Ensuring the Court Admissibility of Computer-Generated Records

ROGER KING and CAROLYN STANLEY
University of Colorado

An informal methodology is described for optimizing the likelihood of computer-generated records being admissible in a U.S. court of law. This methodology is intended for individuals who are converting to automated office procedures, as well as for those whose businesses are already highly computerized. However, this paper does not purport to be a formal legal guide; rather, it is intended as an overview of this issue.

Categories and Subject Descriptors: J.1 [**Computer Applications**]: Administrative Data Processing—*law*

General Terms: Legal Aspects

Additional Key Words and Phrases: Evidence, records

1. INTRODUCTION

Computer scientists are usually more concerned with hardware and software than with the social and legal aspects of using computers in an office environment. However, some of these human aspects should be considered when planning a conversion from a manual to an automated office. One important consideration often overlooked in the rush toward "office automation" is the possibility that the computer-generated records from that office might be needed as evidence in a court trial. Riggs [16] cites a recent survey where, in 118 civil cases involving the admissibility of computer-generated records, objections were raised in 15 cases, and 4 of these objections were sustained. Indeed, issues of admissibility are accelerating as computers become the standard for business record keeping. This paper is an attempt to explain, in terms useful to computer science professionals, what legal authorities have written about this issue.

The methodology in this paper is intended as a guide for individuals planning a conversion to an automated office, or for computer and management profes-

This research was sponsored by IBM through a Faculty Development Award.
A preliminary version of this paper, An Informal Conversion Methodology for Ensuring the Court Admissibility of Computer Generated Records, by R. King and C. Stanley, appeared in the *Proceedings of the IEEE 1st International Conference on Office Automation* (New Orleans, La., Dec. 17–19), IEEE, New York, 1984. © IEEE 1984. The portions of this paper that appeared in the earlier version are reprinted with permission.
Authors' addresses: R. King, Department of Computer Science, University of Colorado, Boulder, CO 80309; C. Stanley, 4723 Commons Drive, #102, Annadale, VA. 22003.

sionals who may be concerned about the acceptability of their computer records in a court of law. The methodology is tailored primarily to the legal system of the United States, and while we hope it proves useful to individuals in other countries, we urge any non-U.S. readers to consult a legal authority in their own country before drawing any conclusions from this paper. Before presenting our methodology, it is necessary to establish the reason this issue is important now. It is also important to define, in lay terms, several of the specific legal terms used herein. But first, we briefly attempt to place the issue of court admissibility in perspective within the larger issue of computer-related law.

2. COMPUTER LAW

While physicians and engineers have long since learned—via the necessity of being licensed—that the law is an important aspect of their careers, computer experts are only just now becoming aware that they, too, must learn to understand the law. As the possibility of some day needing to be licensed as professionals looms ahead, computer scientists are suddenly more interested in the laws affecting computer-related negligence and malpractice lawsuits. Along with a concern over lawsuits is a growing concern about computer crime. Innocent "hacking" leading to the theft of computer time, the free use of software, and the embezzlement of money are no longer being tolerated by law enforcement agencies. Already, for the sake of financial self-preservation, many computer programmers are becoming experts in another aspect of the law—software protection. Copyrights, patents, trade secrets, and contracts are being used as vehicles to protect against the unauthorized use of programs.

In the preface to his book *Law and the Computer*, which covers all these topics and more, Gemignani states:

> Computer science, in the few decades since the first stored-program computer was built, has evolved at a rate that has outstripped society's ability to deal with the novel issues this technology has raised. [9]

To a computer professional, the issue may quickly seem overwhelming. In this paper, we address one specific issue, evidence, and attempt to make the computer professional aware of its importance.

3. JUSTIFICATION FOR RAISING THE ADMISSIBILITY ISSUE

Because so many varieties of equipment and software are available, with salespeople for each manufacturer or software house touting his or hers as "the best" for all purposes, the final choice of what and how much equipment to install may be predicated on factors other than cost or productivity of the system. No one plans to need business records in a court case; however, they are sometimes necessary. Current statutes follow naturally from what has become generally accepted good business practices. Thus, the individual concerned with the court admissibility of computer-generated records will find that the key to assuring the admissibility of computer records lies in developing computer systems which model accurate and reliable business practices. The issue of the accuracy and reliability of computer-generated records often does not arise in a civil case because of such measures as *discovery*, the right of an attorney to view the opposition's evidence before the trial.

Among the various court cases in which computer-based records have been offered in evidence have been these which are cited most often as precedent setting:

(1) The *Transport Indemnity Co. v. Seib* case[1] in which the computer printouts were used to prove the amount of premiums owed on an insurance policy [1].

