A RECONSIDERATION OF THE ADMISSIBILITY OF COMPUTER-GENERATED EVIDENCE

I. INTRODUCTION

Since the beginning of their use at the end of World War II, electronic digital computers have fostered a virtual second industrial revolution in American society. They have been used for a multitude of purposes, the most significant of which is information processing and retrieval. Nearly every aspect of society has been affected by computer-assisted technological changes. Yet the impact of computer science has just begun to be felt and is expected to increase drastically in the future.

The widespread use of computers poses complex problems for the legal system. With government and business relying heavily on computers for data processing and recordkeeping, the courts face

---

1 There are two general types of computers: analog and digital. The analog computer operates by measuring continuously changing values such as temperature. The digital computer, on the other hand, operates by counting discrete quantities. The digital models comprise the vast majority of computers used for electronic data processing and other purposes. See Roberts, A Practitioner's Primer on Computer-Generated Evidence, 41 U. Chi. L. Rev. 254 n.1 (1974); Freed, Computer Print-Outs As Evidence, 16 Am. Jur. Proof of Facts Ann. 273, 276 (1965).


4 See generally, 195 Science 1087-1240 (1977) (entire issue devoted to electronics and computers).

5 For a brief set of predictions regarding the anticipated effect of computers on American society, see A. Vazsonyi, supra note 3, at 358-63. For statistics illustrating the enormous increase in the number and computing power of computers during the last 30 years, see Davis, Evolution of Computers and Computing, 195 Science 1096, 1099 (1977).

an increasing number of requests to admit into evidence computer-generated materials in the form of printouts, visual media, or testimonial evidence culled from nonvisual computer files.

This Comment examines the issues surrounding the admissibility of routinely prepared computerized records in civil and criminal litigation. Since this evidence is usually offered to prove the truth of the statements contained therein and involves the contents of written material, this discussion focuses on the hearsay and best evidence rules and their respective exceptions. The contemporary judicial approaches to traditionally and electronically maintained records under the hearsay and best evidence rules are outlined, and then the degree to which courts should alter their treatment of computer-generated evidence because of the various errors accompanying modern electronic data processing (EDP) is explored. Finally, it is suggested that judges should require proponents of computer-generated evidence to demonstrate its reliability with greater certainty than is presently required in most jurisdictions.

II. TRADITIONALLY MAINTAINED RECORDS AND THE RULES OF EVIDENCE

A. The Hearsay Rule and Relevant Exceptions

The common law proscribes the use in court of hearsay,\(^7\) which is defined as written evidence or testimony of out-of-court statements offered to prove the truth of the matters asserted therein.\(^8\) Underlying this rule is the belief that the factfinding process is enhanced by requiring that the declarant, the individual making the out-of-court statement, present his evidence in court, under oath, and subject to cross-examination so that the jury may observe his demeanor and evaluate his credibility.\(^9\)

There are a number of exceptions to the hearsay rule.\(^10\) Two of them, the business records exception and public record exception, are particularly relevant to the problems of computer evidence. Underlying these, as well as all hearsay exceptions, is the premise

\(^7\) McCormick, Evidence § 246 (2d ed. 1972).

\(^8\) Id. §§ 244-248.


\(^10\) For a description of the various exceptions to the hearsay rule and their historical development, see McCormick, supra note 7, §§ 253-327.
that "under appropriate circumstances a hearsay statement may possess circumstantial guarantees of trustworthiness sufficient to justify nonproduction of the declarant in person at the trial even though he may be available."  

1. The Business Records Exception

Beginning with the "shop book" rule of the seventeenth century, the common law permitted, as an exception to the hearsay rule, the introduction of regularly maintained business records as evidence of the truth of the matters contained therein. Due to the rigid requirements courts imposed on the shop book rule, this exception eventually proved to be inadequate in light of the increasingly complex nature of business recordkeeping. As a result, several statutory modifications of the shop book rule have been proposed during the past fifty years. They include: the Commonwealth Fund Act, the Uniform Business Records as Evidence Act, rules 63(13) & (14) of the 1953 Uniform Rules of Evidence, rules 803(6) & (7) of the recently adopted Federal Rules of Evidence.

---

12 McCormick, supra note 7, §§ 305-306.
13 Id.
15 The text of the Uniform Business Records as Evidence Act, proposed by the National Conference of Commissioners on Uniform State Laws (NCCUSL) in 1936, may be found in 9A U.N.F. L. Ann. 506 (1965), and in McCormick, supra note 7, § 316 n.12. This statute is the most widely adopted of all the business records acts. See Advisory Committee Notes to Federal Rules of Evidence, Rule 803(6), 56 F.R.D. 183, 307 (1972). For a table of states that have enacted the Uniform Business Records as Evidence Act as of 1965, see 9A U.N.F. L. Ann. 506 (1965).
dence, and rules 803 (6) & (7) of the 1974 revision of the Uniform Rules of Evidence. Each of the above modifications rely on the regularity of the record's preparation near the time of the re-


Rule 803. Hearsay Exceptions; Availability of Declarant Immaterial

The following are not excluded by the hearsay rule, even though the declarant is available as a witness:

(6) Records of regularly conducted activity.—A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

(7) Absence of entry in records kept in accordance with the provisions of paragraph (6).—Evidence that a matter is not included in the memoranda reports, records, or data compilations, in any form, kept in accordance with the provisions of paragraph (6), to prove the nonoccurrence or nonexistence of the matter, if the matter was of a kind of which a memorandum, report, record, or data compilation was regularly made and preserved, unless the sources of information or other circumstances indicate lack of trustworthiness.

(8) Public records and reports.—Records, reports, statements, or data compilations, in any form, of public offices or agencies, setting forth (A) the activities of the office or agency, or (B) matters observed pursuant to duty imposed by law as to which matters there was a duty to report, excluding, however, in criminal cases matters observed by police officers and other law enforcement personnel, or (C) in civil actions and proceedings and against the Government in criminal cases, factual findings resulting from an investigation made pursuant to authority granted by law, unless the sources of information or other circumstances indicate lack of trustworthiness.

