1978


David Bender

Follow this and additional works at: http://repository.jmls.edu/jitpl

Part of the Computer Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation
David Bender, Computer Evidence Law: Scope and Structure, 1 Computer L.J. 699 (1978)

http://repository.jmls.edu/jitpl/vol1/iss1/22

This Article is brought to you for free and open access by The John Marshall Institutional Repository. It has been accepted for inclusion in The John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of The John Marshall Institutional Repository.
INTRODUCTION

Computer evidence law may broadly be defined as the intersection of the law of evidence with the technology and art of computing, or alternatively, as that body of evidentiary principles applicable to things and concepts related to the computer. While the majority of judicial opinions in computer evidence law deal with the admissibility of computer-generated business records, computer evidence law is not limited to this category, and its shape is gradually taking form. It extends across the entire computing milieu, and into numerous traditional rubrics of evidence law. While not as well-settled as the admissibility of business record printouts, many of these other areas can be expected to become quite important in the future.

Computer evidence law is not, and never will be, a separate area of law as, for example, is torts, contracts, or constitutional law. Rather, it is an area where a rapidly moving field of technology is impacting a venerable corpus of law. The burgeoning amount of litigation and counseling now occurring in this area suggests that it is increasingly important for litigators and other lawyers to develop a
facility for applying traditional evidentiary concepts to computer technology.

The purpose of this article is threefold: to define the topic of computer evidence law; to comment on the structure of that law; and to note briefly some important aspects of the topic which have not yet received extensive comment in cases and periodicals, especially those aspects which seem destined to ripen and emerge in the near future.

I. ADMISSIBILITY AND COMPUTER EVIDENCE

The technical aspects of the admissibility of computer evidence have received extensive comment elsewhere, and will not be discussed at length. Admissibility is obviously one of the foremost hurdles which the proponent of computer evidence must clear. Conversely, if the adversary prevails on this single point, the evidence is out of the case. Some technical aspects of admissibility which may profitably be explored are:

Laying a proper foundation
Best Evidence Rule
Rule Against Hearsay Evidence, and pertinent exceptions:
Business records
Official records

Declarations against interest
Treatises and trade publications
Ancient documents
Admissions
Photocopy statute

Computer evidence is surprisingly multifaceted. The majority of cases to date involve its most obvious aspect—the admissibility of computer-generated records. But this is just the tip of an emerging iceberg, the boundaries of which are only now beginning to manifest themselves. Computer evidence extends across the entire spectrum of evidence; it goes beyond the question of admissibility, and far beyond business records.

As an example of recent interest, consider a monopolization suit in the computer industry. One's ability to prove the nature of hardware, software, and services, as well as their interaction, might be crucial in establishing the concept of relevant market. Or consider a suit alleging an unlawful tie-in of software with hardware. A basic knowledge of the technology, and how to present that knowledge in court, would be vital to establishing whether there are, in fact, two separate entities (hardware and software), or just one (a "computer system"). To be sure, in these two examples, the substantive law is antitrust. But the vehicle for reading that substantive law on the computing milieu is computer evidence law.

II. THE NATURE OF COMPUTER EVIDENCE

To understand better the full scope of computer evidence law, and also to understand the technical aspects of admissibility, the universe of evidence law may be divided into six major categories: testimonial, experimental, observational (or "view"), and tangible, with the last being subdivided into writing, record and demonstrative evidence. To appreciate the distinctions between and among

---

4. The sale of any product or service which is distinguishable as a matter of commercial practice from other products or services will ordinarily constitute a relevant product market, even though, from the standpoint of most purchasers, other products may be reasonably, but not perfectly, interchangeable with it in terms of price, quality, and use.

5. "A tying arrangement (or 'tie-in') exists when the seller requires his buyer or lessee to take a product he does not want (the tied item) as a condition to obtaining a product he does want (the tying item)." Id. § 2.9, at 193.

6. This categorization is offered solely as a matter of convenience. The category names employed, while widely used in evidence law, have no universally accepted definitions. No claim is made that those categories are all-inclusive.
these categories, it is instructive to consider each separately, with reference to specific examples of each type of evidence.

A. Testimonial Evidence

This is the most common form, consisting of a witness answering questions or telling his story, with the "trier . . . asked to believe that certain facts are true only because the witness . . . states them to be so." Example: The testimony of a company's data processing manager as to the nature of the company's computer system.