(2) The *King v. State ex rel. Murdock Acceptance Corp* case[2] in which computer printouts were used to determine the amount of damages due the plaintiff. In this case, the defendant was convicted of affixing false notarial certificates to a deed of trust. The Mississippi Supreme Court affirmed the admission of the printouts as evidence, saying "the law always seeks the best evidence and adjusts its rules to accommodate itself to the advancement of the age it serves" [1].

(3) The *United States v. Young Bros., Inc.* case[3] which was appealed to the United States Court of Appeals, Fifth Circuit, in 1984. In this case, the government used computer-generated records to prove essential elements of its case; that is, some of the records were used to prove that the conspiracy that was the heart of the case affected interstate commerce, and other records were used to prove the actual amounts of bids involved in the case.[3]

(4) The *Harned v. Credit Bureau of Gillette* case[4] which was appealed to the Supreme Court of Wyoming in 1973. In this case, the Harneds showed that the computer-generated records that were admitted in a lower court should not have been allowed on two grounds: (a) the recapitulation, which was a summary of antecedent records, was not made in the regular course of business, and (b) the computer printout violated the best evidence rule, inasmuch as the original invoices were available and were not produced in court.

In our opinion, the diversity of these cases and the increasing complexity of business practices are major reasons why the design of an automated office should include strong consideration of the admissibility issue.

Although the courts, which are traditionally conservative, have overcome the aversion to admission of computer-generated records as evidence, it is still incumbent on the one who proposes to have such records admitted to meet certain requirements under which these records can be admitted as evidence [2]. Although we think it is likely that the computer-generated records prepared in established businesses today will be admitted when supported by the pertinent testimony of appropriate witnesses, this may not always be true. Thus, management of these businesses should give consideration to the issues raised in this paper. Another avenue which should not be overlooked it the possibility of using an expert witness to verify the accuracy of computer records, thereby sidestepping the problems inherent in the "hearsay" nature of computer records.

The usual method of getting computer-generated records admitted is submission under the business records exception to the Hearsay Rule[5] [17]; this exception is codified in Rule 803(6) of the Federal Rules of Evidence, which took

[1] 178 Neb. 253, 132 N.W.2d 871 (1965), noted in Annot., 11 A.L.R.3d 1377 (1967).
[2] 222 So.2d 393 (Miss. 1969), noted in 41 Miss.L.J. 604 (1970).
[3] 728 F.2d 682, 693-694 (5th Cir. 184).
[4] 513 P.2d 650, 5 CLSR 394.
[5] The Hearsay Rule and lay definitions of certain legal terms are given in Section 4 of this paper.

effect in 1975, replacing the Federal Business Records Act [3]. Although this law now prevails in federal court and in a majority of states, the Uniform Business Records as Evidence Act (which bears a strong resemblance to Rule 803(6)) is still effective in some states, while a few states still retain other statutes (e.g., the common-law business records exception to the Hearsay Rule entitled the Shop-Book Rule) [3].

4. BACKGROUND INFORMATION

Before considering the ramifications of the problem of attempted admission of computer-generated records as evidence, certain lay definitions of legal terms and concepts are necessary.

4.1 Definitions

These definitions are intended to help the reader understand the concepts as used in this paper and are not intended to be used as legal definitions for these terms.

Evidence is testimony, documentation, or physical items submitted (or offered) to determine the truth of alleged facts. Admissible evidence is that testimony which a judge and/or jury can properly consider when trying to decide a case; in other words, it is admitted for consideration when deciding the case. Specific requirements have been adopted regarding the admissibility of various kinds of evidence. Direct evidence is that offered by a witness who knows a fact by virtue of having witnessed an event or having been a part of a transaction, etc.; by contrast, *hearsay* (or hearsay evidence) is an out-of-court statement (or conduct) offered in court to prove the truth of the matter in that statement [4, 5].

A *custodian* is a person who has custody of the evidence; that is, he or she has possession of the evidence and is responsible for it. In this paper, this refers to the person or persons who had custody at the time relating to the issue under consideration in the trial; it does not refer to the person responsible for safeguarding the evidence once the trial is in progress. Often the custodian is someone in a management position; at other times the custodian refers to the sequence of people who successively have custody of the evidence. It should be noted that federal courts now allow evidence to be presented by other qualified witnesses in addition to the custodian; often this is one person who is capable of explaining the justification for the admission of the evidence as well as describing its relevance.