(9) Records of vital statistics.—Records or data compilations, in any form, of births, fetal deaths, deaths, or marriages, if the report thereof was made to a public office pursuant to requirements of law.

(10) Absence of public record or entry.—To prove the absence of a record, report, statement, or data compilation, in any form, or the nonoccurrence or nonexistence of a matter of which a record, report, statement, or data compilation, in any form, was regularly made and preserved by a public office or agency, evidence in the form of a certification in accordance with rule 902, or testimony, that diligent search failed to disclose the record, report, statement, or data compilation, or entry.

corded event, the informant's duty to accurately report his knowledge of the transaction, and the systematic reliance upon such records by the business community to assure the trustworthiness of the proffered evidence. Once the testimony of the custodian or other suitable witness establishes these circumstances, the court may allow the business records to be introduced.

The courts are divided on whether to admit evidence of the absence of an entry in order to prove that a disputed transaction did not take place. Rule 803(7) of the Federal Rules of Evidence specifically provides that the absence of an entry in a business record maintained in accordance with the provisions of rule 803(6) is admissible to prove "the nonoccurrence or nonexistence of the matter, . . . unless the source of information or other circumstances indicate lack of trustworthiness." 21

2. The Official Records Exception

A common law exception to the hearsay rule exists for the written statements of public officials acting under an official duty to accurately report the recorded events. 22 Rule 803(8) of the Federal Rules of Evidence provides for the admission of reports of "matters observed pursuant to [a] duty imposed by law as to which matters there was a duty to report, . . . unless the sources of information or other circumstances indicate lack of trustworthiness." 23 Similarly, rule 803(10), the public records analogue to rule 803(7), allows the admission of a properly certified statement that a diligent search has failed to disclose the existence of a par-


22 McCormick, supra note 7, § 315; Maguire, supra note 14, at 693-94.

23 See also Fed. R. Evid. 803(9), supra note 17 (providing for the admission of vital records such as birth or death certificates under a similar official duty exception). The text of Uniform Rules of Evidence rules 803(8) & (9) may be found at 13 Unif. L. Ann. 242 (1975). See also 28 U.S.C. § 1733 (1964) (providing that originals or certified copies of United States government agency official records are admissible to prove the acts or events cited therein); Uniform R. Evid. 63(15) & (16), 9A Unif. L. Ann. 637-38 (1965); Uniform Vital Statistics Act §§ 16 & 17, 9C Unif. L. Ann. 360-61 (1957).
ticular entry to prove the "nonoccurrence or nonexistence" of the matter. 24

3. The Hearsay Rule and the Constitutional Right of Confrontation

The sixth amendment to the United States Constitution states that "In all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him." The purpose of the confrontation clause, like that of the hearsay rule, is to enable the trier of fact to observe the witness' demeanor and evaluate his credibility. 25 Although the exact outline of the constitutional limitation upon the use of hearsay evidence is unclear, 26 the hearsay rule and the confrontation clause do not completely overlap. 27 For present purposes it suffices to say that traditionally maintained business records and routine public records are admissible in criminal proceedings as they do not run afoul of the confrontation clause. 28

B. The Best Evidence Rule and Relevant Exceptions

The best evidence rule, codified as rules 1001 to 1004 of the Federal Rules of Evidence, provides that if the contents of a writing are in issue, an original copy must be produced unless a sufficient justification for its absence is presented. 29 The emphasis on

24 FED. R. EVD. 803(10), supra note 17. See also UNIFORM RULES OF EVIDENCE 803(10), 13 UNIF. L. ANN. 242-43 (1975); UNIFORM RULES OF EVIDENCE 63(17), 9A UNIF. L. ANN. 638 (1965).


26 MCCORMICK, supra note 7, § 252.


29 FED. R. EVD. 1001-1004 provides, in pertinent part:

ARTICLE X. CONTENTS OF WRITINGS, RECORDINGS, AND PHOTOGRAPHS

RULE 1001. DEFINITIONS

For purposes of this article the following definitions are applicable:

(1) Writings and recordings.—"Writings" and "recordings" consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation.

(3) Original.—An "original" of a writing or recording is the writing or recording itself or any counterpart intended to have the
the original writing is intended to prevent fraud and to aid in interpretation where the words used are terms of art.\textsuperscript{30} Of the several common law and statutory exceptions to the rule,\textsuperscript{31} the official records and voluminous writings exceptions are most relevant here.

The official records exception, codified as rule 1005 of the Federal Rules of Evidence, allows the contents of an official record to be proved through the admission of a certified copy of the record.\textsuperscript{32}

\begin{quote}
same effect by a person executing or issuing it. . . . If 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".

(4) \textit{Duplicate}.—A "duplicate" is a counterpart produced by the same impression as the original, or from the same matrix . . . or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original.

\textbf{Rule 1002. Requirement of Original}

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 Act of Congress.

\textbf{Rule 1003. Admissibility of Duplicates}

A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original.

\textbf{Rule 1004. Admissibility of Other Evidence of Contents}

The original is not required, and other evidence of the contents of a writing, recording, or photograph is admissible if—

(1) \textit{Originals lost or destroyed}.—All originals are lost or have been destroyed, unless the proponent lost or destroyed them in bad faith; or

(2) \textit{Original not obtainable}.—No original can be obtained by any available judicial process or procedure; or

(3) \textit{Original in possession of opponent}.—At a time when an original was under the control of the party against whom offered, he was put on notice, by the pleadings or otherwise, that the contents would be a subject of proof at the hearing, and he does not produce the original at the hearing; or

(4) \textit{Collateral matters}.—The writing, recording, or photograph is not closely related to a controlling issue.

See also Uniform Rules of Evidence, 1001-1004, 13 Unif. L. Ann. 253-54 (1975). For the historical foundations of the best evidence rule see generally, McCor\textsc{m}ick, \textsc{supra} note 7, §§ 230-231.


\textsuperscript{31} See Mc\textsc{c}orra\textsc{m}ick, \textsc{supra} note 7, §§ 237-243.

