PEPPERDINE UNIVERSITY

Pepperdine Law Review

Volume 13 | Issue 2 Article 6

1-15-1986

The Discovery and Use of Computerized Information: An Examination of Current Approaches

Richard M. Long

The Discovery and Use of Computerized Information: An Examination of Current Approaches

In recent years, the legal profession has run head on into the increasing use of computers and computerized information. Discovery and evidentiary rules developed to deal with written documentation may not be flexible enough to adequately cover this relatively new method of storing information. This comment examines various methods by which courts have attempted to deal with discovery and evidentiary problems involving computerized information, and suggests certain areas that should be explored in supporting or attacking the credibility of such information.

I. INTRODUCTION

The increasing importance of computers in society has had an inevitable effect on the legal profession. Technological advances relating to computers have presented such novel legal issues as the possibilities of patent, copyright, and trade secret protection for software.[1] Computers offer the potential for increasing efficiency and productivity within the practice of law.[2] Computers also present special concerns as to the manner in which litigation is conducted. Computerized information is unique. The computer stores in a format different from that of the traditional manual business record or file cabinet. It lacks many of the guarantees of reliability found in traditional methods of storing information. Computerized information involves new technology and new terminology, both of which can be confusing and distracting to a court or practitioner. It offers the possibility of being able to analyze large amounts of data while also increasing the possibility of unnecessarily disclosing information. Computers offer new and often complicated ways of presenting evidence while doing little to decrease the possibility that such methods will be used to mislead.

This comment addresses some of the problems that will likely be encountered in dealing with the discovery and use of computer-gen-

1. Lynch, *The Hot New Areas of Law Practice*, A.B.A. J., Oct. 1984, at 72.

2. *See* Blodgett, *The Gospel of Computers According to Bernstein*, A.B.A. J., June 1984, at 70; Frost, *Automating Real Estate Closings*, A.B.A. J., Aug. 1984, at 156; Goldstein, *Law Firm Time-and-Billing Systems Compared*, A.B.A. J., June 1984, at 137; Grumer, *The Paper Chase: Managing Your Records*, A.B.A. J., Sept. 1984, at 74; Harrington, *High Marks for Computerized Research*, A.B.A. J., Sept. 1984, at 153; Naisbitt, *Megatrends For Lawyers and Clients*, A.B.A. J., June 1984, at 45.

erated evidence. The first part of this comment focuses on how computer technology has generally affected the discovery of different types of computer-generated information. The second part deals with some of the evidentiary hurdles that will likely be encountered in trying to admit computer-generated evidence. The third part will deal with factors to consider when attacking or supporting the credibility of computer-generated evidence.

II. DISCOVERY PROBLEMS

A. Discovery of Computer-Related Information

Discovery principles should generally apply to computerized information. However, the differences between discovery of manually-generated records and computer-generated records should be noted. These differences include the method in which computerized information is stored, the ability to deal with large amounts of information, and the lack of an audit trail in verifying information.

The problems presented by the discovery of computerized information are partially due to the media in which the information is stored, typically magnetic tape or disc. Because information stored in such forms is nearly impossible to understand without some sort of printout, courts can probably compel the production of a printout.[3] It remains unclear whether a party can compel the production of information stored in a different medium. Where a large amount of information is involved, it may be more convenient to produce the information in a machine-readable form rather than, or in addition to, a computer printout. Several courts have expressed a willingness to order the production of information in machine-readable form.[4]

The computer's ability to manipulate large amounts of data removes many of the practical difficulties inherent in discovering large amounts of information. As computers broaden the already liberal scope of discovery, the danger of unnecessarily disclosing sensitive information increases. Both the discovering and the responding parties must focus their attention on the purposes for which the discovery is sought and the nature of the information sought. For example, it would not be unusual in a complicated case for one party to

---

3. FED. R. CIV. P. 34(a) provides in part:

> Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on his behalf, to inspect and copy, any designated documents (including writings, drawings, graphs, charts, photographs, phono-records, and other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form) . . . .

4. *See, e.g.*, Fauteck v. Montgomery Ward & Co., 91 F.R.D. 393, 389-99 (N.D. Ill. 1980); National Union Elec. Corp. v. Matsushita Elec. Indus. Co., 494 F. Supp. 1257, 1262 (E.D. Pa. 1980); Adams v. Dan River Mills, Inc., 54 F.R.D. 220, 221-22 (W.D. Va. 1972).

seek another party's entire data base. The responding party in such a case should question the relevancy of the entire data base. Where programming or data processing procedures are being sought, instead of the underlying data itself, courts should allow production only where the program or procedure itself is in issue[5] or where the reliability of the system is in question.[6] Even where this information is relevant, it may be privileged[7] or work product opinion.[8] The information may also be protected by considerations of privacy,[9] or may fall under traditional trade secret protection.[10] In any such case, a protective order should be considered.[11]

Perhaps the most important difference between computerized and manually-generated information is the lack of an audit trail.[12] Since information within a data base can be changed or destroyed without leaving a trace, circumstantial evidence must be used to verify information contained within the system. In the absence of an audit trail,

---

5. *See, e.g.*, Dunn v. Midwestern Indem., 88 F.R.D. 191, 195 (S.D. Ohio 1980) (racially discriminatory standards were allegedly programmed into defendant's computers).

6. Because reliability of the computer system is such an important factor in evaluating the credibility of evidence produced by the system, the reliability of the system will commonly be in question. Thus information concerning the equipment, procedures, and programming used to produce the information should be discoverable. Several courts have recognized the impeaching party's need to obtain information through pretrial discovery concerning the accuracy of procedures for inputting and processing the information. *See, e.g.*, United States v. Liebert, 519 F.2d 542, 547-48 (3d Cir.), *cert. denied*, 423 U.S. 985 (1975); United States v. Russo, 480 F.2d 1228, 1241 (6th Cir. 1973), *cert. denied*, 414 U.S. 1157 (1974); United States v. Dioguardi, 428 F.2d 1033, 1038 (2d Cir.), *cert. denied*, 400 U.S. 825 (1970).

7. FED. R. CIV. P. 26(b)(1) provides for "discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action . . . ."

8. FED. R. CIV. P. 26(b)(3) provides in part that even where material prepared by an opposing party in anticipation of trial is ordered produced, "the court shall protect against disclosure of mental impressions, conclusions, opinions, or legal theories of the attorney or other representative of a party concerning the litigation." *Id.*

9. *See, e.g.*, United States v. Liebert, 519 F.2d 542 (3d Cir.), *cert. denied*, 423 U.S. 985 (1975) (computer list of tax nonfilers relevant for showing the accuracy and reliability of IRS computer system, but not discoverable because of privacy concerns and the presence of alternative methods of securing the same information).