B. Experimental Evidence

An "experiment" is an in-court demonstration permitted by the court if its value to the fact-finding process outweighs possible confusion and delay. The experiment can be persuasive (when it works), and is one means of holding the trier's interest while demonstrating the operation of any machine deemed important to one's case. To be valid, a similarity of circumstances must exist between the experiment and the system or event it purports to represent.

Example: In one case, the issue was whether certain read-write heads, ordered by plaintiff for his computer, were defective for his intended use. On plaintiff's computer, sixty heads were required for a thirty track drum. During trial the defendant demonstrated the use of the heads on his own computer—a different type of machine using only three pairs of heads with a single track drum. By running his computer without head error for a certain period of time, the defendant attempted to establish that the heads would function without error for the same duration in plaintiff's computer, and therefore, the heads were not defective. The court found the experiment invalid because of a lack of similarity of circumstances, since the issue was not the amount of time the heads would operate without error, but the number of bits read by the heads without error. The court credited the testimony of plaintiff's witness that it would be "rather dangerous to try to extrapolate from these tests and to conclude that, since the heads worked a few times with a

8. 4 J. Wigmore, Evidence § 1154a, at 333 (J. Chadburn rev. ed. 1972). Obviously, it is important to the proponent that the experiment work, as it can be fatal to his case otherwise.
10. Id. at 751, 1 CLSR at 177.
11. Because plaintiff's computer had more tracks and heads, it performed many more read-write operations per unit of time than defendant's machine. Id. at 751, 1 CLSR at 178.
given problem, they are perfectly satisfactory in general.\textsuperscript{12}

C. View

The court may permit a trip to view material, places or things not easily brought into the courtroom. Direct observation may be used where the additional information is deemed more important than the delay and disruption that occurs.\textsuperscript{13} Example: In one celebrated case, a tour of computing facilities at Cape Canaveral was scheduled so that the court might observe the use and importance of computers in the United States space program.\textsuperscript{14}

D. Tangible Evidence

This is evidence which permits the trier to perceive facts directly through use of his senses. It is often useful for getting and keeping the trier's attention, but care must be taken to ensure that it is not prejudicial or misleading. Tangible evidence can be subdivided into three classes:

- **Writing**—tangible evidence offered to show its informational content. Example: A contract setting forth the terms under which a software house will develop a specific program for a customer.

- **Record**—Tangible evidence introduced to show the truth of its informational content. Example: A printout sheet offered to show the status of a customer account.

- **Demonstrative Evidence**—tangible evidence offered to show its characteristics exclusive of any informational content. Demonstrative evidence may be useful to illustrate a point, or to get the trier's attention. Example: A reel of tape offered to show a defect.

In terms of the number of judicial decisions to date, the most frequently discussed of these categories, by far, is records. But many cases have involved other categories, and the number of such cases should grow as the application to computers of the law attendant to these categories becomes better appreciated.\textsuperscript{15}

\textsuperscript{12} Id. at 752, 1 CLSR at 178.
\textsuperscript{13} In most jurisdictions, a view is solely for the purpose of aiding the trier of fact, and does not actually constitute evidence. C. McCormick, Evidence § 216, at 539 (2d ed. E. Cleary 1972).
\textsuperscript{15} Chart I sets forth examples of computer evidence in each of these categories. As noted, evidence in each category can exist in either circumstantial or direct form.
## EXAMPLES OF VARIOUS TYPES OF COMPUTER EVIDENCE

<table>
<thead>
<tr>
<th>DIRECT</th>
<th>CIRCUMSTANTIAL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Testimonial</strong></td>
<td></td>
</tr>
<tr>
<td>Testimony that a computer program in question, if executed properly by the hardware, and operating on the data allegedly input, could not cause the incorrect output in question.</td>
<td>Testimony that in the particular circumstances in suit, the probability of software failure is 1,000 times higher than the probability of hardware failure, where the fact in issue is which of these two types of failure was responsible for incorrect output.</td>
</tr>
<tr>
<td><strong>Writing</strong></td>
<td>Print-out of accounts printed out by the same computer at about the same time as the account in issue, offered to show patent inconsistencies of the type alleged to be in the account in issue.</td>
</tr>
<tr>
<td>A facilities management contract offered to prove the obligations of the parties, where that is in issue.</td>
<td></td>
</tr>
<tr>
<td><strong>Tangible</strong></td>
<td>Records printed out in the regular course of business and offered to prove the status of a party's account, where that is in issue.</td>
</tr>
<tr>
<td>Demonstrative</td>
<td>A magnetic tape offered to prove that it was defective and responsible for the incorrect output in suit, where an issue is determination of the responsibility for the error.</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Experiment</td>
<td>A showing in court that a particular portable console functions properly as to input and printout, where such functioning is in issue.</td>
</tr>
<tr>
<td>View</td>
<td>A showing at a computer facility that a particular tape drive functions properly, where such functioning is in issue.</td>
</tr>
</tbody>
</table>