Hearsay is defined by Rule 802 of the Federal Rules of Evidence, which reads in part:

> Hearsay evidence is not admissible except as provided by these rules prescribed by the Supreme Court pursuant to statutory authority or by Act of Congress.

Here the word *except* refers to the exceptions that are given in Rule 803 of the Federal Rules of Evidence.

4.2 The Admissibility Rules—Relating to Printouts as Hearsay Evidence

A computer printout is considered to be an out-of-court statement, and when it is offered in court for the truth of what it asserts, it is deemed to be hearsay;

therefore, it must fall under one of the exception categories to be admissible as evidence. In most states and at the federal level, the most commonly used exception is the business records exception [17].

The reason for relying on computer printouts (or computer-generated records) as evidence is because sometimes no human witness is available to testify to the truth of the matters contained in the printouts. Often, information is entered on an original form by a clerk who (even if identifiable) has no recollection of the specific transaction in question. The first computer entry is likewise made along with so many other entries that the person entering it is not really aware of what is being entered. The processing is done by one or more programs to produce the final data, and the final output is printed automatically as the result of another computer program. Of course, as small workstations and integrated, computerized office facilities become more widespread, the anonymity of the entry personnel should prove to be less of an issue. However, the clerk is still not likely to be aware of the inner workings of the computer.

Even before the advent of computers, similar successions of events were so common in commercial practice that since very early times it has been necessary to develop an exception to the Hearsay Rule to comply with the situation. An early case in which records previously created by a person who died before the trial was held (*Price v. Lord Torrington*, 1703, in England) developed because of the death of a drayman who had made an entry in his records shortly before his death concerning some beer he had delivered. Because the drayman was shown to be thorough in his recordkeeping and his records were vital to the case, the courts allowed those records to be admitted in evidence. After the Price case, the English court set up three conditions for the admission of such records: (1) the person making the records must be proved dead (if alive, he or she must testify); (2) the entry must have been made contemporaneously with the act; and (3) the entry must have been made in the regular course of business [2, p. 117]. Decisions made in England in the 1700s still manifest themselves today in U.S. laws.

Historically, U.S. courts have progressed from the common law concept prevalent in England to statutes enacted to govern given situations. For situations for which there is no specific statute, the ruling in the first pertinent case becomes the "precedent" and is used as the law until a statute is enacted. The development of laws covering the actual admissibility of the records generated from computers followed this path. First, the ruling from the Price v. Lord Torrington case gave rise to the "Shop-Book Rule," which covered those situations in which the records of a small business were used to determine the truth of the issue. Then, as businesses grew larger and more were engaged in interstate commerce, the Federal Business Records Act was enacted, and the Uniform Business Records as Evidence Act was adopted by a majority of the states. In 1975, the U.S. Congress adopted the Federal Rules of Evidence to be used in those cases tried in federal courts. Subsequently, most of the individual states have adopted this set of rules or a similar set for cases to be tried in the state courts.

4.2.1 *The Shop-Book Rule.* The conditions set up by the court in England in the 1700s led to the adoption in many U.S. courts, both federal and state, of a common law that has come to be known as the Shop-Book Rule. This rule sets

the following criteria for admission of business records in a trial:

(1) The records must have been made routinely during the regular course of business.
(2) The entry must have been made contemporaneously or within a reasonable time of the transaction being recorded.
(3) The entry must have been made by a person who is unavailable as a witness.
(4) The person who entered the record must have personal knowledge of the event.
(5) The person must have no motive to misrepresent or misstate the facts [2, p. 119].

The Shop-Book Rule, although replaced by legislation in most states, is still the law in others [2, p. 121]. Some courts have broadened the Shop-Book Rule; for instance, the Mississippi version has been interpreted to say that computer printout sheets of business records are admissible under certain conditions. First, they must be relevant and material. Also, the individuals who made the entries in the regular course of business need not be identified and located to testify as witnesses if

(1) the electronic computing equipment is standard equipment,
(2) the entries are made in the regular course of business at or reasonably near the time of the happening of the event recorded, and
(3) the foundation testimony satisfies the court that the sources of information, the method, and the time of preparation were such as to indicate its trustworthiness and justify its admission [7, p. 336].

4.2.2 *Uniform Business Records as Evidence Act.* The National Conference of Commissioners on Uniform State Laws sanctioned the Uniform Business Records as Evidence Act in 1936. About half of the states adopted it; although many have since replaced it with the new Uniform Rules of Evidence (patterned after the Federal Rules of Evidence), it remains in effect in several states. The Uniform Business Records as Evidence Act provides, in part

a record of an act, condition or event, shall, insofar as it is relevant, be competent evidence if three conditions are met:

(1) the custodian or other qualified witness testifies to the identity and the mode of its preparation;
(2) the record was made in the regular course of business, at or near the time of the act, condition or event;
(3) in the opinion of the court, the sources of information and the method and time of preparation were such as to justify its admission [2, p. 123].