\textsuperscript{32} Fed. R. Evid. 1005 provides as follows:

\textbf{Rule 1005. Public Records}

The contents of an official record, or of a document authorized to be recorded or filed and actually recorded or filed, including data compilations of any form, if otherwise admissible, may be proved by copy, certified as correct in accordance with rule 902 or testified to be correct by a witness who has compared it with the original. If a copy which complies with
This provision lessens inconvenience to the public and diminishes the risk of losing government records.\textsuperscript{33}

"Forced upon the courts by sheer necessity,"\textsuperscript{34} the voluminous writings exception admits summaries of voluminous documents as long as they are individually admissible and the opposing party has had an opportunity to inspect them and the proposed exhibits. This exception is incorporated into the Federal Rules of Evidence as rule 1006.\textsuperscript{35}

III. COMPUTER-GENERATED EVIDENCE AND EXISTING LAW

A. The Statutory Framework

Only a limited number of jurisdictions have altered their rules of evidence to reflect changes in computer technology. Although the Federal Rules of Evidence expressly provide for the admissibility of all computerized records, only a few states have done likewise.\textsuperscript{36}

The Federal Rules of Evidence permit the use of computer output to the same extent as conventionally prepared records. Rules 803(6)-(10) state that the business and public record exceptions to the hearsay rule apply to "data compilation[s], in any form."\textsuperscript{37} The Advisory Committee Notes to rule 803(6) explain that this term "includes, but is by no means limited to, electronic computer storage."\textsuperscript{38} Moreover, in clarifying the scope of the best evidence rule, the Federal Rules of Evidence defines the terms "writings", "recordings", and "originals" as follows:

\begin{quote}
the foregoing cannot be obtained by the exercise of reasonable diligence, then other evidence of the contents may be given.
\end{quote}


\textsuperscript{33} See McCormick, supra note 7, § 240.

\textsuperscript{34} Maguire, supra note 14, at 213.

\textsuperscript{35} Fed. R. Evid. 1006 provides as follows:

\begin{quote}
The contents of voluminous writings, recordings, or photographs which cannot conveniently be examined in court may be presented in the form of a chart, summary, or calculation. The originals, or duplicates, shall be made available for examination or copying, or both, by other parties at reasonable time and place. The court may order that they be produced in court.
\end{quote}


\textsuperscript{36} See notes 41-44 infra.

\textsuperscript{37} Fed. R. Evid. 803(6)-(10).

\textsuperscript{38} 56 F.R.D. 183, 311 (1972).
"Writings" and "recordings" consist of letters, words or numbers, or their equivalent set down by . . . magnetic impulse, mechanical or electronic recording, or other form of data compilation. . . . An "original" of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. . . . If data are stored in a computer or similar device, any printout readable by sight, shown to reflect the data accurately, is an "original." 39

These definitions show enough flexibility to permit the admission of existing and new forms of data storage and output media. 40

At least eighteen other jurisdictions have also adopted general evidentiary rules or more limited ones that account for the use of computers. Closely modeled on the Federal Rules of Evidence, the rules of evidence in Arizona, 41 Arkansas, 42 Florida, 43 Maine, 44 Minnesota, 45 Nebraska, 46 New Mexico, 47 and Wisconsin 48 provide for the admission of many types of computerized records. In addition, the New Jersey rules of evidence allow the entry of reasonably permanent, visually readable reproductions of generally accepted data storage methods to the same extent as conventionally prepared writings. 49

39 FED. R. EVID. 1001(1) & (3).
40 For a discussion of new data storage techniques, see Rajchman, New Memory Technologies, 195 SCIENCE 1223 (1977).
48 WIS. STAT. ANN. §§ 908.03(6)-(10), 910.01 (West 1975).
49 The New Jersey provision is as follows:

"Writing" means handwriting, typewriting, printing, photostating, photography and every other means of recording upon any tangible thing any form of communication or representation, including letters, words, pictures, sounds or symbols, or combinations thereof, provided that such re-
Several states have passed statutes which deal with computerized records in more limited contexts. Delaware, Kansas, and North Carolina provide for computerized records in their general corporation statutes. Under section 224 of the corporation law, Delaware permits a corporation to maintain its records in the form of, punch cards, magnetic tape, . . . or any other information storage device, provided that the records so kept can be converted into clearly legible written form within a reasonable time. . . . [This legible print-out] . . . shall be admissible in evidence, and accepted for all other purposes, to the same extent as an original written record of the same information would have been . . . .

Kansas has enacted a similar statute. North Carolina has been even more liberal toward corporate computer records than either of these two states. Its law specifies that any records maintained by a corporation may be kept on any information storage device "provided that the records so kept can be converted into a clearly legible form . . . . Where records are kept in such manner, the cards . . . or other information storage device together with a duly authenticated printout or translation shall be admissible in evidence . . . .

A number of states have statutes that refer to computerized records in a limited fashion. Iowa has added the phrase "including electronic means and interpretation thereof" to the definition of admissible evidence found in section two of the Uniform Business Records as Evidence Act. Indiana has a law sanctioning the admission of computerized hospital records if the proponent has presented an adequate foundation. Colorado's public records

\[
\text{recording is (a) reasonably permanent and (b) readable by sight. When information or data is recorded by means of a generally accepted method or system, which is operated with suitable controls to safeguard the reliability and accuracy of the information or data, and which is equipped with means for providing a reproduction that is a "writing", such reproduction shall be treated as the equivalent of the information or data, notwithstanding that the form of recording does not itself constitute a "writing" as defined by this rule.}
\]

N.J. R. EVID. 1(13) (emphasis added).