**Chart I**

In determining how to treat computer evidence, one must first ask for what purpose it is offered. Until that question is answered, the parties do not know with what rules the evidence must comply. The same item, offered for different purposes, may qualify as any of the three types of tangible evidence. For example, a fifty page printout, if offered to show the bulk associated with fifty pages of printout, is demonstrative evidence; if offered to show what it contains, is a writing; but if offered to show the truth of its contents, is a record. Hence, the purpose for which it is offered determines what kind of foundation must be laid for its introduction, whether compliance with the Best Evidence rule is necessary, and whether the hearsay rule creates a problem.

These determinations are quite important. If one is unable to state at trial one’s position vis-a-vis the admissibility of computer evidence in precise terms, i.e., if there is any significant fuzziness to the statement, one runs a very real risk. A growing number of courts have held that a failure at trial to use the “magic words” connoting a particular objection constitutes waiver of that objection.

16. The rule is this: in proving the terms of a writing, where the terms are material, the original writing must be produced unless it is shown to be unavailable for some reason other than the serious fault of the proponent. C. McCormick, supra note 13, § 230, at 560.

17. Hearsay evidence is defined as “testimony in court, or written evidence, of a statement made out of court, the statement being offered as an assertion to show the truth of matters asserted therein, and thus resting for its value upon the credibility of the out-of-court asserter.” Id. § 246, at 584. The hearsay rule precludes the introduction of hearsay evidence at trial, except in specifically enumerated instances. See, e.g., Fed. R. Evid. 802-03.

18. See, e.g., United States v. Fendley, 522 F.2d 181, 6 CLSR 265 (5th Cir. 1975). In Fendley, the Government introduced and authenticated a series of exhibits under the old Federal Business Records Act (former 28 U.S.C. § 1732(a)). The Government then introduced, through the same witness, without proffer of authentication, a computer print out. The defendant conducted a voir dire and objected:

on the basis that there is no accuracy shown that the instrument is accurate as to the figures it reflects;

And that the preparer was someone other than the witness here, that we cannot determine the accuracy of it, and therefore, it shouldn't be admitted;

Because it would be hearsay and, again, I cannot cross-examine the paper, obviously, without having the party assigned to compiling the figures on it before us.

Id. at 185, 6 CLSR at 269. The majority saw this as an objection “(1) that the document was hearsay; (2) that the witness laying the foundation for its introduction was someone other than the preparer; and (3) that the witness laying the foundation was unable to personally attest to the accuracy of the figures contained in the document.” Id. According to the majority,

[There was no objection on the only grounds which would have permitted the trial court to have required that a fuller foundation be laid for the admission of the exhibit—that the printout was made and kept in the regular course of business, for regular business purposes and relied upon by the
This is true even though the party is objecting "all around" the correct objection. Indeed, where counsel makes numerous, rather similar objections, the burden of specificity may be even greater.\textsuperscript{19}

\section*{III. Probative Value}

Of all of the topics properly encompassed within computer evidence law, the one that may contain the largest untapped potential is probative value. Securing admissibility for one's evidence is only the first step faced by a litigator; the crucial second step is establishing the weight to be accorded the evidence by the trier of fact, \textit{i.e.,} the evidence's "probative value." Insofar as can be discerned from published opinions, in computer-related cases the importance of probative value has often been ignored. To be sure, some of the effort devoted to laying a proper foundation may impact on probative value, but, to the extent that published opinions reflect the parties' contentions, the battle often apparently rages solely on the issue of admissibility. If the evidence is admitted, the opponent often sub-

\begin{flushright}
\textit{Id.}
\end{flushright}

To object as the defendant did that "the preparer is someone other than the witness here" and that consequently "there is no accuracy shown that the instrument is accurate as to the figures it reflects" in no way apprises the trial court that the defendant attacks the reliability of the method of preparation of the exhibit.