10. *See, e.g.*, United States v. IBM Corp., 67 F.R.D. 40, 46-47 (S.D.N.Y. 1975) (trade secret requirements applied to computerized sales data).

11. *See, e.g., id.* (sealed protection for revenue, sales, and manufacturing data and for expert testimony denied). *But see* Zenith Radio Corp. v. Matsushita Elec. Indus. Co., 529 F. Supp. 866 (E.D. Pa. 1981) (sealed protection for sales data approved).

12. "The *audit trail* is the accumulation of *source documents and records* maintained by the client which are the support for the transactions that occurred during the period. It includes such things as duplicate sales invoices, vendor's invoices, canceled checks, general and subsidiary ledgers, and all types of journals." A. ARENS & J. LOEBBECKE, AUDITING: AN INTEGRATED APPROACH 440 (1980).

more emphasis must be placed on data input and retrieval procedures. The adequacy of protections against equipment failure and unauthorized use are also important points of inquiry. Any weaknesses discovered will prove valuable in arguing against the admissibility and credibility of any computer-generated evidence.[13]

Various courts have recognized the aforementioned changes and have adopted flexible approaches for dealing with the discovery of computer-related information. Where the required information is difficult to isolate and produce, the responding party may be required to assist in the search for information by providing someone knowledgeable with the system,[14] or by writing programs to aid in the search of the system and the accumulation of data.[15] Where actual data processed through the system is sought for purposes of impeaching the accuracy of the system, and for some reason cannot be produced, actual testing of the system may be a viable alternative.[16]

While computers may increase discovery costs as illustrated above, the principles for allocating such costs should not change. The burden of producing the evidence will usually remain on the responding party, although the court retains the power to prevent abuse.[17] In practice, the willingness of the courts to allow the discovery of computerized information has been matched by a tendency to place its costs on the party seeking discovery.[18] The power to allocate costs remains largely within the discretion of the trial court,[19] although there are limits.[20]

B. Discovery of Litigation Support Systems

Because computerized litigation support systems[21] are developed in

---

13. *See infra* notes 101-21 and accompanying text.

14. *See, e.g.*, Greyhound Computer Corp. v. IBM Corp., 3 Computer L. Serv. Rep. 138 (D. Minn. 1971).

15. *See, e.g.*, Bell v. Automobile Club of Mich., 80 F.R.D. 228 (E.D. Mich. 1978), *appeal dismissed*, 601 F.2d 587 (6th Cir.), *cert. denied*, 442 U.S. 918 (1979).

16. *See, e.g.*, United States v. Liebert, 519 F.2d 542 (3d Cir.), *cert. denied*, 423 U.S. 985 (1975).

17. *See infra* note 20.

18. *See, e.g.*, Adams v. Dan River Mills, Inc., 54 F.R.D. 220, 222 (W.D. Va. 1972); Pearl Brewing Co. v. Joseph Schlitz Brewing Co., 415 F. Supp. 1122, 1141 (S.D. Tex. 1976).

19. *See, e.g.*, United States v. Davey, 543 F.2d 996 (2d Cir. 1976) (refusal to place duplication costs on the discovering party).

20. *See, e.g.*, Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340 (1978) (reversed lower court ruling placing costs of over $16,000 incurred in retrieving computerized information on the responding party).

21. In general terms, a computerized litigation support system replaces "the trial notebooks, tab locators, or card indexes which lawyers have long used to find relevant material in the mass of pretrial pleadings, discovered information, interviews, affidavits, legal research, and transcripts of hearings." Sherman & Kinnard, *The Development, Discovery, and Use of Computer Support Systems in Achieving Efficiency in Litigation*, 79 COLUM. L. REV. 267, 268-69 (1979). *See also* Goodrich, *Lawyers' Consider-*

preparation for litigation, their discovery falls under the provisions of Federal Rule of Civil Procedure 26(b)(3).[22] If the discovering party can demonstrate substantial need[23] of the materials and an inability to obtain the substantial equivalent of the materials without undue hardship,[24] then the question arises whether a computerized litigation support system will be protected by the work product rule.[25]

There are several ways in which discovery of an opponent's computerized litigation support system could reveal attorney's work product opinion.[26] The method of indexing documents could reveal an attorney's work product opinion, especially where the documents are arranged as to issues rather than objective terms, such as dates, names, and places.[27] Although parties could conceivably try to index on the basis of subjective criteria alone, this will not likely succeed because the benefits of a versatile information retrieval system would be lost.[28] Where both subjective and objective criteria are used to index, the responding party could still be compelled to retrieve documents using the objective criteria. Where documents are

ations and Requirements for Systems Support During Discovery, 14 JURIMETRICS J. 5 (1974) (special issue); Halladay, *Anatomy of an Automated Lawsuit,* 3 LITIGATION 13 (Spring 1977); Halverson, *Coping With the Fruits of Discovery in the Complex Case — The Systems Approach to Litigation Support,* 44 ANTITRUST L.J. 39 (1975); Olson, *Lawyers' Considerations and Requirements for Systems Support During Trial Preparation and Conduct,* 14 JURIMETRICS J. 20 (1974) (special issue); Olson & Goodrich, *Litigation Support Systems — Present Status and Future Use,* 11 FORUM 832 (1976); Prendergast, *The Use of Data Processing in Litigation,* 17 JURIMETRICS J. 227 (1977); Rust & Rome, *The Combination of a Manual and an Automated Approach to Trial Preparation,* 11 FORUM 810 (1976); Sanders, *Employment of Litigation Support Systems in Preparation of a Products Liability Case,* 11 FORUM 918 (1976); Sidney, *A Trial Lawyer's Solution to an Age-Old Problem Using a High-Speed Idiot With a Long Memory,* 11 FORUM 865 (1976); Turner, *The Employment of Modern Techniques and Technology in Trial Preparation,* 11 FORUM 797 (1976); Vovakis, *Litigation File Management: Preparation for Trial,* 11 FORUM 820 (1976).

22. FED. R. CIV. P. 26(b)(3) provides that materials prepared in anticipation of litigation can be discovered "only upon a showing that the party seeking discovery has substantial need of the materials in the preparation of his case and that he is unable without undue hardship to obtain the substantial equivalent of the materials by other means." *Id.*

23. *See* 8 C. WRIGHT & A. MILLER, FEDERAL PRACTICE AND PROCEDURE § 2025, at 211-28 (1972 & Supp. 1985); Sherman & Kinnard, *supra* note 21, at 274-76.