4.2.3 *Federal Rules of Evidence: The Hearsay Rule.* In 1975, the federal government adopted the Federal Rules of Evidence. Rule 803(6), which defines the business records exception to the Hearsay Rule (Rule 802), replaced the Federal Business Records Act, which was substantially like the Uniform Business Records as Evidence Act. Subsequently, the National Conference of Commissioners on Uniform State Law withdrew its support of the Uniform Business

Records as Evidence Act. Binder [3] in the *Hearsay Handbook*, reports that one by one the states that had adopted the Uniform Business Records as Evidence Act are repealing it, usually to replace it with Rule 803(6) or something similar.

Unless conditions are such that the evidence meets one of the exceptions to the Hearsay Rule, it cannot be admitted under Rule 801; an exception to the Hearsay Rule occurs when the hearsay evidence meets a specific set of governing conditions.

Some exceptions to Rule 802 are given in Rule 803. For example, one exception to the Hearsay Rule (Rule 802) is the Business Records Exception Rule 803(6), which reads:[6]

> [Exceptions to those items automatically excluded because they are hearsay shall include] a memorandum, report, record, or data compilation in any form of acts, events, conditions, opinions or diagnoses
>
> [a] made at or near the time
> [b] by, or from information transmitted by, a person with knowledge,
> [c] if kept in the course of a regularly conducted business activity, and
> [d] if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation,
> [e] all as shown by the testimony of the custodian or other qualified witness,
> [f] 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, professions, occupation, and calling of every kind, whether or not conducted for profit.

Another exception to the Hearsay Rule is given in Rule 803(7). This rule excepts from the Hearsay Rule "evidence that a matter is not included in the memoranda, reports, records, or data compilation, in any form, kept in accordance with the provisions of Rule 803(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." In other words, if the records in question comply with Rule 803(6), the absence of an entry relating to a transaction will indicate that the transaction never occurred.

4.3 Other Applicable Evidence Rules

In addition to the hearsay evidence rules, two other evidence rules are used to determine the admissibility of computer records: the best evidence rule and the voluminous writings rule.

4.3.1 *The Best Evidence Rule.* The best evidence rule requires that the contents of an available document be proved by the introduction of the original document itself [2]. Under this rule, the original writing is required. Again, exceptions have been established. One exception relates to referring to computer printouts as a "copy of the original" with the actual keystrokes performed to enter the information into the computer being referred to as the "original." The exception says that if the original is destroyed through no malicious intent of the custodian, the copy can be offered as evidence. Because the original in this

[6] Letter designations have been added by the author.

situation is always destroyed, this part of the best evidence rule is usually not applicable [2]. This situation was alleviated for federal cases by Rule 1001(3) of the Federal Rules of Evidence which reads in part: "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.'" However, since this definition is not used in all states, it may be necessary for the offerer of the evidence to be prepared to show that the printout is indeed the original document.

4.3.2 *The Voluminous Writings Rule.* The voluminous writing rule (Rule 1006 of the Federal Rules of Evidence) provides that, where the original writings are so voluminous that it would be impractical to produce them in court, the judge can allow a summary of the material to be offered. However, the summary must be made by a competent individual, and the originals must be made available to the adverse party to examine or copy at a reasonable time and place [2]. This rule states that the court reserves the right to order that they [the originals] be produced in court.

4.3.3 *The Requirements for Authentication or Identification.* Rule 901 of the Federal Rules of Evidence specifies that a condition necessary for admissibility of evidence is that the evidence must be what the proponent claims it is. Rule 901(6) specifically enumerates one of the examples of authentication conforming with the requirements of this rule: "Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result."

4.4 Pertinence of the Methodology to the Rules of Evidence

Although the various hearsay rules (the Shop-Book Rule, the Uniform Business Records as Evidence Act, and the Federal Rules of Evidence) differ somewhat in their requirements, we are primarily addressing the requirements of the Federal Rules. While the proposed conversion methodology is our attempt to prepare its implementors to meet the requirements of each of these manifestations of the rules, it is especially designed to meet the requirements of Rule 803(6). Modifications and/or additions to the methodology may be necessary for meeting the requirements for admissibility in a particular state that may not have adopted Rule 803 (or a facsimile).