\begin{flushright}
\textit{Id.} at 186, 6 CLSR at 271. Defendant was therefore not permitted to raise this point on appeal. In vigorous dissent, Judge Godbold argued that the prosecution's failure should not be salvaged at the appellate level by the palliative that there was an insufficient objection. * * * There can be no real doubt that all present and participating knew that the subject matter of the [objection] was the question of whether the printout had been authenticated as required by the Business Records Act. * * * It is disingenuous to treat this matter as though everyone has discovered for the first time on appeal, and to his surprise, the point which the defendant was seeking to call to the judge's attention.
\end{flushright}

\begin{flushright}
\textit{Id.} at 191, 6 CLSR at 278-80 (Godbold, J., dissenting). In Judge Godbold's opinion, "[b]eyond the overall clarity of what the relevant trial events were all about, the wording of the objection, considered alone, does not permit the narrowing construction imposed by the majority." \textit{Id.} at 191, 6 CLSR at 280 (Godbold, J., dissenting).
\end{flushright}

\begin{flushright}
\textit{Id.} at 191, 6 CLSR at 278-80 (Godbold, J., dissenting).
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
\end{flushright}

\begin{flushright}
\textit{Id.} at 1038, 2 CLSR at 652-53.
mits meekly, sometimes refraining from any attack at all on its probative value. Or, if such an attack is mounted, it is made in a general, vague manner, as by asserting that the computer system used in generating the evidence was not accurate, but without any supporting facts. This circumstance should and will change, and the future should witness more spirited debate on the issue of probative value.

Figure 1
Block Diagram of Account Updating System

A. Defining the Appropriate Human-Computer System

In discussing the probative value of computer evidence, one must usually deal not solely with the computer, but with the "human-computer system," i.e., the combination of people and machines which operates on input according to some predetermined plan to create output. The system accepts input, then purportedly functions as directed (the human portion in accordance with verbal or written instructions, and the machine portion in accordance with program instructions), and finally disgorges output. The equation governing this system is "Input + Processing = Output." Correct input, fed in and processed properly, must yield accurate output. Conversely, one desiring to show that the output is inaccurate must demonstrate either incorrect input or improper processing.

In assessing probative value, it is useful to construct a human-computer system particularized to one's own situation. Care must be taken in choosing that system. If it is overly inclusive, it will be unnecessarily complex; if it includes too little, it may not embrace important sources of error. Figure 1 illustrates, for an account updating system, a simplified system diagram, with the solid line embracing the human-computer system, and the dashed line the central processing unit. For such a system, one may analyze the two equally important aspects of probative value: tactical and substantive.

B. Tactical Aspects of Probative Value

If counsel believes in, and desires the trier of fact to embrace, his or her version of reality, counsel must strive for a high degree of intelligibility. The attorney must function effectively as a pedagogue in an area of knowledge where, even under the best of conditions, the transfer of knowledge may be slow and painful—and the adversary process hardly qualifies as the best of conditions. Diagrams, if clear and uncluttered, may be of great aid in this respect. For example, Figure 2 depicts a non-detailed flowchart of a program used to

20. A "central processing unit" (or CPU) is "[a] unit of a computer that includes circuits controlling the interpretation and execution of instructions." American Nat'l Standards Inst., Dictionary for Information Processing (1977), reprinted in 1 R. Bigelow, Computer L. Serv. § 1-3, art. 1, at 27 (1978) (emphasis omitted) [hereinafter ANDIPI].

21. A flowchart is "[a] graphical representation of the definition, analysis, or method of solution of a problem, in which symbols are used to represent operations, data, flow, equipment, etc." Id. at 66 (emphasis omitted).
effect account updating, and Figure 3 depicts a somewhat more
detailed flowchart of that same program.

**Figure 2**
Non-Detailed Flowchart of Program for Account Updating


An important aspect of intelligibility is that of organization. Until the scheme of things becomes evident, discrete facts, no matter how clear they may be in and of themselves, will not convey coherent thoughts. This bears special mention with regard to computer evidence because, as the unfamiliarity of the subject matter increases, so does one's need for some framework on which to arrange the symbols of one's incipient understanding.

The pace of education should be slow at first. When a print out is used, it should, if possible, be accurately and comprehensively labeled. The use of computer jargon by lawyers and witnesses should be eschewed, and strange terms explained. Witnesses must be taught to speak in terms which the trier of fact will understand. It is

22. After hearing the evidence in this case the first finding that the court is constrained to make is that, in the computer age, lawyers and courts need no longer feel ashamed or even sensitive about the charge, often made, that they confuse the issue by resort to legal "jargon," law Latin or Norman French. By comparison, the misnomers and industrial shorthand of the computer world make the most esoteric legal writing seem as clear and lucid as the Ten Commandments or the Gettysburg Address; and to add to this Babel, the experts in the computer field, while using exactly the same words uniformly disagree as to precisely what they mean.

advisable to subject the more technical parts of the trial to a dress rehearsal before someone who is not knowledgeable about com-
puters, and to be guided by his or her reaction on various crucial points.