24. *See supra* note 23.

25. The protection of an attorney's work product is provided for in FED. R. CIV. P. 26(b)(3). Where discovery of trial preparation materials is ordered, that section states in part that "the court shall protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of an attorney or other representative of a party concerning the litigation." *Id.*

26. Sherman & Kinnard, *supra* note 21, at 284-90.

27. *Id.* at 286-87.

28. *Id.*

summarized, the content of a summary stored within the system may reveal work product opinion.[29] The dangers present in allowing discovery of systems that use summaries or subjective indexing can be minimized by disclosing only the identity of documents within the system.[30] Although identification of the documents alone may reveal work product opinion, this argument is unpersuasive. Placing a document within a litigation support system should not automatically make that document the subject of work product opinion, and should not prevent the disclosure of the identity of documents.[31]

Although there are few cases on point,[32] once the substantial need and undue hardship requirements are met, materials within opponent's litigation support system should be discoverable. Discovery of entire documents should be allowed where the system is little more than a repository for miscellaneous documents. Where an attorney for the responding party is heavily involved in the system's design and implementation, discovery should be restricted. However, the mere identity of documents within the system should still be discoverable. The work product privilege should not come into play where one side is seeking to facilitate discovery by having the opposing party use its litigation support system in the production of a document.

C. Discovery of an Opponent's Experts

Pretrial discovery is perhaps the main tool in the effort to discredit an opponent's computerized evidence, especially when this information comes in the form of models and simulations prepared by an expert.[33] Under the Federal Rules of Evidence, an expert is not required to disclose on direct examination the basis for his opinion.[34] The expert can also base his opinion on evidence, which might otherwise be inadmissible,[35] such as a model. These rules, together with

---

29. *Id.* at 287-90.

30. *Id.* at 287.

31. *See, e.g.*, United States v. AT&T, 461 F. Supp. 1314, 1339 n.76 (D.D.C. 1978) (court suggested that the document selection process might not constitute work product within the meaning of FED. R. CIV. P. 26(b)(3)).

32. *See In re* IBM Peripherals, 5 Computer L. Serv. Rep. 878 (N.D. Cal. 1975) (discovery of defendant's computerized litigation support system barred). For criticism of this decision, see Comment, *Computer Discovery in Federal Litigation: Playing by the Rules*, 69 GEO. L.J. 1465, 1475 (1981); *see also* Sherman & Kinnard, *supra* note 21, at 276-78.

33. *See, e.g.*, Shu-Tao Lin v. McDonnell Douglas Corp., 574 F. Supp. 1407 (S.D.N.Y. 1983), *rev'd*, 742 F.2d 45 (2d Cir. 1984) (limitation on discovery of computer program used to form opinion by plaintiff's expert partly responsible for reversal).

34. FED. R. EVID. 703 states: "The expert may testify in terms of opinion or inference and give his reasons therefor without prior disclosure of the underlying facts or data, unless the court requires otherwise. The expert may in any event be required to disclose the underlying facts or data on cross-examination." *Id.*

35. FED. R. EVID. 705 states:

the notion that cross-examination is an effective means of discrediting an expert witness, place the burden of being sufficiently informed on the opposing party in order to conduct an effective cross-examination. In light of the sophisticated nature of some computer models,[36] this knowledge must be gained through pretrial discovery, preferably conducted with the aid of an expert.

The clearest situation illustrating when discovery of an opponent's experts will be allowed occurs when the expert plans to present at trial conclusions based upon computer models and simulations. In order to properly challenge an expert's conclusions, some commentators have suggested that the opposing party should be given access to the underlying data used by the model, the programs used to manipulate the data, and the theories upon which the system is premised.[37]

Courts will not, however, necessarily grant this right to the opposing party. In *Perma Research & Development v. Singer Co.*,[38] the district court allowed expert testimony based on a computer simulation without requiring that programs and theories involved in the simulation be disclosed prior to trial. Although the case was upheld on appeal, the appellate decision is often noted for Justice Clark's comment:

> [I]t might have been better practice for opposing counsel to arrange for the delivery of all details of the underlying data and theorems employed in these simulations in advance of trial to both avoid unnecessarily belabored discussion of highly technical, tangential issues at trial, Fed.R.Civ.P. 26(b)(4)(A), and protect truly propietary [sic] aspects of the programs.[39]

Also noteworthy is Judge Van Graafeiland's vigorous dissent.[40]

Where discovery of an expert is allowed, the discovering party is usually given wide latitude. While Federal Rule of Civil Procedure 26(b)(4) names interrogatories as the usual methodology of discovery,[41] it also provides for any other means of discovery as the court

---

> The facts or data in the particular case upon which an expert bases an opinion or inference may be those perceived by or made known to him at or before the hearing. If of a type reasonably relied upon by experts in the particular field in forming opinions or inferences upon the subject, the facts or data need not be admissible in evidence.

36. *See, e.g.*, Harper, *Computer Evidence is Coming*, A.B.A. J., Nov. 1984, at 80 (computer-simulated reenactment of auto accident admitted as evidence to prove that the defendant was not driving).

37. 8 C. WRIGHT & A. MILLER, FEDERAL PRACTICE AND PROCEDURE § 2218, at 660 (1970). 1-pt.2 J. MOORE, MOORE'S FEDERAL PRACTICE, MANUAL COMPLEX LITIGATION, ¶ 2.715 (2d ed. 1984).

38. 542 F.2d 111 (2d Cir.), *cert. denied*, 429 U.S. 987 (1976).

39. *Id.* at 115.

40. *Id.* at 116 (Van Graafeiland, J., dissenting).