5. THE METHODOLOGY

The office conversion methodology is an item-by-item preplanning guide for those who are contemplating converting from a manual (or paper-oriented) office to an automated, computer-oriented office or upgrading the system in an already automated office. This is not primarily a guide for programmers, although it may be used as such; rather, it is directed more toward the management of the business. We believe compliance with this methodology will aid legal counsel if the computer-generated records produced in that office ever do need to be offered as evidence in a trial. Verification of the completion of each item can be accomplished at any time during the conversion process. Because this is not a sequential step-by-step methodology, it can serve well as a checklist for those who have already begun or completed the conversion. Retroactive compliance with the items of this methodology should aid anyone who might be called on to

A. System Selection
  A.1 Establish the reliability of the hardware
  A.2 Confirm and maintain software reliability
B. Management Policy
  B.1 Separate the functions of management and data entry
  B.2 Provide training for data entry personnel
  B.3 Have management personnel become familiar with the entire system including the specifics relating to the entry procedures
  B.4 Provide written instructions governing entry techniques
  B.5 Ensure the regularity of entering information at or near the time of the tranaction being recorded
C. Integrity and Security of the Database
  C.1 Develop and implement physical security measures
  C.2 Ensure accuracy and integrity of the database
D. Documentation of the Processing Program
  D.1 Prepare explicit documentation detailing the processing system used
E. Keeping or Destroying Backup Paper Records
  E.1 Establish the exact point in the processing system at which the raw data input forms will be destroyed (or establish that these are to be permanently retained)

Fig. 1. The admissibility methodology.

produce computer-generated records for trial, not just those who have recently converted to an automated office.

One of the limitations to codifying this set of guidelines into a formal methodology is that admissibility of computer-generated records is still governed by state law. Not all states have adopted Rule 803(6); this methodology, which focuses on meeting the requirements of Rule 803(6), does not address acceptance of the computer-generated evidence in those states that have dissimilar laws. However, it should enhance the chances for acceptance. Also, various factors affect the weight of any evidence that is admitted; although a few of these factors are mentioned, this paper is not meant to address this issue.

It should be emphasized that the authors do not intend for this methodology to be used without further consultation with legal counsel. These issues are presented for careful consideration during the planning stages of conversion. This methodology is presented as a guide for the inevitable discussions which must ensue before the conversion. Additionally, for those who have already begun the conversion, this methodology should generate immediate discussions with the corporate attorney relating to these issues.

5.1 Overview of the Methodology

The methodology consists of 11 specific items in 5 separate areas, which were developed specifically to reflect the requirements of Rule 803(6). These items are summarized in Figure 1, the admissibility methodology.

5.2 System Selection

Selection of the hardware and software for the office information system probably will be dictated by the planned uses of the office. However, along with the usual considerations of functionality (ease of use, cost, etc.) that the conversion planners typically take into account, reliability of the accuracy of the results produced by the system should also be considered (see part f of Rule 803(6)).

In the past, the choice of the complete system, both software and hardware, was often dependent on one or the other; choosing software from a given company meant that one had to use hardware from the same vendor, and vice versa. Today, it is possible to purchase hardware from one vendor, an operating system from another, a word processor from a third, a database management system from a fourth, etc. However, even though each portion of the system functions perfectly in some configurations, in a given configuration it might give unacceptable performance. Therefore, selection of such a hybrid system necessitates careful checking of the system; in addition to factors relating to the usefulness of the system, this can prevent either hardware or software vendors from later maintaining that any failure of the system is entirely the fault of the other vendor(s).

Any subsequent preparation of in-house software (or modifications to purchased software) must be integrated into the system with care. We think thorough retesting of the entire system is necessary whenever any such additions and/or modifications are made. In our opinion reliability of the accuracy of the output is one of the most important considerations with respect to future admissibility of computer-generated records.

5.2.1 *Hardware.* The first critical fact that must be established when attempting to introduce computer-generated records as evidence is the reliability of the hardware of the system. In the early years of computer use (i.e., at least until the 1960s), the failure rate of computer hardware was high enough to cause the courts much concern in this area [1]. By 1975, when the current version of Rule 803(6) was written, this issue was of much less concern. Thus the law was phrased in such a way that the opponent of someone attempting to introduce computer-related records must show that the system is such as to cause the records to lack trustworthiness; the proponent indicates trust in the system simply by accepting the output and using it in the business; however, the proponent should be prepared to refute any issues raised by the opponent in this regard.