It may be advantageous to desanctify the "Sacred Cow," i.e., the computer, by characterizing it as an overgrown adding machine with no mind of its own. It may also be of benefit to capture the trier's attention with tangible evidence, such as punch cards, tape reels, or print outs. Counsel has a head start in this area because of the glamour popularly associated with computers, but that advantage should not be lost through sloppy organization or overcomplexity. Further, the trier's attention may be held more readily if the computer evidence is related to his or her own experience. A bank's account debiting program may seem more comprehensible if it is made clear that its function is to balance the bank's accounts, much as one balances a checkbook.

If counsel wants to discredit the accuracy of computer evidence, numerous "horror stories" can be dredged up. Attempts can be made to capitalize on unfavorable computer-related experiences the trier of fact personally may have had. Testimony may be elicited about the high number of calculations necessary to reach a result, the great number of components in the computer, or the number of human operations necessary to prepare input data. Safeguards used on the system in question may be compared to those used in similar, or even more critical, applications.

Each such gambit is an attempt to discredit the accuracy of the result without pointing to any known defect in that result or in the input or process giving rise to it. It is an attempt to discredit any product of the system, a "parade of horribles" used in an effort to show "inaccuracy in the air." In any given case, such a tactic may succeed, but it will generally prove less effective than facts, if such exist, probative on the issue of why the specific evidence offered is untrustworthy. It should often be possible to overcome a general reliability attack by establishing the safeguards used in the particular system, the safeguards used in similar systems, the long term reliance of the user and others on output from the system, and the fact that complaints have not risen above a certain level.\footnote{23. To one attacking the credibility of computer evidence, an adversary's customer complaint file may be a source of valuable evidence.}

Of special importance in an area like computing, where practitioners may be viewed as members of a high priesthood, is to have credible priests. If the proponent's witness tells a plausible tale, and seems reasonably confident even on cross-examination, he may well be able to overcome the "inaccuracy in the air" argument on that basis alone. Such a witness may convince the trier that, while it may
not understand what is going on, the witness does, and everything is under control.

C. Substantive Aspects of Probative Value

The fallibility of the human-computer system has two aspects, system reliability and system security. “System reliability” is the “probability that a system will accurately perform its specific task under stated tactical and environmental conditions.”24 “System security” is a more nebulous concept, defined for present purposes as the measure of a system's safety against tampering or other activities intentionally designed to influence improperly output from the system. The difference between these two concepts goes essentially to whether an incorrect result stems from inadvertence or subversion.25 In both cases, there are myriad potential error sources which can be probed, as well as numerous methods of reducing, if not avoiding, those errors.

1. System Reliability

In defining error sources and methods for reducing error, it is convenient to divide errors into human, hardware, and software.26 Any attempt to list a major portion of these possible sources and methods would exceed the space and time limitations of this article.27 Associated with most error sources is an error avoidance method, i.e., some mechanism or procedure designed to eliminate or reduce errors which might enter from that source. Some of the most important error sources and methods for avoiding errors are listed in Chart II.

2. System Security

System security addresses the system fallibilities which remain after one removes from the universe of sources denigrating the trustworthiness of a system those representing unintentional acts. System security has aroused a great deal of interest in the past few

25. Overall reliability and security problems generally emanate from seven sources: natural disaster, human error, equipment malfunction, vandalism, industrial espionage, theft, and fraud. The first three are examples of reliability problems, while the others pose security problems.
26. This is a convenient division, even though software errors usually, and hardware errors sometimes, are caused by humans.
27. For an extensive discussion on this topic, see BENDER, supra note 1, at 8-15 to 8-45, and the materials referenced therein.
Some Error Sources
and Error Avoidance Methods