41. FED. R. CIV. P. 26(b)(4)(A)(i).

deems appropriate.[42] Reports, notes, and other memoranda are probably subject to discovery, although the discovering party may have to bear the costs.[43] The discoverability of expert information is one of the reasons why it has been suggested that communications with an expert, especially one who will testify at trial, should be limited.[44]

Where an opponent retains an expert in anticipation of litigation, but he is not expected to be called as a witness at trial, the discoverability of information relating to the expert is not as clearly defined. Although at least one commentator has described such an expert as "largely immune" from discovery, there are situations where discovery will be allowed. In *Pearl Brewing Co. v. Joseph Schlitz Brewing Co.*,[45] plaintiffs sought to prove anticompetitive conduct and constructed a model simulating the beer industry in Texas. The model was to be used by plaintiff's expert economist, Dr. Massy. The court ordered that all documentation of the system be produced. The court also allowed the discovery of two experts whom plaintiffs did not intend to call at trial. The court analyzed Federal Rule of Civil Procedure 26(b)(4) and found that the "exceptional circumstances" necessary to justify the discovery of nontrial experts existed in the case. Factors contributing to this finding included: the inability of the trial expert to provide information as to the programming used in the system; the close relationship between the information known by the nontrial experts and the conclusions to which the trial expert was expected to testify; and the absence of improper motive[46] on the part of the discovering party.

It is arguable whether experts can be questioned about alternative systems which will not be used at trial. The court in *Pearl* allowed such discovery with respect to trial experts. The court applied the "exceptional circumstances" analysis to the question of whether nontrial experts can be so questioned, and denied discovery. The court held that the discovering party must first show that the information sought is not otherwise obtainable through the trial expert.[47]

---

42. FED. R. CIV. P. 26(b)(4)(A)(ii).

43. Quadrini v. Sikorsky Aircraft Div., United Aircraft Corp., 74 F.R.D. 594 (D. Conn. 1977).

44. *See* Daniels, *Managing Litigation Experts*, A.B.A. J., Dec. 1984, at 64.

45. 415 F. Supp. 1122, 1137-40 (S.D. Tex. 1976).

46. Examples of improper motive include the desire to avoid the cost of compensating expert witnesses and the desire to develop one's own case entirely from the mouth of an opponent's experts. *Id.* at 1138.

An assumption running throughout the present analysis is that the information sought cannot otherwise be independently obtained without expending inordinate amounts of time, money, or resources. *Id.*

47. *Id.* at 1140.

III. EVIDENTIARY PROBLEMS

A. Hearsay Rule and the Business Records Exception

Because computer-generated records are hearsay,[48] they are inadmissible as evidence unless they fall under an exception to the hearsay rule.[49] While this comment focuses on the business records exception,[50] other possible exceptions are worth noting. Where information from a party's own computer is offered against that party, it may be considered an admission by a party-opponent.[51] Where the information originates from computers belonging to a public office or agency, it may be considered a public record.[52] Information which

48. FED. R. EVID. 801(c) states: "Hearsay is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted."

49. Under FED. R. EVID. 802, "[h]earsay is not admissible except as provided by these rules or by other rules prescribed by the Supreme Court pursuant to statutory authority or by Act of Congress." *See generally* Roberts, *A Practitioner's Primer on Computer-Generated Evidence*, 41 U. CHI. L. REV. 254 (1974); Comment, *A Reconsideration of the Admissibility of Computer-Generated Evidence*, 126 U. PA. L. REV. 425 (1977).

50. The business records exception to the hearsay rule is embodied in FED. R. EVID. 803(6), which states:

> 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.

51. FED. R. EVID. 801(d)(2)(B). For an example of an application of this rule, see Leone v. Precision Plumbing & Heating of S. Ariz., Inc., 121 Ariz. 514, 591 P.2d 1002 (1979). Plaintiff sued to recover on an alleged oral contract which provided for a bonus of one half the difference between the estimated and actual cost of a construction project. In holding that printouts, which were supplied on a weekly basis by the defendant and which compared costs to date with total estimated costs, were admissible as admissions by a party-opponent, the court stated: "[u]nlike a business record, where admissibility turns on reliability of the processes which generate the record, . . . an admission is admissible regardless of reliability; it need only have been made by and offered against a party-opponent." *Leone*, 121 Ariz. at 516-17, 591 P.2d at 1004-05 (citation omitted).

52. FED. R. EVID. 803(8) states:

> 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

fails to meet the requirements of any of the other exceptions but nevertheless contains circumstantial guarantees of trustworthiness may fall within the residual exception.[53]

Although computerized records are clearly encompassed by the business records exception,[54] such records do necessitate a different emphasis in the application of the exception. The basic requirements of the rule still apply. However, courts must pay more attention to the reasons behind the exception. The business records exception is based upon the premise that records kept, and relied on, in the normal course of business bear sufficient guarantees of trustworthiness to justify an exception to the hearsay rule.[55] As the form of the record changes from manual to electronic, the inherent guarantees of reliability also change.[56] Various methods of insuring reliability must be examined in light of these changes. The elements of the rule must be applied flexibly and with these considerations in mind.

Mechanical application of the "at or near the time" requirement might work to bar the introduction of computer records despite other indicia of trustworthiness. Where a computer printout was not made soon after data was entered into the system, the record was arguably not made "at or near the time" of the transaction. The better view, and one which has been adopted by a number of courts, is that the timeliness requirement applies primarily to the time at which the information was entered into the system.[57] Several commentators have

---

law, unless the sources of information or other circumstances indicate lack of trustworthiness.

53. FED. R. EVID. 803(24) states:

> A statement not specifically covered by any of the foregoing exceptions but having equivalent circumstantial guarantees of trustworthiness, if the court determines that (A) the statement is offered as evidence of a material fact; (B) the statement is more probative on the point for which it is offered than any other evidence which the proponent can procure through reasonable efforts; and (C) the general purposes of these rules and the interests of justice will best be served by admission of the statement into evidence. However, a statement may not be admitted under this exception unless the proponent of it makes known to the adverse party sufficiently in advance of the trial or hearing to provide the adverse party with a fair opportunity to prepare to meet it, his intention to offer the statement and the particulars of it, including the name and address of the declarant.

For an argument that the residual exception may provide a method for admitting computer-generated evidence, see Comment, *Guidelines for the Admissibility of Evidence Generated by Computer for Purposes of Litigation,* 15 U.C.D. L. REV. 951, 966-68 (1982).

54. "The expression 'data compilation' is used as broadly descriptive of any means of storing information other than the conventional words and figures in written or documentary form. It includes, but is by no means limited to, electronic computer storage." FED. R. EVID. 803(6) advisory committee note.

55. *See* M. GRAHAM, EVIDENCE, TEXT, RULES, ILLUSTRATIONS AND PROBLEMS 190 (1983).

56. *See, e.g.,* Sprowl, *Objecting to Computerized Business Records,* A.B.A. J., Dec. 1984, at 128.