50 DEL. CODE ANN. tit. 8 § 224 (1975).
54 The relevant provisions of the Indiana statute are as follows:

34-3-15.5-2. Reproductions.—Admissibility in evidence.—The recording of hospital medical records by an electronic image system or reproduction process, shall, for the purposes of this chapter [34-3-15.5-1 to 34-3-15.5-4],
statute defines "writings" to include "cards, tapes, recordings, or other documentary materials regardless of physical form or characteristics." 55 An Oregon law permits a "transcript" of a computerized public record to be admitted into evidence if the certifying officer states that "it is a correct transcript of specified data contained within the data processing device or computer." 56 Virginia has passed a similar statute admitting reproduction of public records including "[a]ny printed reproduction of data electronically recorded on magnetic surfaces." 57

One state, California, has dealt with computer evidence by permitting computer records to be used to satisfy the best evidence rule. The statute allows certified reproductions including "a reproduction from an electronic recording of video images on magnetic surfaces" to be admitted in lieu of the original writing if it is lost or destroyed. 58

In addition to the jurisdictions that have changed some or all of their evidentiary rules to account for computer records, over half of the states have enacted the Uniform Photographic Copies of Business and Public Records as Evidence Act, 59 which may arguably be used for the same purpose. 60 This law provides that a copy of a business or public record "is as admissible in evidence as the original itself . . . whether the original is in existence or not," if the proponent can show that both the copy and the original were

be considered a photographic process. The making or recording of hospital medical records by electronic data processing systems is an original written record, and print-outs or other types of retrieved information in written or printed form shall be treated as original records in all courts or administrative agencies for the purpose of its admissibility into evidence.

34-3-15.5-3. Authentication.—Entries made in a hospital medical record may be authenticated by showing that:

(1) the electronic data processing equipment is standard equipment in the hospital;

(2) the entries were made in the regular course of business at or reasonably near to the happening of the event or order, opinion, or other information recorded;

(3) the security of the entries from unauthorized access can be demonstrated through the use of audit trails; and

(4) records of all original entries and subsequent access to the information are maintained.


60 Id. 453-63.
made "in the regular course of business or activity." Although this Act does not refer to copies generated by computers, it does allow for reproductions created by any "other process which accurately reproduces or forms a durable medium for so reproducing the original." B. An Overview of Case Law Treatment

Many judges in states without specific provisions for computer evidence have shown considerable ingenuity in permitting these types of records to be introduced under the various versions of business and public records statutory exceptions to the hearsay rule. These statutes include the New York, Georgia, and federal counterparts of the Commonwealth Fund Act,63 the federal statute pertaining to certified copies of official records,64 the Uniform Business Records as Evidence Act,65 the "hybrid" Texas business records statute,66 the 1953 version of the Uniform Rules of Evidence,67 and in the absence of any governing statute, the common law, shop book rule.68 The result has been that a significant number of courts have treated business and government records stored in computers in the same fashion as those conventionally maintained.69

61 Id. 457.
62 Id.
64 E.g., United States v. Farris, 517 F.2d 226 (7th Cir. 1975), cert. denied, 423 U.S. 892 (1975). But cf. Sunset Motor Lines, Inc. v. Lu-Tex Packing Co., 256 F.2d 495 (5th Cir. 1958) (Agriculture Department IBM punch card held inadmissible because it lacked the certification required by Federal Rule of Civil Procedure 44(a)).
68 E.g., State v. Hodgson, 305 So. 2d 421 (La. 1975); King v. Murdock Acceptance Corp., 222 So. 2d 393 (Miss. 1969).
69 See notes 77-78 infra.
Computer-generated evidence has been introduced in criminal as well as civil proceedings to prove both the nonoccurrence of unrecorded events and the occurrence of recorded transactions.

Many judges have also been willing to treat records stored in computers as though they were more traditionally prepared for the purposes of the best evidence rule. Computer printouts have been held to satisfy the originality requirements of the rule, while oral testimony pertaining to the contents of computer data files has been excluded for violating original or best evidence requirements. The introduction of computer-generated summaries of voluminous written records has been permitted in lieu of the underlying documents.

IV. A CRITICISM OF THE CURRENT JUDICIAL TREATMENT OF COMPUTER-GENERATED EVIDENCE

A. The Nature of the Problem: Computer Data Processing Is Qualitatively Different From Conventional Record Processing Techniques

The courts have made a laudable effort to adjust existing rules of evidence to accommodate computer materials. In light of complex computer systems' susceptibility to numerous possibilities for error, the question arises whether additional safeguards should be required before computerized records are admitted into evidence.

72 E.g., United States v. De Georgia, 420 F.2d 889 (9th Cir. 1969); see United States v. Liebert, 519 F.2d 542, 547 (3d Cir. 1975), cert. denied, 423 U.S. 985 (1975).
74 E.g., King v. Murdock Acceptance Corp., 222 So. 2d 393 (Miss. 1969).
75 State v. McGee, 131 N.J. Super. 292, 329 A.2d 581 (App. Div. 1974) (excluding testimony concerning the contents of a National Crime Information Center computer file); State v. Springer, 263 N.C. 627, 197 S.E.2d 536 (1973) (excluding testimony about the contents of a credit card data file). But cf. United States v. De Georgia, 420 F.2d 889, 894 (9th Cir. 1969) (refusal to consider on procedural grounds the defendant's best evidence rule challenge to testimony regarding the contents of an automobile rental company's computerized files). Had the defendant in De Georgia raised a timely objection to the admission of this testimony, the motion may have been sustained by the trial court. The government only produced information about the file's contents in the court below and failed to show the impossibility of making a print-out of the information displayed or printed on the witness' on-line terminal.
Many courts have not insisted that proponents of computerized evidence adequately demonstrate the accuracy of their data processing systems. Computerized evidence has often been admitted on the basis of the minimum statutory foundation, a custodian’s testimony that the records were made in the regular course of business at or near the time of the transaction by someone under a business duty to accurately report the transaction.

Judges and commentators who have considered the foundation accorded conventional records to be equally satisfactory for computer-generated ones have failed to account for the significant differences between the two types of evidence. With traditionally prepared records a trier-of-fact can recognize potential sources of error. The personal experience of a judge no doubt encompasses common clerical and bookkeeping errors such as misplacing a decimal point, making a subtraction error, or forgetting to record a transaction. A judge is usually able to properly evaluate a set of records if he is told how they were prepared. There is little need for a proponent of the evidence to go into a lengthy discourse on the possibility of error and the precautions taken. There is a serious risk with computer records that the judge, and perhaps even more so the jury, will be overly impressed by the computer’s mystique and will unnecessarily accept its output as reliable.