<table>
<thead>
<tr>
<th>Error Sources</th>
<th>Error Avoidance Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Human</strong></td>
<td></td>
</tr>
<tr>
<td>Clerical mistake in input.</td>
<td>Reduce the role of humans in system.</td>
</tr>
<tr>
<td>Judgment mistake in input.</td>
<td>Check source documents against keypunch sheets.</td>
</tr>
<tr>
<td>Source data recording problem.</td>
<td>Verify keypunching.</td>
</tr>
<tr>
<td>Improper user instructions re-</td>
<td>Label tapes internally.</td>
</tr>
<tr>
<td>garding source data.</td>
<td></td>
</tr>
<tr>
<td>Computer operator error.</td>
<td>Use check digits where possible.</td>
</tr>
<tr>
<td>Library error.</td>
<td>Use functionally designed input forms.</td>
</tr>
<tr>
<td></td>
<td>Use input validation checks for form and limit.</td>
</tr>
<tr>
<td><strong>Hardware</strong></td>
<td></td>
</tr>
<tr>
<td>Character out of line on im-</td>
<td>Frequent use of diagnostic programs.</td>
</tr>
<tr>
<td>pact printer.</td>
<td>Use parity checks.</td>
</tr>
<tr>
<td>Card reader incorrectly wired.</td>
<td>Use duplicate processing.</td>
</tr>
<tr>
<td>Supplies failure.</td>
<td>Use echo checks.</td>
</tr>
<tr>
<td>Failure of electronic element.</td>
<td>Filter Foreign matter from air.</td>
</tr>
<tr>
<td>Power fluctuations.</td>
<td>Maintain humidity above 30% but below condensation point.</td>
</tr>
<tr>
<td>Normal electric shock.</td>
<td>Make provision for constant power level.</td>
</tr>
<tr>
<td><strong>Software</strong></td>
<td></td>
</tr>
<tr>
<td>Misleading documentation.</td>
<td>Use thorough de-bugging procedures.</td>
</tr>
<tr>
<td>System software logic error.</td>
<td>Use of more qualified programmers and analysts.</td>
</tr>
<tr>
<td>Application software logic er-</td>
<td>Require current documentation.</td>
</tr>
<tr>
<td>ror.</td>
<td>Use only software which has been in use for years.</td>
</tr>
<tr>
<td>Program bug.</td>
<td></td>
</tr>
<tr>
<td><strong>System</strong></td>
<td>Use record count.</td>
</tr>
<tr>
<td></td>
<td>Use proof figures.</td>
</tr>
<tr>
<td></td>
<td>Use secret account.</td>
</tr>
<tr>
<td></td>
<td>Use logs reflecting downtime.</td>
</tr>
<tr>
<td></td>
<td>Analyze customer complaints.</td>
</tr>
</tbody>
</table>

Chart II

years, often under the name “computer abuse". While system security has an impact on probative value, its effect is less substantial than that of system reliability.

Speaking to probative value as a whole, what one can do depends, as in so many other areas, largely on the size of one's pocketbook. Counsel in well-financed litigation involving a $2 million dispute will be able to do much more than counsel whose suit involves $10,000; but both should at least be thinking of probative value, and doing what they can within the constraints of their situation.

IV. SIMULATION BY COMPUTER

A second area of computer evidence, which is becoming increasingly important, is that of simulation by computer, i.e., the use of a computer to reflect the behavior of some actual or proposed process, system, or event. Mathematical models of physical (or other) processes, systems, or events are created and, through use of the computer, are subjected to varying simulated conditions in order to determine how they behave. The technologist or social scientist is able to create such a model because he or she is aware of the physical or other laws apparently or hypothetically controlling its operation. Through such simulation a great deal can be learned about systems of interest, often at tremendous savings of time, expense, and exposure to danger.

Simulation by computer is widely used today in such diverse applications as the study of nuclear chain reactions, the growth of forests, the flow of funds in an economy, and the effects on population of various attitudes regarding birth rates. Simulations may

28. Note, however, that “computer abuse" is defined by some authors to include the concept of system reliability, e.g., as “those incidents caused by intentional acts, negligent acts or accidental occurrences in which a perpetrator realized or could have realized a gain and/or a victim suffered or could have suffered a loss." Nycum, Intentional Misuse of Computers, in PLI, COMPUTER ABUSE—1976, at 7, 9.

29. BENDER, supra note 1, § 8.02[2][b].


31. For example, the flight of a spacecraft can be simulated by expressing the forces acting on it mathematically, and using Newton's laws to relate the forces to accelerations. Then, through a process known as “numerical integration," the accelerations are converted to velocities and positions.