57. United States v. Russo, 480 F.2d 1228, 1240 (6th Cir. 1973), *cert. denied,* 414

suggested that the "at or near the time" requirement is irrelevant to computer-generated records.[58] There is nothing inherently unreliable about information stored electronically in a computer's memory for a period of time before a printout is made. The amount of time between input and printout could possibly have a bearing on reliability; a longer period may increase the possibility of errors or tampering. However, the duration of time passage alone should not prevent computer records from being admitted.

Because it is anticipated that foundational requirements with respect to computerized records will be met through the testimony of a "person with knowledge,"[59] the extent to which the witness must be familiar with the data and with the system has been the subject of litigation. The witness need not have personal knowledge of the subject matter of the transaction.[60] It is not necessary that the witness was the custodian at the time the record was made,[61] or that the witness was employed at the time the record was made,[62] or that the witness was personally involved in the production of the printout.[63] The key factor determining sufficiency of the custodian's testimony is his familiarity with the business and its practices for making, maintaining, and retrieving records.[64] The witness must provide foundation adequately insuring the reliability of the system producing the record.[65] Where a custodian or other qualified witness is not available, an adequate foundation may be established by other means.[66]

U.S. 1157 (1974) (to hold that computer product and input must be produced at or within a reasonable time of the transaction would too severely restrict the admissibility of computerized records).

58. *See* Younger, *Computer Printouts in Evidence: Ten Objections and How to Overcome Them*, 2 LITIGATION 28, 29 (Fall 1975); Note, *Appropriate Foundation Requirements for Admitting Computer Printouts into Evidence*, 1977 WASH. U.L.Q. 59.

59. *See supra* note 50.

60. *See* M. GRAHAM, *supra* note 55, at 193-94.

61. *Id.*

62. *Id.*

63. *See* American Oil Co. v. Valenti, 179 Conn. 349, 357-60, 426 A.2d 305, 309-11 (1979). The court reviewed previous cases for an indication of the proper qualifications of the foundational witness and decided that the witness should have some computer expertise to enable him to testify accurately regarding the system producing the evidence. "What is crucial is not the witness' job description but rather his knowledgeability about the basic elements that afford reliability to computer print-outs." *Id.* at 360, 426 A.2d at 311.

64. *Id.* at 361, 426 A.2d at 311.

65. *Id.* at 360, 426 A.2d at 311. *See infra* notes 101-21 and accompanying text.

66. *See* Zenith Radio Corp. v. Matsushita Elec. Indus. Co., 505 F. Supp. 1190, 1236 (E.D. Pa. 1980) ("[I]n the absence of a 'custodian or other qualified witness,' plaintiffs must show regularity of practice in some precise and explicit manner, either by external evidence or from the documents themselves plus surrounding circumstances.").

In some situations, it may be necessary to rely upon the content of the statement itself as evidence of the witness' personal knowledge.[67]

In addition to the normal foundational requirements for business records,[68] the admission of computerized records requires that a sufficient foundation of trustworthiness be established.[69] Courts have disagreed as to what constitutes a sufficient foundation for computerized business records.[70] In general, certain features common to most

---

67. M. GRAHAM, *supra* note 55, at 195.

68. *Id.* at 189-204.

69. *See supra* note 58.

70. Beyond the application of the usual requirements for business records, foundational requirements for computer-generated business records have varied widely. A case often cited is King v. State *ex rel.* Murdock Acceptance Corp., 222 So. 2d 393 (Miss. 1969). That case stated:

> [P]rint-out sheets of business records stored on electronic computing equipment are admissible in evidence if relevant and material, without the necessity of identifying, locating, and producing as witnesses the individuals who made the entries in the regular course of business if it is shown (1) that the electronic computing equipment is recognized as 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 satisfes [sic] the court that the sources of information, method and time of preparation were such as to indicate its trustworthiness and justify its admission.

Id. at 398. This formulation is not very helpful because standard equipment is difficult to define in an area of rapid technological advances, and because the second and third requirements add little to the customary requirements for business records. *See* Note, *supra* note 58, at 84-85 (various formulations of foundational requirements criticized). Nevertheless, *King* has been followed in some jurisdictions. *See, e.g.,* Missouri Valley Walnut Co. v. Snider, 569 S.W.2d 324, 328 (Mo. Ct. App. 1978).

Other courts have also used formulations that are not really helpful in setting admissibility standards for computer-generated evidence. *See, e.g.,* State v. Springer, 283 N.C. 627, 197 S.E.2d 530 (1973). The *Springer* court held that:

> [P]rintout cards or sheets of business records stored on electronic computing equipment are admissible in evidence, if otherwise relevant and material, if: (1) the computerized entries were made in the regular course of business, (2) at or near the time of the transaction involved, and (3) a proper foundation for such evidence is laid by testimony of a witness who is familiar with the computerized records and the methods under which they were made so as to satisfy the court that the methods, the sources of information, and the time of preparation render such evidence trustworthy.

Id. at 636, 197 S.E.2d at 536.

Cases following the *Springer* decision include State v. Hunnicutt, 44 N.C. App. 531, 261 S.E.2d 682 (1980); State v. Rodgers, 49 N.C. App. 403, 271 S.E.2d 535 (1980); State v. Passmore, 37 N.C. App. 5, 245 S.E.2d 107, *cert. denied,* 295 N.C. 556, 248 S.E.2d 734 (1978).

Courts have frequently forsaken structured requirements and simply taken various facts into account to determine whether the foundational requirement of trustworthiness has been met. *See, e.g.,* Reisman v. Martori, Meyer, Hendricks & Victor, 155 Ga. App. 551, 271 S.E.2d 685 (1980); Westinghouse Elec. Supply Co. v. B.L. Allen Inc., 138 Vt. 84, 413 A.2d 122 (1980); Roderick Timber Co. v. Willapa Harbor Cedar Products, Inc., 29 Wash. App. 311, 627 P.2d 1352 (1981); State v. Smith, 16 Wash. App. 425, 558 P.2d 265 (1976).