Because a judge usually has little knowledge about computers he is unlikely to be aware of the various mechanical, environmental and human factors that could cause errors in a computer’s output. For example, in a poorly controlled system even a speck of dust could significantly change a given record by concealing a magnetic impulse on a tape file. A judge cannot determine the reliability of the exhibits admitted into evidence unless the foundation deals with the various possibilities for error. Moreover, because most mistakes originate as human error, most notably input errors, the reliability of a computer’s output may be overestimated by underestimating the chances for mistake in the human interaction with the computer system.

---

77 E.g., United States v. Fendley, 522 F.2d 181 (5th Cir. 1975).
80 See text accompanying notes 84-133 infra.
81 Roberts, supra note 1, at 262.
Judicial unfamiliarity with potential computer error sources does not necessarily require that an expert witness testify regarding dust particles or other technical problems every time a computerized exhibit is offered into evidence. Nor is it necessary for the court to hold a "minitrial" to determine the accuracy of a given system. Rather, the proponent of the evidence should include an overview of the possible errors in the data processing system and the procedures used to detect and eliminate them.

Much has been written about auditing computer systems, minimizing computer errors, and detecting and preventing computer fraud. 82 Extensive checklists of error sources and internal auditing controls have been published. 83 A brief description of several sources of computer errors and the prevention controls available is set out below. These controls provide the circumstantial guarantees that a particular computer-generated exhibit is trustworthy and should therefore be admitted under the business or official records exceptions to the hearsay rule.

B. Computer Errors and Controls

There are at least five major classifications of electronic data processing errors. Technologists label environmentally induced errors and hardware failures as mechanical shortcomings. They consider systems design and programming errors, operating mistakes, and input errors to be human errors. 84 Human errors occur far more often than mechanical ones. 85 Input errors alone account for more computer processing mistakes than any other source. 86

1. Environmentally Induced Errors

Despite their sturdy and often massive physical appearance, electronic digital computers are delicate devices which require a

---


83 An extensive checklist can be found in J. MARTIN, supra note 82, at 492-590. See also B.A.I, supra note 82, at 49-52, 87-89; PORTER, supra note 82, at 49-53; Joplin, An Internal Control Checklist for EDP, MANAGEMENT SERVICES, July-August, 1964 at 32, reprinted in Carmichael, supra note 82, at 247.

84 This classification of error sources is the author's. For an alternate classification, see J. MARTIN, supra note 82, at 22-27.

85 E.g., J. MARTIN, supra note 82, at 11; 16 AM. JUR. P. OF F., supra note 1, at §§ 13, 15.

86 E.g., J. MARTIN, supra note 82, at 25.
proper environment in order to function well. The various types of input/output and data storage media employed in a data processing system are also sensitive to environmental conditions. Excessive heat, humidity, dust, power source fluctuations and electromagnetic and magnetic interference may cause the system to malfunction. This is unlikely to occur, however, since almost all computer installations have rigidly controlled environments and are located away from radio, television and radar transmitters in properly grounded buildings to prevent injury to data files from electromagnetic radiation or electrical storms. In addition, most manufacturers equip their computers with a variety of self-protection devices including fuses, air filters, power regulators, and thermostatic control switches which can disable a computer before any of the hardware is seriously damaged.

While there have been some published reports of tapes and disks being erased by magnets, "the story that tapes inside their canisters have been erased by boy scouts walking through an installation with magnets in their pockets is simply not true." Nevertheless, a computer installation can be protected from magnet-armed saboteurs (or boy scouts) through the use of magnet detectors that set off an alarm and lock the entrance to the computer room.

2. Hardware Failures

Independently caused hardware or component failures are very rare. Nevertheless, some components, especially the telecommunications lines used in either time sharing or on-line real time (OLRT) systems to connect the computer with its various point-of-transaction terminals, are more error prone than others. If designed properly, however, error detecting circuits and codes can be used to catch virtually all of the hardware errors that are likely to occur.

---

88 See id. 65-66.
89 See J. Martin, supra note 82, at 329; Beardsley, supra note 87, at 48-49.
90 J. Martin, supra note 82, at 323, 329 (relates an incident in which protestors armed with magnets erased 1000 reels of magnetic tape at a Dow Chemical installation).
91 J. Martin, supra note 82, at 329. See also Beardsley, supra note 87, at 47.
92 Beardsley, supra note 87, at 48. Beardsley, however, does not recommend the use of these devices. Id. at 48.
93 J. Martin, supra note 82, at 22.
in a computer system or its telecommunications lines. Moreover, a regular program of preventative maintenance by qualified customer engineers (servicemen) will further reduce the likelihood of breakdowns.

3. Systems Design and Programming Errors

A computer only performs tasks for which it is programmed. There are several levels of computer program complexity. At the lowest level are application programs that instruct the computer to perform relatively minor tasks; at the highest level are the complex, software operating systems which, among other things, supervise and monitor all of the computer system’s operations, schedule tasks according to priorities, and check the error detecting or correcting codes.

Programming errors at any one of the various levels are relatively common. A single mistake may be seriously compounded if a computer obediently uses an erroneous instruction several times. Programming errors are notorious for producing absurd results.

Programming mistakes can easily be detected and even avoided if proper program design and debugging procedures are followed. First, the managerial and data processing staff must agree on the appropriate goals and systems design. Second, adequate documentation should be prepared and maintained on a current basis, including: systems flow charts, program block diagrams, program instruction listings, input/output format listings, and textual descriptions of each program. Third, all programs should be

94 Id. at 22, 90-109. See B.A.I., supra note 82, at 28-31. These codes may also be used to detect wiretapping and other forms of surreptitious or fraudulent manipulation of data banks by embezzlers, data pirates and others. See generally L. Hoffman, Security and Privacy in Computer Systems 43-404 (1973); J. Martin, supra note 82, at 145-77, 204-48, 333-48.