32. It is generally believed that mathematical simulation is more fraught with
also be used "retrospectively" to help explain some event. For example, given the fact that a certain aircraft has crashed, numerous alternative conditions may be introduced into a computer simulation of the aircraft in an attempt to "reproduce" the disaster.

Whether a given simulation behaves as the actual or hypothetical system in question did, or would, depends on the validity of the assumptions used in creating the simulation, as well as the accuracy with which the mental model is given computer-related form—including the integrity of any input. The simulation itself is not direct evidence of the system or event in question, and is evidence at all only to the extent that it is a valid and accurate representation, i.e., only insofar as it permits valid inferences about the actual or hypothetical event, system, or process being simulated.

Creation of a simulation is not dependent on the existence of a computer. Simulation has come into its own so rapidly after the widespread adoption of computing techniques because the solution of modeling equations generally requires a large number of painstakingly detailed and repetitive steps, each of which must be performed with accuracy. Prior to the advent of the computer, any simulation beyond the most rudimentary would have required a large investment of humanpower and time to reach a result which, in part because of the fallibility of human calculation, would probably never have been completely trusted. This type of repetitive work, however, is "grist" for the computer and, as a result, the marriage of simulation and computing has been a fruitful one.

Computer simulations are surfacing in litigation with increased frequency. One interesting case in point is Perma Research & Development v. Singer Co.,33 where the plaintiff secured a judgment of about $7 million, in large part due to a computer simulation prepared for trial. The issue before the court was whether the defendant had breached a contractual obligation to use its best efforts to perfect and manufacture a patented, automotive antiskid device. The device had never been shown to work, and defendant contended that it was not perfectible. The plaintiff was placed in the posture of having to show the perfectibility of a device which had never been perfected.

Plaintiff's experts prepared for trial a computer simulation of a 1968 Thunderbird automobile, equipped with the patented device,

---

performing a series of stops. The court admitted testimony as to this simulation, despite plaintiff’s refusal to produce the program constituting the simulation.\textsuperscript{34} Judgment for the plaintiff was affirmed on appeal.\textsuperscript{35} However, in an opinion which is required reading for any student of computer evidence, Judge Van Graafeiland dissented, arguing that admissibility was improper for a number of reasons.\textsuperscript{36}

First, he believed that the plaintiff’s failure to disclose the computer program, which embodied the model used to simulate the operation of the device, denied the defendant the right fairly to cross-examine plaintiff’s expert witness.\textsuperscript{37} Second, he contended that a proper foundation was lacking, and that the algorithm\textsuperscript{38} on which the simulation was based was of questionable origin, apparently emanating from the hearsay opinions of non-witnesses. In addition, Judge Van Graafeiland challenged the breadth of the simulation. He noted that whereas the contractual understanding between the parties included the use of the device in many different cars, models, years, road surfaces, road grades, weather and altitudes, the simulation dealt solely with the operation of a 1968 Thunderbird car under standard conditions.\textsuperscript{39} Further, he challenged the simulation’s depth. Even for the single car embodied in the model, he felt that by the witness’ own admissions, there were numerous, potentially important characteristics of the vehicle’s structure and operation for which the model made no provision.\textsuperscript{40} He also believed that the expert opinions expressed were no more than mere speculation.\textsuperscript{41} He noted that, generally in practice, a simulation is validated by experimentation on actual devices before reliance is placed upon it. He was of the opinion that, even in the absence of apparent de-

\textsuperscript{34} Id. at 124, 6 CLSR at 105 (Van Graafeiland, J., dissenting).
\textsuperscript{35} Id. at 116, 6 CLSR at 116-28, 6 CLSR at 99-108 (Van Graafeiland, J., dissenting).
\textsuperscript{36} Judge Van Graafeiland may also have concluded that this contravened the Best Evidence Rule. See note 16 supra.
\textsuperscript{37} An algorithm is “[a] finite set of well-defined rules for the solution of a problem in a finite number of steps . . . .” ANDIP, supra note 20, at 10.
\textsuperscript{38} Among the things which were not simulated in the theoretical device of plaintiff’s witness were engine stalls and vacuum loss, the transfer value, the plunger in the hydraulic cylinder, the gears, the freedom of motion in the adapter gear, the tortional elasticity of the flexible shaft, the performance of the drive gear, the backlash in the gears, the oscillation between a retaining pin and the cam gear and the friction in the governor. Indeed, plaintiff’s expert ignored the measurements and figures in plaintiff’s existing unit.
\textsuperscript{39} 542 F.2d at 111, 6 CLSR at 100.
\textsuperscript{40} Id. at 122 n.11, 6 CLSR at 101 n.11.
\textsuperscript{41} Id. at 123, 6 CLSR at 103.
ffects, a simulation without parallel experimentation was inherently incapable of proving perfectibility.\textsuperscript{42}