The decision in United States v. Russo, 480 F.2d 1228 (6th Cir. 1973), *cert. denied,* 414 U.S. 1157 (1974), is an excellent example of a court considering the problems inherent in computer-generated evidence. The court stated: "[T]he foundation for admission of such evidence consists of showing the input procedures used, the tests for accuracy and

computerized information should be addressed.[71] Evidence should be produced concerning the controls dealing with the input of information into the system, programs and equipment used in processing the data, security of the data processing center and the data base, and integrity of the output.[72]

B. The Best Evidence Rule

The best evidence rule mandates a preference for the production of the original where a party seeks to prove the contents of a writing.[73] The application of the best evidence rule to computerized information presents some conceptual problems, and has generated discussion by various commentators.[74] The rule should not, however, provide a major obstacle to the admission of computerized evidence.[75]

The "original" of a computer-generated record is arguably the electronic pattern found in the computer's memory. A litigant could argue that a printout represents a translation of this pattern into readable form; thus it is not the original and should be excluded.[76] However, this argument is weak because it is virtually impossible to understand computerized information without a printout.[77] The Federal Rules solve this problem by taking the position that the electronic pattern in a computer's memory constitutes a "writing"[78] and therefore defines a printout as an "original."[79]

---

reliability and the fact that an established business relies on the computerized records in the ordinary course of carrying on its activities." *Russo*, 480 F.2d at 1241. *See* Note, *supra* note 58, at 88-90 (arguing that even the *Russo* court did not go far enough in testing the reliability of the computer printouts).

71. *See generally* Fenwick & Davidson, *Use of Computerized Business Records as Evidence*, 19 JURIMETRICS J. 9, 18 (1978).

72. For a more detailed discussion of the evaluation of such controls, see *infra* notes 101-121 and accompanying text.

73. FED. R. EVID. 1002 states: "To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as provided in these rules or by Acts of Congress."

74. *See infra* note 76.

75. *See generally* 5 D. LOUISELL & C. MUELLER, FEDERAL EVIDENCE § 551 (1981).

76. *See* Younger, *supra* note 58, at 28, 29-30; Fenwick & Davidson, *supra* note 71, at 13-14.

77. *See, e.g.*, King v. State *ex rel.* Murdock Acceptance Corp., 222 So.2d 393, 398 (Miss. 1969) ("In admitting the print-out sheets reflecting the record stored on the tape, the Court is actually following the best evidence rule.").

78. FED. R. EVID. 1001(1) states: " '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."

79. FED. R. EVID. 1001(3) provides in part: "If data are stored in a computer or

A litigant might also argue that where information in a computer has been input from paper records, these records themselves constitute the best evidence and should be produced.[80] Even assuming that these records constitute the "originals," both the common law and the Federal Rules allow secondary evidence where the originals cannot be obtained,[81] such as where paper records are destroyed in the normal course of business.[82] Where the original paper records are still available, both the common law and the Federal Rules provide an exception for voluminous data.[83] Whether the content of a writing is actually being "proved" is one of the more difficult conceptual areas of the best evidence rule, and one where litigants occasionally stumble. Where the computer record is merely corroborative, the best evidence rule is not involved; the transaction can be proven by other means.[84] Where the evidence is based solely on the printout, the printout must be produced unless its absence can be adequately explained.[85]

---

similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original'."

It has been suggested that FED. R. EVID. 1001(3) should be construed to require only the minimal showing that the data was not altered during printout, and that the broader questions of reliability should be discussed in the context of hearsay and authentication requirements. 5 D. LOUISELL & C. MUELLER, *supra* note 75, § 557.

80. Fenwick & Davidson, *supra* note 71, at 14.

81. FED. R. EVID. 1004 states:

> The original is not required, and other evidence of the contents of a writing, recording, or photograph is admissible if—
>
> (1) Originals lost or destroyed. —All originals are lost or have been destroyed, unless the proponent lost or destroyed them in bad faith; or
>
> (2) Original not obtainable. —No original can be obtained by any available judicial process or procedure; or
>
> (3) Original in possession of an 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) Collateral matters. —The writing, recording, or photograph is not closely related to a controlling issue.

82. *See, e.g.*, Schiavone-Chase Corp. v. United States, 553 F.2d 658 (Ct. Cl. 1977) (computer billing lists admitted where original source documents had been destroyed after two years in accordance with government policy); Sears, Roebuck & Co. v. Merla, 142 N.J. Super. 205, 361 A.2d 68 (1976) (trial court's decision to refuse admission of computer printout due to original invoices being destroyed reversed on appeal).

83. FED. R. EVID. 1006 states:

> 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.

84. 5 D. LOUISELL & C. MUELLER, *supra* note 75, § 551 n.45.

85. *See* State v. Springer, 283 N.C. 627, 197 S.E.2d 530 (1973) (testimony by bank investigator regarding computer report detailing use of a stolen credit card held inadmissible because no foundation was laid and the printout itself was not offered into evidence). For a criticism of *Springer*, see Sprowl, *Evaluating the Credibility of Computer-Generated Evidence*, 52 CHI.-KENT L. REV. 547, 561 (1976) (arguing that the in-

C. *Expert Testimony and Scientific Evidence*

Several commentators have suggested that computer-generated analyses, simulations and models[86] be used as a basis for expert testimony as a means of getting such evidence before the trier of fact over hearsay and original writing rule objections.[87] Federal Rule of Evidence 703 allows an expert to base his opinion on evidence that would otherwise be inadmissible.[88] However, the computer models and simulations used as a basis for expert opinion must still be of a type reasonably relied on by experts in a particular field.[89] Where a party seeks to admit the model itself into evidence, the model will be treated as scientific evidence. In many jurisdictions this evidence will have to meet the *Frye* test, which requires that the scientific technique be generally accepted by the scientific community to which it belongs.[90]

Even where the requirements for expert opinion or scientific evidence have been fulfilled, the evidence may still be barred as unfairly prejudicial or cumulative.[91] Whether Federal Rule of Evidence 403 will apply, however, is unclear.[92] In any event, courts have used two methods to overcome Rule 403 objections. The first involves requir-

herent guarantees of reliability within the report should have been considered rather than just the method in which the evidence reached the court). *See also* United States v. DeGeorgia, 420 F.2d 889 (9th Cir. 1969) (testimony presented concerning computer report indicating that car was not rented and therefore was stolen would have been barred but defendant failed to raise the best evidence rule and therefore waived objection).

86. *See generally* Eastin, *The Use of Models in Litigation: Concise or Contrived?*, 52 CHI.-KENT L. REV. 610 (1976) (a discussion of the usefulness of models in presenting evidence and an explanation of basic underlying theories and techniques); Jenkins, *Computer-Generated Evidence Specially Prepared for Use at Trial*, 52 CHI.-KENT L. REV. 600 (1976) (discussion of the application of computer models to practical examples).

87. *See* Comment, *Guidelines for the Admissibility of Evidence Generated by Computer for Purposes of Litigation*, 15 U.C.D. L. REV. 951, 968 (1982).

