-mail program.

3 The e-mail message is edited by adding or deleting text.

4 The edited e-mail message is saved.

5 The e-mail program is closed.

6 The edited e-mail message is re-opened using the e-mail program, showing the edited text as part of the e-mail message.

7 The `Properties` option is executed, showing the reset date and time in the e-mail message timestamp.

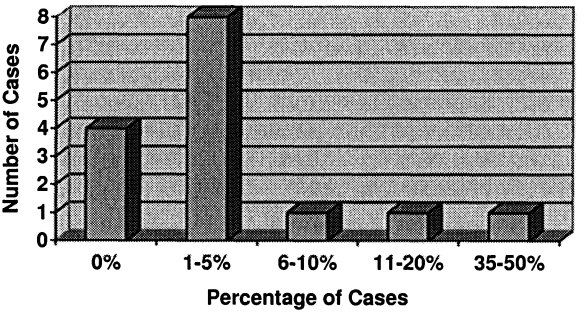

Figure 2. Caseloads of individual officers involving digital evidence.

Digital forensic analysis may be able to detect the modifications made to the e-mail message and the system date and time, but there are some hurdles. Can the costs of such analysis can be afforded by the parties? Is there sufficient skill or sufficient opportunity to use such analysis in every case? The judicial process will render judgment based on the evidence it is provided. How it does so depends, among other things, on judicial perceptions and experience with digital evidence.

4. Judicial Perceptions and Experience

A sample of state judicial officers were surveyed about their perceptions and experience with digital evidence and its reliability. These officers handle divorce, custody and maintenance actions. An examination of trial and appellate results from their jurisdictions indicates that there were more than 26,000 and 34,000 trial cases in 2001 and 2004, respectively [14]. No appellate opinions mentioned digital evidence [14].

4.1 Survey of State Judicial Officers

The survey results indicate that the majority of respondents had digital evidence in cases before them (Figure 2). In all, 75% of the respondents indicated that they had encountered digital evidence in proceedings. (Note that 52% of the individuals who were solicited responded to the survey.) Digital evidence appeared very frequently in cases before one respondent, but for others it was much less so. The frequency distribution suggests future growth in the use of digital evidence.

As shown in Figure 3, e-mail was the most common type of digital evidence in cases before 48% of the surveyed individuals (68% of the respondents), followed by web browsing items (30%/44%) and digital photos (26%/37%). The prevalence of e-mail evidence in domestic relations cases parallels Robins' observation for commercial litigation [20].

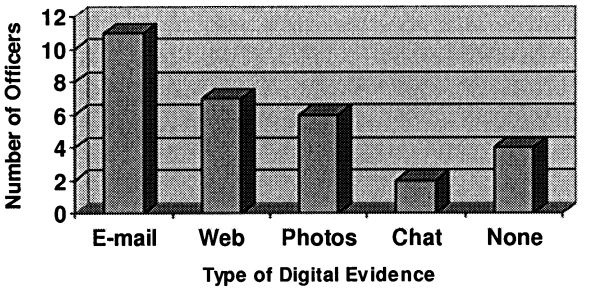

Figure 3. Judicial officers with cases involving digital evidence.

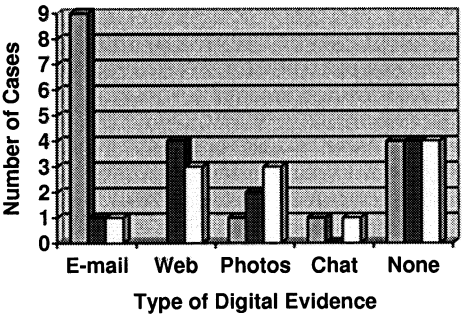

Figure 4. Frequency of various types of digital evidence.

Figure 4 shows that e-mail had the highest frequency of use among all types of digital evidence. 48% of the individuals (68% of respondents) had encountered e-mail evidence (68% of respondents). For 39% (56% of respondents), e-mail was the most frequently used digital evidence.

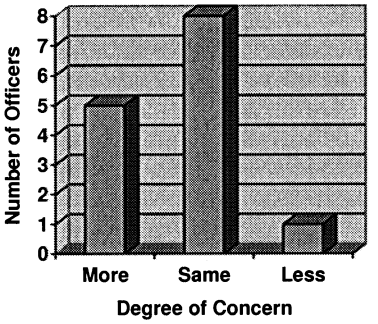

Figure 5. Comparison of concerns about evidence falsification.