95 B.A.I., supra note 82, at 30; Joplin, supra note 83, at 254.

96 Roberts, supra note 1, at 260.

97 See J. Martin, supra note 82, at 188; A. Vazsonyi, supra note 3, at 308-12; Brightman, supra note 2, at 311-36.

98 Roberts, supra note 1, at 259.


100 See Roberts, supra note 1, at 260-61.

101 Id. 261 & n.25.

102 Id. 261; A. Vazsonyi, supra note 3, at 137-74; R. Brightman, supra note 2, at 89-100; Joplin, supra note 83, at 250-51.
thoroughly tested. Test data can be used to review most anticipated data contingencies. The results of these runs can then be compared with those results obtained from existing or modified programs. Finally, standard software and program packages can be obtained from computer manufacturers. These packages have been fully tested by the manufacturers' staffs and are updated on a periodic basis to reflect the error experience of all package users as well as to keep abreast of recent developments.

The use of these programming controls can significantly reduce the number of errors in software systems and programs. Nevertheless, some programming errors are virtually inevitable because of the unavoidable frailties in the human component of computer applications.

4. Operating Procedure Errors

Electronic data processing systems vary according to the degree of human interaction with the system. As the operator becomes more responsible for supervising computer operations and data reception the possibility of operating errors increases. Moreover, these mistakes can be serious. An operator in a poorly controlled system can, among other things, accidentally erase vital data, update financial data more than once, or process an out-of-date backup file and thereby lose a record of all transactions recorded after the expiration date of the backup file.

Operator errors can be minimized through the use of several accepted controls. First, complete, clear, and simple written operating guidelines should be prepared so that oral instructions are not needed to operate the system. Second, a tape librarian should be employed to channel the correct input data to the often harried operators. Third, all programs can be designed to check for data file labels containing identifying information such as creation and retention dates, reel and program numbers, and transaction counts. Fourth, an effort must be made to staff the

---

103 See W. Porter, supra note 82, at 53-58; Roberts, supra note 1, at 260 & n.23; J. Martin, supra note 82, at 22-24.
104 A. Vazsonyi, supra note 3, at 335.
105 See J. Martin, supra note 82, at 24. Cf. Roberts, supra note 1, at 264-65 (stating that the probability of input errors increases as the level of human intervention in the data collection process increases).
106 J. Martin, supra note 82, at 24; B.A.I., supra note 82, at 25.
107 Joplin, supra note 87, at 250-52.
108 See W. Porter, supra note 82, at 29-30, 40; Joplin, supra note 83, at 249.
109 B.A.I., supra note 82, at 32, 51; W. Porter, supra note 82, at 51-52; Joplin, supra note 87, at 253.
computer room with qualified individuals, a hard task since "computer operators are generally difficult to recruit and quick to leave a position, a situation that enhances the possibility of errors." Fifth, reliance on electromechanical unit record devices for sorting and collating data, known as electronic accounting machines (EAM), should be reduced because these functions can be performed by computers with a greater degree of accuracy and speed. Sixth, if EAM devices are used, their easily damaged wire control panels should be inspected on a regular basis, as should all mechanical components of a computer system. Seventh, input/output bins should be used to insure that all materials are dispatched to the proper individuals. Finally, and most importantly, working conditions conducive to good operator morale should be maintained.

5. Input Errors

Incorrect input is by far the largest cause of data processing errors. A computer system is only as accurate as the accompanying data it processes. If the data is in error, incomplete or processed incorrectly the output will be in error.

As a result, most electronic data processing installations use a variety of internal controls to minimize input mistakes. Indeed, many installations will have a separate department for this purpose. The control staff's function is to verify all inputs and outputs, and, in some installations, to maintain the tape library.

The exact organization of input/output controls depends on whether the installation is using a batch processing or on-line real time (OLRT) processing system. With batch processing, transactions are grouped into "batches" and processed on a delayed basis;
in an OLRT system, on the other hand, transactions are processed by the computer simultaneously, with or within a short time after their actual occurrence. For example, a bank which collects all transactions from one teller and groups them into a batch to be processed at the end of the business day is using a batch processing system; whereas a bank employing point-of-transaction terminals to record all transactions on the bank's data files as they are entered into the customers' passbooks is using an OLRT system.

Error controls should be used at each of the four stages in a batch processing system. During the first stage, conventional methods (e.g., handwriting) are used to record the transactions on hard copy forms (e.g., customer order forms). Most of the error controls that can be used at this point are similar to those used in traditional information processing systems, for example, verbal confirmation of the transaction or use of prenumbered forms to account for all transactions.

During the second stage, the information on the hard copies is transferred by keyboard-operated machines (e.g., keypunch) or optical scanners to data processing media such as punched cards or magnetic tapes. The standard controls that should be employed at this stage include verifying the accuracy of the data by rekeying or rescanning the same hard copies and manually adding some of the columns of quantitative information from each transaction, such as the dollar values or customer numbers, to obtain batch or hash totals which can then be punched onto batch control cards.

After the keying and control staff has examined the data for obvious errors (e.g., missing account numbers), the data is fed into the computer system. The basic control that most installations use at this third stage is a data edit program. This program compares the data with a series of validation checks, including the batch and hash totals, magnitude checks (e.g., no payroll check over $500), crossfootings, and error-detecting check digit codes. As a

---

119 See generally A. Vazsonyi, supra note 3, at 57-68; R. Brightman, supra note 2, at 353-71.
120 See Joplin, supra note 83, at 251; B.A.I., supra note 82, at 49-50; W. Porter, supra note 82, at 51.
121 J. Martin, supra note 82, at 54; B.A.I., supra note 82, at 27-28.
122 J. Martin, supra note 82, at 60; B.A.I., supra note 82, at 27; W. Porter, supra note 82, at 51. For a description of the difference between batch totals (the sum of meaningful figures such as dollar amounts) and hash totals (a sum that is meaningless except for validity checking purposes), see J. Martin, supra note 82, at 60.
123 J. Martin, supra note 82, at 54-64; B.A.I., supra note 82, at 31-33, 51; W. Porter, supra note 82, at 51-52; Joplin, supra note 83, at 252-53. A check digit is computed on the basis of a formula that manipulates all of the digits in a
result of this edit program, any batch containing incorrect data will be flagged and not processed until corrected by the control staff. After the data has been electronically processed, the output is usually sent to the control staff to be dispatched. The controls often used at this fourth stage of processing include physical examination of the output by the control staff and recording of the final total figures and cross footings into a ledger book for use in verifying any weekly or monthly reports that may be issued.124