5.2.2 *Software.* The other major consideration when selecting the system is the software. The issue to be addressed by the custodian or qualified witness offering the computer-generated records as evidence is that the "method or circumstances of preparation" of the records (i.e., the complete system used, including both the hardware and software) does not "indicate lack of trustworthiness" (see part f of Rule 803(6)). In other words, the software must be shown to be reliable. Software reliability has been defined by Glass as "the degree to which a system both satisfies its requirements and delivers useful services" [10]. Others often define the term to include the degree to which the requirements are satisfied as well [10, 12, 19]. Thus, the witness must show that the software has indeed satisfied the requirements of the business and delivered useful results, which should satisfy the court's requirements that the system must be trustworthy.

5.3 Management Policy

The management policy should encompass such procedures as division of tasks between management and entry personnel, personnel training (both data entry

and management), and the establishment of data entry techniques and regulations (including such facts as time of entry and the identity of the person making the entry).

5.3.1 *Separate Job Functions.* We believe that separating the functions of management and entry, with the attendant lack of information being given to the entry personnel, will help meet the requirement of the business records exception that the person involved must have no motive to misrepresent or misstate the facts.

The Shop-Book Rule requires that the printouts offered as evidence can only be accepted if the entry leading to the printouts was made by someone who has knowledge of the event (i.e., has general knowledge of the effects of the transactions on the business). At the federal level, this problem is somewhat alleviated. Under the Federal Rules of Evidence, lack of personal knowledge (concerning the event(s) being recorded) by the maker of the business entries may not be used to affect the admissibility of business records, only the weight of the evidence [17]. It is true that even in this case the entry must reflect information transmitted by a person with knowledge of the event. Therefore, even though we think that this separation of job functions might adversely affect the admissibility of computer-generated records in those states that still use the Shop-Book Rule, we think the overriding consideration should be that the separation of the two job functions makes it easier for the qualified witness to show accuracy and trustworthiness of the records in federal cases and in those states that have adopted the Federal Rules of Evidence.

The accuracy of the records is shown through the proper training of the data entry personnel and the enforcement of procedures established regarding the timely and methodical input of the data.

The trustworthiness of records is shown through the proper training of the management personnel and the completeness of that training. This showing of trustworthiness is required as part f of rule 803(6) and is usually done by the qualified witness as defined in part e of Rule 803(6).

5.3.2 *Data Entry Training.* Training of data entry personnel should include emphasis on accuracy of input and on following exact procedures established to be followed at time of input. They should be trained to notice unusual entries and to call these to the attention of the management personnel. We believe this training can then be reported by the qualified witness who is testifying that it was the regular practice of that business activity to make the memorandum, report, or data compilation being introduced.

5.3.3 *Management Training.* Management personnel should become familiar with the entire system, including the entry procedures; this will enable them to testify as qualified witnesses (see parts b and e of Rule 803(6)). In other words, the management personnel can then speak for the data entry personnel, both generically and individually. Also, this will enable the management personnel to authenticate the evidence (see Rule 901 of the Federal Rules of Evidence). According to Gemignani, the witness presenting the computer-generated records is not necessarily required to have personal knowledge of the basic data entered into the system or personal knowledge of the actual physical operation of the

data processing equipment, as long as he or she is familiar with the methods employed in processing the business records [9].

Additionally, having the management personnel become familiar with the total operation will help overcome one of the most common difficulties faced in laying a proper foundation for computer-generated evidence, that of establishing the relevance of the evidence. Fenwick states that it is important that the witness be familiar with the chain of events from those leading up to the recording of the computer-generated records being introduced through the production and use of those records. The witness must also know how the records are used by his or her company [7].

The system itself should be designed to flag and/or reject abnormal entries, which should be handled personally by management trained especially for this. This, too, will add to the overall showing of the trustworthiness of the printouts being offered as evidence.

5.3.4 *The Input Procedures.* The entering of data into the computer leading to the results shown on the computer-generated records being submitted must reflect current transactions and must be an established part of doing business (see parts a, c, and d of Rule 803(6)). Written procedures governing entry techniques and rules that ensure this should be established and enforced and should be used as a part of the training of data entry personnel.

A computer printout produced specifically for litigation "is not produced in the ordinary course of business, and is, in any case, sufficiently self-serving that it is highly unlikely that any court would permit it to be introduced by the party that prepared it, at least under the Business Records Exception to the Hearsay Rule" [9]. However, the "printout itself, which sets forth the business records, does not need to be prepared close to the time that the data [are] entered" [9]. Thus, we think the processing procedures should be extensive enough to allow for the future retrieval of printouts such as weekly reports of monthly reports that might be required to show the regular business activity.