88. FED. R. EVID. 703 provides:

> The facts or data in the particular case upon which an expert bases an opinion or inference may be those perceived by or made known to him at or before the hearing. If of a type reasonably relied on by experts in the particular field in forming opinions or inferences upon the subject, the facts or data need not be admissible in evidence.

89. *See id.*

90. For a review of requirements and trends in the admission of scientific evidence, see Lacey, *Scientific Evidence*, 24 JURIMETRICS J. 254 (1984).

91. FED. R. EVID. 403 states that "[a]lthough relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence."

92. *See, e.g.*, Harper, *Computer Evidence is Coming*, A.B.A. J., Nov. 1984, at 80, 81.

ing advance notice of the intention to use a computer simulation.[93] The second involves making the programs used to develop such models available to counsel in advance of trial.[94]

One disadvantage of presenting computer-generated testimony through expert opinion is that the information is admissible only to establish the basis upon which the expert's opinion was formed and not for substantive purposes. The court may issue a limiting instruction under Federal Rule of Evidence 105, instructing the jury to consider the evidence only for the purpose of evaluating the expert's testimony, and not for the truth of the matter asserted by the evidence. However, the effectiveness of such an instruction is questionable.[95]

Due to the trend of allowing expert opinion based both on computer simulations and the simulations themselves, the possibility that novel expert and scientific evidence will be admitted is strong. Because computers add a degree of complexity to the admissibililty of scientific evidence, the need for effective pretrial discovery is stronger than ever.

D. Authentication and Identification

The "trustworthiness" requirement of the business records exception is paralleled by a similar concern in the authentication requirements. Authentication, a condition precedent to admissibility, requires that sufficient evidence be produced to support a finding that the evidence in question is what its proponent claims.[96] With respect to computerized information, evidence must be produced supporting the accuracy of the process or system producing the result.[97]

---

93. *See, e.g.,* United States v. Russo, 480 F.2d 1228, 1241 (6th Cir. 1973), *cert. denied,* 414 U.S. 1157 (1974); United States v. Dioguardi, 428 F.2d 1033, 1038 (2d Cir.), *cert. denied,* 400 U.S. 825 (1970). *See also* United States v. Weatherspoon, 581 F.2d 595, 598 (7th Cir. 1978); Perma Research & Dev. v. Singer Co., 542 F.2d 111, 115 (2d Cir.), *cert. denied,* 429 U.S. 987 (1976).

94. *See supra* note 93.

95. M. GRAHAM, *supra* note 55, at 323 (arguing that despite a possible limiting instruction, FED. R. EVID. 703 acts as an exception to the hearsay rule and an alternative to authentication requirements).

96. FED. R. EVID. 901(a) states that "[t]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

97. FED. R. EVID. 901(b) states in part:

> (b) Illustrations. -By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule:
>
> (1) Testimony of a witness with knowledge. —Testimony that a matter is what it is claimed to be.
>
> . . . . .
>
> (9) Process or system. —Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.

In proving the accuracy of the system, the same considerations applying to the "trustworthiness" requirement of the business records exception and a general evaluation of the credibility of the evidence should be considered.[98]

Establishing that the printout in question is what it purports to be is an authentication problem that may have to be considered apart from the business records exception. Because computer printouts are readily available and often difficult to distinguish, the proponent should establish a limited chain of custody.[99] The printout should be marked as soon as it is printed. The custodian and others handling the document should likewise mark the document. Testimony that the printout is in substantially the same condition as when it left the computer should be given. A printout could also be self-authenticating as a certified public document.[100]

IV. EVALUATING THE CREDIBILITY OF COMPUTER-GENERATED EVIDENCE

Once computer-generated evidence is admitted, some of the same considerations involved in determining admissibility must be reexamined in more depth. A court, construing the evidence in the light most favorable to the proponent, may be willing to admit the evidence despite doubts as to its probative value. However, once threshold requirements have been met for purposes of admissibility, the

98. *See infra* notes 101-21 and accompanying text. *See also* Comment, *Guidelines for the Admissibility of Evidence Generated by Computer for Purposes of Litigation*, 15 U.C.D. L. REV. 951, 958-59 (1982) (arguing that summaries should be held to a higher standard of reliability than computer analyses and simulations).

99. Fenwick & Davidson, *supra* note 71, at 22.

100. FED. R. EVID. 902(4) provides for admission of certified public records as follows:

> Extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to the following:
>
> . . . .
>
> (4) Certified copies of public records. A copy of an official record or report or entry therein, or of a document authorized by law to be recorded or filed and actually recorded or filed in a public office, including data compilations in any form, certified as correct by the custodian or other person authorized to make the certification, by certificate complying with paragraph (1), (2), or (3) of this rule or complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority.

For applications of this rule, see United States v. Farris, 517 F.2d 226, 228-29 (7th Cir.), *cert. denied*, 423 U.S. 892 (1975) (officially certified computer printout produced by Internal Revenue Service admitted into evidence because it was a self-authenticating public record); Weaver v. State, 404 N.E.2d 1180 (Ind. Ct. App. 1980) (computer printout of defendant's driving record admitted over an authentication objection; the printout was self-authenticating by virtue of being a certified public document).

persuasiveness of the evidence will depend largely upon an advocate's ability to exploit what one commentator has termed "the inevitable uncertainties" inherent in any data processing system.[101] Understanding these potential weaknesses is crucial, since juries may have a tendency to overvalue neat tabulations contained in computer printouts.[102]

An attorney faced with the task of supporting or attacking computer-generated evidence can benefit from placing himself in the position of an auditor. An auditor's role is generally to obtain sufficient and competent evidential matter and render an opinion as to the fairness of an entity's financial statements.[103] Auditors have necessarily had to deal with the problem of whether information contained within a computer system is reliable. While undertaking a full audit will generally not be cost effective and may also be precluded by discovery limitations, a certain amount of investigation should take place.[104] Critical points of inquiry include: (1) input procedures; (2) programs, including testing and documentation; (3) equipment; (4) safeguarding of information; (5) system security; (6) integrity of the output; and (7) opportunities for falsification.