In an OLRT system all of the processing stages have been collapsed. The recording, processing, and output dispatchment stages of each transaction occur within a very short period of time. Moreover, because a hard copy of each transaction may not exist in many OLRT systems (known as the disappearing or nonexistent audit trail), the opportunity to compare the computer and manual results may not exist in some systems.125 Consequently, the error control emphasis in these systems will be placed on immediate feedback controls. These controls include validation checks similar to those performed by a batch edit program, examination of the error detecting codes, and descriptive textual feedback.126

In those OLRT systems which still maintain hard copies of transactions (such as a bank OLRT system which requires tellers to collect deposit and withdrawal slips) batch and hash totals may be used as error controls. Finally, in any system distributing tangible objects such as machine parts or currency by on-line transac-
tions errors may be reduced by taking periodic balances or inventories of the tangible objects.\textsuperscript{127}

6. Administrative Controls

In addition to the above described data processing controls,\textsuperscript{128} an EDP installation will often use a series of administrative or managerial controls such as the separation of the individual employees' duties and the use of time sheets for logging staff members' activities.\textsuperscript{129} These procedures further reduce errors and help trace individual responsibility when they do occur. These controls also reduce opportunities for fraudulent misuse of a poorly controlled data processing system.\textsuperscript{130}

C. Computer Evidence and the Business Records Exception: The Need for Greater Foundation Testimony

A number of judges have insisted that litigants seeking the admission of computer evidence under the business records exception to the hearsay rule offer an evidentiary foundation responsive to the possible errors discussed in the preceding section. It is these cases\textsuperscript{131} that set the desirable precedent, rather than those which

\textsuperscript{127} Id. 77.

\textsuperscript{128} See text accompanying notes 89-127 supra.

\textsuperscript{129} Id. 371-77; B.A.I., supra note 82, at 33-34; W. Porter, supra note 82, at 49; Joplin, supra note 83, at 248-49.


permit entry of computer material on a basis similar to that afforded manual business records.\textsuperscript{132}

In a 1965 case dealing with the admissibility of computer records, \textit{Transport Indemnity Co. v. Seib},\textsuperscript{133} the Supreme Court of Nebraska affirmed a trial court's decision to permit entry of computer materials largely because of the extensive foundation testimony which accompanied them. The plaintiff had sought to convince the judge that a computer printout of the defendant's insurance transactions was reliable by having the accounting manager detail the company's bookkeeping, premium computation, claims reporting, and computer procedures.

Since \textit{Seib}, other courts have similarly required proponents of computer evidence to describe in detail the activities affecting the output of the machines. In \textit{Railroad Commission v. Southern Pacific Company},\textsuperscript{134} the Texas Court of Civil Appeals reversed a trial court for admitting computer evidence where the proponent had failed to offer testimony as to the type of computer employed, the permanent nature of record storage, and how daily processing of information fed into the computer was conducted. Likewise, in \textit{State v. McGee},\textsuperscript{135} the Appellate Division of the New Jersey Superior Court reversed a defendant's conviction for transporting a stolen gun into the state, in part because the trial court had erred in permitting a prosecution witness to testify that the National Crime Information Center had reported the gun stolen. The appel-

\textsuperscript{132} See, \textit{e.g.}, United States v. De Georgia, 420 F.2d 889 (9th Cir. 1969) (government's foundation merely indicated that auto rental company relied upon its computer system and otherwise no specific foundation on the system's accuracy was presented); Merrick v. United States Rubber Co., 7 Ariz. App. 433, 440 P.2d 314 (1968) (foundation presented by a company credit manager who had "no personal knowledge of the actual physical operation of the plaintiff's IBM accounting [EAM] equipment" was held to be sufficient); City of Seattle v. Heath, 10 Wash. App. 949, 520 P.2d 1392 (1974) (foundation by custodian of a printout held sufficient although no foundation supporting the accuracy of the underlying data processing system was presented). \textit{Cf.} Perma Research & Development v. Singer Co., 542 F.2d 111 (2d Cir.), \textit{cert. denied}, 429 U.S. 987 (1976) (computed-generated evidence of the performance of an unproduced automotive part held admissible in support of a $7 million damage award although the proponent's programming procedures were not disclosed on "work product" grounds); United States v. Fendley, 522 F.2d 181 (5th Cir. 1975) (insurance company printout admitted on procedural grounds despite the government's failure to "completely lay a proper foundation"). See also, Bobbie Brooks, Inc. v. Hyatt, 195 Neb. 596, 239 N.W.2d 782, 784 (1976) (foundation testimony was incorrect as a matter of generally accepted auditing standards); Matthews Estate, 47 Pa. D. \& C.2d 529, 534-5 (Orphans' Ct. 1969) (foundation testimony was misleading in stating that it was "physically impossible" to alter or eliminate a magnetic tape record).

\textsuperscript{133} 178 Neb. 253, 132 N.W.2d 871 (1965).