5.4 Integrity and Security of the Database

In addition to the problems that can be caused by unreliable software, there are five other possible areas of concern affecting the integrity and security of the database: physical security problems, improper use of legitimate database operations, use of bit-level utility programs, improper deletion of data, and an inability to recover from crashes.

Implementation of security measures for protecting the database against the physical dangers of heat, cold, dust, etc., and against the ordinary dangers of tampering by unauthorized personnel will help ensure the integrity of the database. The extent of these security measures is another issue being addressed currently by computer scientists. The growing types and extent of computer crime have spawned extensive studies in this field [15]. However, these measures are not addressed in this paper.

Although it may become expedient under the pressure of deadlines to use legal database operations to improperly alter data that had previously been entered into the database, we believe that evidence of such alteration will negate the admissibility of any of the office records. For example, an insurance company

might have a practice of supplying each person presenting a claim with a copy of the records within two days of discharge from the hospital. A bill from the hospital differs from the insurance company records by some amount, say $875.32. This discrepancy could have been caused by the duplication of a $124.68 entry for anesthesia and a $1000 keypunch error. Entering a miscellaneous entry of $875.32 to balance the records is unjustified, even to meet the deadline. (This is just as true for an 8¢ error as it is for an $800.00 error; the 8¢ could represent two very large errors, one positive and one negative, which almost cancel each other out.) Strong preventative measures must be implemented to prevent this practice.

By using current computer hardware and software technology, it may be possible for personnel to alter portions of the database or the programs at some point in the system by means of bit-level utility programs to change bits on the storage medium, thus changing the values stored there. Company policy must be developed and enforced to prevent this practice.

Measures must be implemented to prevent personnel from deleting entries that should not be deleted. For example, if a friend of an employee has an outstanding balance, the employee should not be able to remove the record leading to the balance owed. This does not mean that entries should not be deleted from the database in the normal course of business. If such actions would be taken with paper records, the same actions are properly a part of doing business in an automated office (see part d of Rule 803(6)). For example, an insurance company might not maintain a paper file relating to a person who has canceled a policy that has no outstanding claims. Consequently, such computer-related records could also be eliminated. However, such elimination should be handled cautiously; for different types of businesses the required length of time for maintaining such a file will vary.

In some situations, the system might crash because of incorrect data being entered. There are standard database management techniques of rollback and recovery which should be a part of the overall system plan to be used when this happens. However, the way in which these techniques are used by the business should be documented, along with the characteristics of the system and other procedures.

5.5 Documentation of the Processing Program

Available documentation should completely define the processing of records that is done in the automated office. (This is in addition to the documentation required for training purposes.) The documentation should fully describe the system, addressing both the hardware and the software, including any programs purchased or any written in-house (as well as any modifications to any of these programs). It should also detail how each of the elements is used to process the records leading to the printout being offered as evidence. This will enable one person to act as custodian of the data or as a qualified witness, rather than having to call on a lengthy succession of witnesses to show a continuity of custodianship and concurrent knowledge of the processing being done at each step. Also, this one person could testify regarding entries made in the past by personnel no longer with the business.

Having the complete documentation should aid the qualified witness showing the reliability of the specific printout offered as evidence. Gemignani [9] explains

this in this way: "To show reliability, it must be shown that from entry to retrieval, there was sufficiently little chance of error or tampering that the evidence should at least be presented to the trier of the fact, be it judge or jury, who can then give it what weight and credibility they deem fitting."

5.6 Keeping or Destroying Backup Paper Records

Any paper records that actually form the basis for on-line records should not be destroyed before the accuracy of the on-line data has been confirmed; this accuracy can best be demonstrated by being electronically verified by personnel different from those who originally entered the data. After the records have been electronically verified and the reliability of the entire system has been established, we believe it is sufficient to maintain only the electronically stored records. Bear in mind that the conversion process is not instantaneous; we think that the actual paper records necessary to reenter the data should be kept until the reliability of the system actually meets the standards for the type of business being converted (e.g., when a business consistently produces a weekly report, there is no need to save these reports if they can be regenerated by reentering the original data, should the need for such reports arise).

6. SUMMARY

This paper describes a methodology of 11 items designed to ensure the court admissibility of computer-generated records from an automated office. These 11 items relate to the 5 aspects of conversion: system selection, management policy, database integrity and security, documentation, and maintenance of raw data. Each of the items of the methodology is designed to satisfy one or more of the requirements for admissibility of computer-generated records as given in the Federal Rules of Evidence and/or other evidence rules.