The survey results also indicate that the majority of judicial officers had the same concerns about the falsification of digital evidence as non digital evidence. However, as shown in Figure 5, 22% (36% of

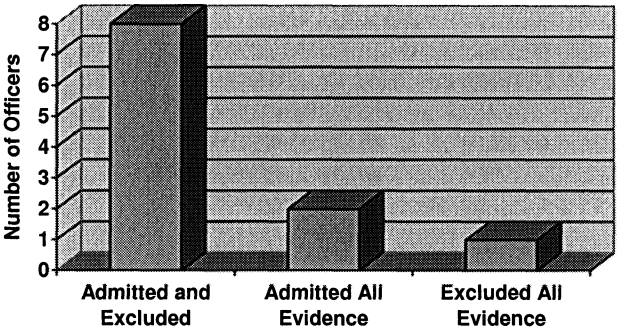

Figure 6. Judicial officers admitting and excluding digital evidence.

respondents) were more concerned about the possible falsification of digital evidence than non digital evidence. This also shows a difference in perception among some judicial officers about the reliability of digital evidence as opposed to traditional evidence.

4.2 Reliability Concerns

The survey results also indicate that the majority of judicial officers who were faced with digital evidence in cases had both admitted and excluded the evidence (Figure 6). They applied the state's rules of evidence, modeled on the U.S. Federal Rules, that test for relevance, undue prejudice, hearsay and authenticity in deciding whether to admit or exclude evidence [29, 30, 33, 34].

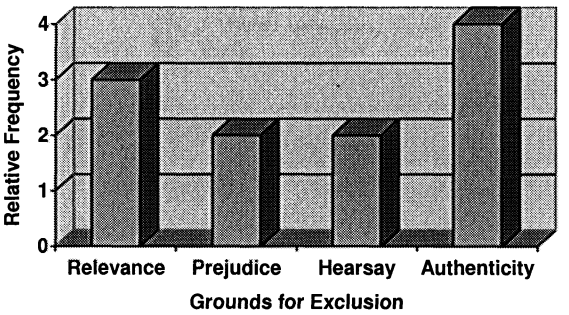

Figure 7. Grounds for excluding digital evidence.

Figure 7 shows that the lack of authenticity was the most frequent reason for excluding digital evidence. Hearsay, another reliability filter, was also noted as a ground for exclusion. Relevance and undue prejudice were also grounds for excluding evidence, but decisions regarding them are often made prior to determining authenticity. As a result, evidence

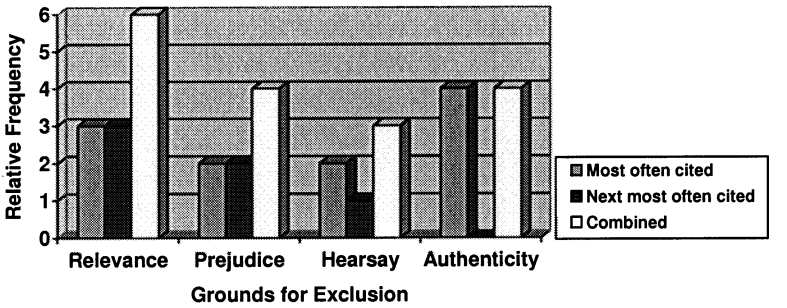

Figure 8. Most common grounds for excluding evidence.

excluded for reasons of hearsay or prejudice are usually not tested for authenticity.

Figure 8 shows the relative frequencies of the most often cited and the next most often cited grounds for excluding digital evidence. Combining the values for the most often and next most often grounds for exclusion show that relevance and undue prejudice play significant roles in excluding digital evidence in domestic relations proceedings. Some of these cases may have benefited from digital forensic analysis, but others did not.

The default response, absent digital forensic analysis, is that traditional factors are used to decide authenticity, such as credibility and circumstantial evidence. Thus the author of an e-mail message can be authenticated by distinctive characteristics and the circumstances surrounding the e-mail message as well as by circumstantial evidence of the author's style and personal information he/she would have known [17, 23, 27].

Does the easy fabrication of e-mail evidence, coupled with the lack of digital forensic expertise and the use of non-technical, circumstantial evidence, by default, raise questions about the fairness and reliability of digital evidence? Should a domestic violence case involving e-mail threats be dismissed due to the technical superiority of one party over another, e.g., Rabic v. Constantino [8]? Does this raise ethical and social issues that must be addressed by the digital forensics discipline?