\textsuperscript{134} 468 S.W.2d 125 (Tex. Civ. App. 1971).

late court held that the trial court had been lax in not requiring
the prosecution to produce the computer evidence underlying the
testimony; the prosecution should have also indicated "how and
who fed the information into the computer; ... who programmed
the computer and how it was done; how the data was retrieved from
the computer; the accuracy of those who operated the computer." 136

Some courts have been impressed by the specificity of a particu-
lar proponent's foundation. In King v. State ex rel. Murdock
Acceptance Corporation, 137 the Supreme Court of Mississippi held
that a computer printout was admissible under the common law
shop book rule to prove the balance due on six conditional sales
contracts. The electronic data processing manager not only pointed
out the type of data processing equipment used, but also explained
the company's key punching, key verifying, and customer tape file
maintenance procedures. 138 Moreover, in United States v. Green-
lee, 139 a tax fraud case, the government succeeded in bringing in
computer evidence under the Federal Business Records Act 140 by
showing the intricate key punch and verification processes employed
by the Internal Revenue Service. 141

Courts have also been concerned with other types of error
in computer systems. In State v. Hibbs, 142 a prosecution for mak-
ing obscene telephone calls, several witnesses testified as to the
error controls used to prevent hardware failures and environ-
mentally induced malfunctions in the computerized electronic tele-
phone tracing equipment. 143

Judges who have expressed concern about the reliability of
computer data have generally preferred that high-ranking employees
of computer departments, as opposed to accountants or comptrollers,
describe the machinery and procedures. 144 There are, however,
cases in which accountants have provided satisfactory testimony. 145

In addition to being careful about the nature and presentation
of the foundation surrounding computer evidence, a number of

136 Id. at 298-99, 329 A.2d at 584-85.
137 222 So. 2d 393 (Miss. 1969).
138 Id. 396-97.
141 380 F. Supp. at 654-55.
142 123 N.J. Super. 152, 301 A.2d 789 (Mercer County Ct. 1972), aff'd, 123
143 Id. at 159-60, 301 A.2d at 793-94.
144 See cases cited notes 134, 137, 139 supra.
courts have sought collateral means of insuring reliability. Commentators have suggested that proponents of computer evidence notify their opponents early in the pretrial stage so that the evidence can be examined, the systems controls investigated, the underlying data verified, and even "hands-on" access to the proponents' systems provided for independent testing. In civil proceedings discovery of the proponent's computer-related materials would be governed by rule 34 of the Federal Rules of Civil Procedure. In criminal trials rule 16 (2) (1) (c) of the Federal Rules of Criminal Procedure may allow defendants to gain access to the prosecution's computer evidence. However, in those criminal cases where the computerized evidence was generated by a government data processing installation, discovery of the prosecution's data files may be denied in order to protect the secrecy or operational integrity of the government's files. Nevertheless, even where such security considerations apply, the prosecution should make the government installation's operating and programming procedures available to the defendant even if the actual data files are not produced.

D. Computer Evidence and the Official Records Exception

Designed to minimize inconvenience to public agencies, the official records exception has enabled some parties to use computer evidence without supplying the assurances of trustworthiness often required in the business records context. Those parties who have sought to introduce computerized official evidence have encountered varying requirements for admissibility. Others who have argued that the absence of an official computerized record evidenced that an event or transaction had not occurred have been able to do so merely by obtaining a custodian's testimony that a "diligent search failed to disclose the . . . data compilation."

146 See Manual, supra note 2, at §§ 2.714, 2.715 & 2.717; United States v. Davey, 543 F.2d 996 (2d Cir. 1976) (taxpayer ordered to provide original tape files to I.R.S.).


149 See McCormick, supra note 8, § 315; J. Maguire, supra note 14, at 693-94.


151 Fed. R. Evid. 803(10).
This lenient approach offers little guarantee that computer-generated evidence is being used in a reliable manner.

The most cautious way to eliminate the weakness of the official records exception is to require all parties using official records to demonstrate the same circumstantial guarantees of trustworthiness insisted upon by courts dealing with business records. This would mean that government computer experts or accountants would be required to describe the computer systems and procedures in great detail. In order to avoid interference with ongoing government work, the courts might allow independent government or certified public accountants to perform the same task.

E. Computer-Generated Records and the Best Evidence Rule

As noted earlier,\textsuperscript{152} computer-generated evidence has been treated in a manner comparable to the treatment of conventionally prepared writings under the best evidence rule. Rule 1001 (3) of the Federal Rules of Evidence states that a visual printout prepared from nonvisual data media qualifies as an original document under the best evidence rule. Several other jurisdictions have achieved the same result either through the adoption of rules of evidence patterned after the Federal Rules\textsuperscript{153} or through judicial construction of the common law best evidence rule.\textsuperscript{154}

Although not expressly stated, Rule 1001 (3) does not bestow "original" status upon a printout unless the conventionally prepared, hard copy documents which formed the basis for the data file are unavailable due to destruction in the regular course of business. Under these circumstances the printout could be offered as a summary of the voluminous original, hard copy documents, an exception to the best evidence rule.\textsuperscript{155} Although the admission of summaries of voluminous documents often simplifies matters in complex litigation, a court should not permit their use unless the opposing parties have had an adequate opportunity to examine the underlying data and programming documentation as well as the proposed computer-generated exhibit.\textsuperscript{156}

\textsuperscript{152}See text accompanying notes 74-76 supra.
\textsuperscript{153}See text accompanying note 49 supra.
\textsuperscript{155}See FED. R. EVID. 1008.
\textsuperscript{156}See MANUAL, supra note 2, at §§ 2.711-2.717.
In addition, certified government printouts are admissible under the official records exception to the best evidence rule regardless of whether the original hard copy documents are available or not. The courts should not, however, confuse the official records exception to the best evidence rule with the official records exception to the hearsay rule. The fact that a certified printout may be presented in lieu of an original document should not prevent the courts from requiring a foundation witness, accountant's opinion, or other circumstantial guarantee that the certified printout is reliable.

V. CONCLUSION

The courts have viewed existing statutory and common law rules of evidence in a flexible manner and have held that computer-generated evidence is admissible in both civil and criminal proceedings to the same extent as conventionally prepared evidence under the hearsay and best evidence rules. State legislatures have increasingly indicated support for these judicial advances by adopting rules of evidence modeled after the liberal Federal Rules of Evidence.

Some courts have been too lenient in allowing the admission of computer evidence inadequately supported by corroborating testimony. The facts are that the reliability of computer records is clouded by a large number of nonobvious opportunities for error or misuse. Courts should not allow computer evidence to be introduced unless the proponents of the evidence demonstrate that their data processing systems have satisfactory controls. Judges should also encourage widespread criminal and civil discovery and any other means of verifying the reliability of computer evidence.

---

168 See text accompanying notes 149-151 supra.