Input procedures should be closely examined since the quality of the output will depend on the quality of the input.[105] Input error can occur in several ways, including the incorrect creation of data, document loss, lost data, added data, improper authorization, and improper conversion into machine-readable form. Repetitive keypunching or typing, which is often used to enter information into a computer system, increases the probability of error.[106] Although several kinds of input controls are available to eliminate error,[107] the error rate will generally be more than zero because of cost-benefit considerations.[108] Furthermore, controls which are theoretically in effect may not be followed in reality. The party using the system

---

101. Fenwick & Davidson, *supra* note 71, at 21.

102. Commentators have repeatedly noted the danger that juries will tend to overvalue evidence presented in computer printouts. *See, e.g.*, Connery & Levy, *Computer Evidence in Federal Courts*, 84 COM. L.J. 266, 271 (1979); Sprowl, *supra* note 85, at 547.

103. *See, e.g.*, A. ARENS & J. LOEBBECKE, *supra* note 12, at 109-10.

104. For a description of the planning and execution of such an investigation, see DeHetre, *Data Processing Evidence-Is It Different?*, 52 CHI.-KENT L. REV. 567 (1976).

105. This concept is sometimes phrased "garbage in, garbage out." For an example of a court taking judicial notice of this principle, see Sears, Roebuck & Co. v. Merla, 142 N.J. Super. 205, 361 A.2d 68 (1976).

106. *See* Sprowl, *supra* note 85, at 558.

107. Examples of input controls would include keypunch verifying, check digits, control totals, transmittal controls, and route slips. For example, a control total would involve summarizing information and then comparing the total to amounts input into the system. For further information on input controls, see A. ARENS & J. LOEBBECKE, *supra* note 12, at 448-49; G. DAVIS, AUDITING & EDP 57-59 (1968).

108. Cost benefit considerations apply to the notion that at some point the cost of eliminating errors exceeds the costs of allowing the errors to exist. Consequently, a

should probably provide the actual error rate.[109] If such statistics are not kept, testing may be necessary.[110]

The programs used to process information should also be examined. Such programs will frequently be used to alter raw data into a format more convenient for analysis, storage, and subsequent retrieval. Program errors are inherent in computer programs, especially those of greater complexity.[111] Whether the system has been properly documented and tested should strongly indicate the possibility of such errors. But even where reasonable precautions have been taken, program errors are not unusual.[112] The existence and proper operation of system controls designed to detect the erroneous processing of information should be examined. Programs should also be examined to determine whether the reports generated are slanted in favor of one party. The possibility of a biased report will depend in part on the extent to which information is being summarized.[113]

The equipment used to process the data should be examined for the possibility of malfunctions which could result in altered data. While several commentators take the position that computers are mechanically reliable and that their proper functioning is of no real concern in evaluating credibility,[114] at least some attention should be paid to the proper operation of a system's hardware. Indications of the hardware's reliability include the use of preventative maintenance procedures and the system's downtime record (machine breakdown). Statistics on the equipment's error rate in storing and retrieving information is another factor. Inquiry should be made into the controls within the hardware designed to detect alterations in data, especially where data is transmitted over telephone lines.[115] The procedures used by the data processing center in handling reported errors should also be considered.[116]

The data processing installation procedures for safeguarding records and files is another area of concern. Data may be acciden-

---

certain number of errors are tolerated. For further discussion, see Sprowl, *supra* note 85, at 553.

109. *See id.* at 558.

110. *Id.*

111. *See* G. DAVIS, *supra* note 107, at 79-81; Sprowl, *supra* note 85, at 559.

112. *See supra* note 111.

113. A computer-generated summary was admitted into evidence in United States v. Russo, 480 F.2d 1228 (6th Cir. 1973), *cert. denied*, 414 U.S. 1157 (1974). For a vigorous criticism of this holding, see Sprowl, *supra* note 85, at 552-65.

114. *See* Note, *supra* note 58, at 79-80; Sprowl, *supra* note 85, at 553.

115. G. DAVIS, *supra* note 107, at 50-51.

116. A. ARENS & J. LOEBBECKE, *supra* note 12, at 447.

tally destroyed in several ways, including fire, extreme variations in temperature, power outages, mishandling of data processing equipment and files, and equipment malfunction. While controls are available to prevent such occurrences,[117] whether steps have actually been taken to prevent losses of data is a point of concern. Also relevant is the procedure for recreating lost files,[118] especially if part of the data base has actually been destroyed for some reason. Reconstruction implies that relatively large amounts of data will have to be processed, thereby increasing the chance that data will be altered.

The security of the system should be questioned because computerized information can be changed without leaving a trace, and because data processing facilities tend to centralize record keeping functions. This inquiry will be especially sensitive, due to the natural reluctance of a business to disclose information that could facilitate tampering with the system.[119] Although the extent to which discovery will be allowed is unclear, some information should be discoverable. Any weaknesses in security that existed at a relevant point in time should work to discredit evidence generated by the system. In general, some controls should be present to limit access to the physical equipment, the system, and the data storage facilities.[120] Whether the system is protected from external tampering will also be of concern where access to the system can be gained over telephone lines.[121]

The integrity of the output data should also be considered. Because computer reports are easily printed and often indistinguishable, evidence should be produced that indicates that the specific report offered at trial was produced in accordance with whatever controls are theoretically in use.

The identity of the party offering the computer report into evidence and the identity of the computer's owner are other factors to be considered in arguing the credibility of computer-generated information. Where the printout is offered by a party who had sole possession and control of the computer and had the motive to falsify information contained therein, such information should be subjected to close scrutiny.

---

117. Examples of processing controls include tests for invalid data, crossfooting tests, reasonableness tests, and file and label controls. For a further explanation of such controls, see A. ARENS & J. LOEBBECKE, *supra* note 12, at 449-50; G. DAVIS, *supra* note 107, at 87-102.

118. For a description of backup procedures, see G. DAVIS, *supra* note 107, at 95-101.

119. *See* Harper, *supra* note 92, at 83 (commenting that banks are opposed to strong foundational requirements for the admission of computer records).

120. For a further discussion of security measures, see W. PERRY, THE ACCOUNTANTS' GUIDE TO COMPUTER SYSTEMS 261-75 (1982).

121. For an example of the dangers "hacking" poses to a security system, see Sandza, *The Revenge of the Hackers,* NEWSWEEK, Dec. 10, 1984, at 81.

V. CONCLUSION

The growing use of computer-generated evidence requires that the practitioner become proficient in dealing with the discovery and use of such evidence. While becoming familiar and comfortable with computers may require a certain amount of study, the basic principles needed to understand such devices are not complicated. Computerized evidence is unique. Its attempted admissibility requires that certain considerations, especially reliability, be emphasized to a greater degree. However, the basic principles of discovery and evidence still generally apply. These principles, and not the operation of the computer, must be emphasized.

RICHARD M. LONG