5. Ethical and Social Concerns

The easy fabrication of digital evidence and the existence of a "digital divide" (between those who can afford digital forensic services and those who cannot go) beyond the courts. Unless these issues are addressed, the confidence of any process that relies on digital evidence can be undermined. Natsui [18] notes several due process (basic fairness)

issues concerning information security and electronic personal information (both of which involve digital forensics). Furthermore, while OECD Guidelines hold that information security should be compatible with the fundamental values of a democratic society, they do not explicitly recognize any due process rights [18, 19]. For attorneys, their obligations relating to competence and integrity in working with opposing parties place a professional onus on them to assure that digital evidence is used properly [2–6]. Lack of knowledge may not be a valid defense to ethical and other sanctions in cases where an attorney, exercising diligence in investigating the merits of the case, discovers falsified evidence, e.g., Jimenez v. Madison Area Technical College [22, 26].

The obligations are more diffuse for experts in digital forensics. Expert witnesses in litigation are generally protected under the witness immunity doctrine so long as they do not perjure themselves. However, this immunity is under scrutiny and the possibility exists that expert witnesses could be held to some standards for liability [12, 13]. Such standards might be applied to digital forensic experts as their work moves from laboratory to courtroom, but they will probably be applied first to experts in licensed, regulated professions, e.g., medical practice. To the extent that digital forensics falls with the computing discipline, it does not yet have fully realized practices and procedures requiring responsible engineering and science even though its professional societies (ACM and IEEE) aspire to such [1, 10, 13]. Indeed, Linderman [15] contends that, unlike medical practice, information technology is not a "profession" with attendant, articulated obligations. On the other hand, Denning [9] argues that guidance is needed in the information technology discipline as public trust and confidence, once lost, may take years to rebuild. Without guidance as to what should and should not be done in digital forensics, there is a risk that missteps might be taken that would affect public confidence in the discipline. Clearly, the digital forensics discipline must take greater responsibility for the veracity of digital information. While this is not a perfect solution, it is critical to probative processes in the digital age.

6. Conclusions

The use of digital evidence is growing in American courts. Meanwhile, non-technical tools are becoming available that make it very easy to fabricate digital evidence. At present there is little case law guidance regarding the reliability of digital evidence in court, and some trial judges are concerned that digital evidence offers greater opportunities for falsification than traditional evidence. The discipline of digital forensics

does not currently offer a complete response to those concerns. Judges and lawyers may not be fully versed in the use of digital evidence. Parties may not be able to afford digital forensic expertise, or one party may be able to "outgun" another with experts. And there is still the issue of certification of digital forensics experts, or some other way to validate the competence of purported experts in what is growing area of analysis. Digital forensics must address technology as well as perceptions of reliability and fairness to bridge the gap between computing and judicial processes. Failure to address these matters will hurt the truth-finding enterprise.

Aristotle [7] noted the differences in how the scientific and political disciplines pursue truth, and he advised not to expect more than is possible. The critical tasks are to reduce uncertainty, both intended and unintended, and to promote fairness and truth-finding processes with regard to digital information in every forum.

References

[1] ACM, ACM Code of Ethics and Professional Conduct (www.acm.org/constitution/code.html), October 16, 1992.

[2] American Bar Association, Model Rule 1.1: Competence (www.abanet.org/cpr/mrpc/mrpc_toc.html).

[3] American Bar Association, Model Rule 3.1: Meritorious Claims and Contentions (www.abanet.org/cpr/mrpc/mrpc_toc.html).

[4] American Bar Association, Model Rule 3.3: Candor toward the Tribunal (www.abanet.org/cpr/mrpc/mrpc_toc.html).

[5] American Bar Association, Model Rule 3.4: Fairness to Opposing Party and Counsel (www.abanet.org/cpr/mrpc/mrpc_toc.html).

[6] American Bar Association, Model Rule 3.8: Special Responsibilities of a Prosecutor (www.abanet.org/cpr/mrpc/mrpc_toc.html).

[7] Aristotle, *Nicomachean Ethics*, W. Ross (Translator), Oxford University Press, New York, 1998.

[8] California Court of Appeals (First District, Division Four), Rabic v. Constantino, Case No. A106248, 2004.

[9] P. Denning, Who are we? *Communications of the ACM*, vol. 44(2), pp. 15-19, 2001.

[10] P. Denning, Crossing the chasm, *Communications of the ACM*, vol. 44(4), pp. 21-25, 2001.