An excellent summary of the subject of admissibility of computer-generated records was given by Gemignani in *Law and the Computer*:

> As can be seen from the number and complexity of the areas that must be touched upon to lay the foundation for the introduction of such evidence, convincing the court of the reliability is not a trivial task. It is, therefore, very important that a business that keeps records by means of a computer thoroughly document and test its procedures so that if these records ever do need to be entered into evidence at a trial, the court can be given enough information to be satisfied that they are admissible. It may even be beneficial to have an attorney assist in setting up the computerized record keeping system so that any weak spots in the admissibility of records produced by the system can be identified and corrected before the business finds that a court will not accept its records as reliable. [9, p. 169]

Our hope is that other people will become interested in the admissibility of computer-generated records. Although we recognize the inherent dangers that those who are converting to an automated office must face, and although we realize that we have not given definitive answers, we feel that the ideas presented here should prepare them for the ensuing consultations with legal professionals.

ACKNOWLEDGMENTS

We would like to thank Marianne Wesson, Associate Professor of Law at the University of Colorado, and Alfred R. Cecil, M.B.A., J.D., who each reviewed this paper during its preparation. We would also like to thank Pat Richards, who

assisted with the library research for this paper, and Louis Coker, Engineering Manager, NBI, Inc., Boulder, Colo., who reviewed the methodology. Additionally, we thank the referees who offered extensive, constructive, and very useful suggestions for improving this article.

REFERENCES

1. Appropriate foundation requirements for admitting computer printouts into evidence. *Washington Univ. Law Quart. 1977* (Winter, 1977), 58–92.
2. BEQUAI, A. *Computer Crime.* Lexington Books, D.C. Heath and Co., Lexington, Mass., 1978, pp. 97–181.
3. BINDER, D. F. *Hearsay Handbook.* Shepard's/McGraw-Hill, Colorado Springs, Colo., 1983.
4. CLEARY E. W., ED. *McCormick's Handbook on the Law of Evidence*, 2nd ed. West, St. Paul, Minn., 1972.
5. *Computer Crime—Legislative Resource Manual.* Koba Associates, Inc.; prepared for the Bureau of Justice Statistics (BJS), U.S. Department of Justice (DOJ), 1980.
6. *Computer Crime—Criminal Justice Resource Manual.* Stanford Research Institute International; prepared for the Bureau of Justice Statistics (BJS), U.S. Department of Justice (DOJ), 1979.
7. FENWICK, W. How to get computer-based evidence admitted. In *Use of Computers in Litigation.* J. H. Young, M. E. Kris, and H. C. Trainor (Eds.), cosponsored by the Young Lawyers Division and the Section on Science and Technology of the American Bar Association, Chicago, Ill., 1979, pp. 329–340.
8. FENWICK, W. A., AND DAVIDSON, G. K. Admissibility of computerized business records. In *American Jurisprudence Proof of Facts*, 2nd ed., 14, 1977, pp. 173–251.
9. GEMIGNANI, M. *Law and the Computer.* CBI Publ. Co., Boston, Mass., 1981.
10. GLASS, R. L. *Software Reliability Guidebook.* Prentice-Hall, Englewood Cliffs, N.J., 1979.
11. KING, R., AND STANLEY, C. C. An informal conversion methodology for ensuring the court admissibility of computer generated records. In *Proceedings of the IEEE 1st International Conference on Office Automation* (New Orleans, La., Dec. 17–19), R. W. Taylor, Ed. IEEE, New York, 1984.
12. KOPETZ, H. *Software Reliability.* Springer-Verlag, New York, 1979.
13. LOUISELL, D. W., ET AL. *Federal Evidence, Vol.* 4. The Lawyers Co-Operative Publ. Co., Rochester, N.Y., 1980, pp. 387–402.
14. MYERS, G. T. *The Art of Software Testing.* Wiley, New York, N.Y., 1979.
15. PARKER, D. *Fighting Computer Crime.* Scribner's Sons, New York, N.Y., 1983.
16. RIGGS, P. Computer evidence: What is it and what is allowed?, Brigham Young University, 1983. (Scheduled for publication in *Utah Bar J.*, 1985.)
17. SOMA, J. T. *Computer Technology and the Law.* Shepard's/McGraw-Hill, Colorado Springs, Colo., 1983, pp. 290–295.
18. TAPPER, C. *Computers and the Law*, Weidenfeld and Nicolson, London. 1973, pp. 17–34.
19. WASSERMAN, A. I., AND FREEMAN. P. Software engineering education needs and objectives. In *Proceedings of an Interface Workshop*, Springer-Verlag, New York, 1976.

Received February 1985; revised September 1985; accepted September 1985