[11] J. Givens, Comment: The admissibility of electronic evidence at trial: Courtroom admissibility standards, *Cumberland Law Review*, vol. 34, pp. 95-126, 2003.

[12] J. Harrison, Reconceptualizing the expert witness: Social costs, current controls and proposed responses, *Yale Journal on Regulation*, vol. 18(2), pp. 253-314, 2001.

[13] IEEE, IEEE Code of Ethics (onlineethics.org/codes/IEEEcode.html).

[14] Kentucky Court of Justice, FY 2004 Historical Reports: Circuit Court Data and Circuit Family Data, Domestic and Family Case Closures (www.kycourts.net/AOC/CSRS/ResearchStats.shtm).

[15] J. Linderman and W. Schiano, Information ethics in a responsibility vacuum, *The DATA BASE for Advances in Information Systems*, vol. 32(1), pp 70-74, 2001.

[16] M. Losavio, The secret life of electronic documents, *Kentucky Bench & Bar*, vol. 63(5), pp. 31-34, 1999.

[17] Maine Supreme Court, State v. Turner, 2001 ME 44 (www.courts.state.me.us/opinions/documents/01me44tu.htm), 2001.

[18] T. Natsui, Procedural justice: Changes in social structures in an information society and the maintenance of justice, presented at the *International Conference on the Internet and the Law - A Global Conversation*, 2004.

[19] Organisation for Economic Cooperation and Development, Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (www.oecd.org/dataoecd/16/22/15582260.pdf).

[20] M. Robins, Evidence at the electronic frontier: Introducing e-mail at trial in commercial litigation, *Rutgers Computer & Technology Law Journal* vol. 29, pp. 219-315, 2003.

[21] W. Stallings, *Network Security Essentials (2nd Edition)*, Prentice-Hall, Upper Saddle River, New Jersey, 2003.

[22] U.S. Circuit Court of Appeals (7th Circuit), Jimenez v. Madison Area Technical College, 321 F.3d 652, 2003.

[23] U.S. Circuit Court of Appeals (11th Circuit), United States v. Siddiqui, 235 F.3d 1318, 2000.

[24] U.S. Department of Justice, Part V: Evidence, *Manual for Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, Computer Crime and Intellectual Property Section, Criminal Division, Washington, D.C., 2002.

[25] U.S. District Court (Illinois Northern District, Eastern Division), Tibbetts v. RadioShack Corporation, Case No. 03 C 2249, 2004.

[26] U.S. Government, *Federal Rules of Civil Procedure*, U.S. Government Printing Office, Washington, D.C., 2004.

[27] U.S. Government, Rule 101 (Scope), *Federal Rules of Evidence*, U.S. Government Printing Office, Washington, D.C., p. 1, 2004.

[28] U.S. Government, Rule 102 (Construction and purpose), *Federal Rules of Evidence*, U.S. Government Printing Office, Washington, D.C., p. 1, 2004.

[29] U.S. Government, Rule 402 (Relevant evidence generally admissible; irrelevant evidence inadmissible), *Federal Rules of Evidence*, U.S. Government Printing Office, Washington, D.C., p. 3, 2004.

[30] U.S. Government, Rule 403 (Exclusion of relevant evidence on grounds of prejudice, confusion or waste of time), *Federal Rules of Evidence*, U.S. Government Printing Office, Washington, D.C., p. 3, 2004.

[31] U.S. Government, Rule 702 (Testimony by experts), *Federal Rules of Evidence*, U.S. Government Printing Office, Washington, D.C., p. 13, 2004.

[32] U.S. Government, Article VII: Rules 801-807 (Hearsay), *Federal Rules of Evidence*, U.S. Government Printing Office, Washington, D.C., pp. 15-20, 2004.

[33] U.S. Government, Rule 802 (Hearsay rule), *Federal Rules of Evidence*, U.S. Government Printing Office, Washington, D.C., p. 15, 2004.

[34] U.S. Government, Rule 901 (Requirement of authentication or identification), *Federal Rules of Evidence*, U.S. Government Printing Office, Washington, D.C., pp. 20-21, 2004.

[35] U.S. Government, Rule 1001 (Definitions), *Federal Rules of Evidence*, U.S. Government Printing Office, Washington, D.C., pp. 23-24, 2004.

[36] U.S. Government, Article X: Rules 1001-1007 (Contents of writings, recordings and photographs), *Federal Rules of Evidence*, U.S. Government Printing Office, Washington, D.C., pp. 23-24, 2004.