In short, he believed that this evidence was incompetent and should have been excluded. Noting that a simulation is valid only insofar as it reflects the real world, he saw a general problem in relying on any uncorroborated simulation, and a particular problem in relying on this one, which he believed defective. He also felt that his colleagues were too ready to accept this genre of computer evidence.\textsuperscript{43} He pointed out that the receptiveness of courts to computer evidence has usually been directed toward computer-generated business records, and that a simulation prepared for trial simply did not possess the same generic guarantees of trustworthiness.\textsuperscript{44}

V. JUDICIAL NOTICE

Another topic destined to see increased application to computer evidence is the doctrine of judicial notice,\textsuperscript{45} which, in appropriate circumstances, permits the parties to dispense with the introduction of evidence. Judicial notice can shorten trials, remove confusing scientific questions from the jury, and permit the judge to escape the constraints of the adversary system in obtaining access to relevant information.\textsuperscript{46} There are two categories of adjudicative fact where judicial notice is proper: matters of common knowledge in the community, and matters of verifiable certainty.

A. Matters of Common Knowledge in the Community

While there are suggestions that the concept of "matters of common knowledge in the community" may extend to knowledge common only to a particular trade,\textsuperscript{47} the law seems generally not yet to have reached that point. This category may prove useful for basic matters attendant to the structure, fundamental operation, and common applications of the computer. One court has judicially noticed

\textsuperscript{42} \textit{Id.} at 123, 6 CLSR at 101-02.
\textsuperscript{43} \textit{Id.} at 125, 6 CLSR at 107.
\textsuperscript{44} \textit{Id.} at 125, 6 CLSR at 106-07.
\textsuperscript{45} The doctrine of judicial notice is one of common sense. The theory is that, where a fact is well-known by all reasonably intelligent people in the community, or its existence is so easily determinable with certainty from unimpeachable sources, it would not be good sense to require formal proof. Harper v. Killion, 345 S.W.2\textsuperscript{d} 309, 311 (Tex. Ct. App. 1961).
\textsuperscript{47} \textit{See} United States v. Rappy, 157 F.2\textsuperscript{d} 964, 966 (2d Cir. 1946); United Carbon Co. v. Monroe, 92 F. Supp. 460, 465 (W.D. La. 1950).
that "computerized record keeping is rapidly becoming a normal procedure in the business world." Indeed, computer evidence illustrates one danger of attempting to use this category of judicial notice—the danger of noticing judicially a "fact" which is not correct. For example, there may be numerous communities in which it is "common knowledge" that "computers" (i.e., hardware) often malfunction.

B. Matters of Verifiable Certainty

Where a fact may be ascertained by reference to authoritative materials readily available, that fact may also be judicially noticed. Many matters of common knowledge today were once matters of verifiable certainty. Presumably, many matters of verifiable certainty today will one day be matters of common knowledge, e.g., the fact that hardware is generally much more reliable than software. To be sure, a court may mistakenly accept as authoritative theories no longer believed valid, or not yet generally believed valid by practitioners. In particular cases, courts may even misinterpret conclusions.

Wigmore submits that the validity of scientific evidence depends upon (1) whether the type of apparatus is accepted as dependable; (2) whether the particular apparatus used is an accepted type and is in good condition; and (3) whether the witness using the apparatus is qualified. He notes that the first of these requirements may be satisfied by judicial notice, and indeed, courts have been utilizing the mechanism of judicial notice in scientific areas to establish such facts as the general reliability of radar as a means of detecting vehicle speed, and of the drunkometer as a means of detecting intoxication. So also, a court might judicially notice the fact that a commercial minicomputer may properly be used to control a process for refining oil.

Emphasis seems to be shifting from the "common knowledge"

49. BENDER, supra note 1, § 5.04[2], at 5-72.
50. Id.
52. Richardson characterizes this as showing "scientific acceptance," and concurs that it is a proper application of judicial notice. J. RICHARDSON, MODERN SCIENTIFIC EVIDENCE § 6.3, at 140-41 (2d ed. 1974). See also 3 D. LUISELL & C. MUELLER, FEDERAL EVIDENCE § 382, at 643-44 (1979).
basis to the "verifiable certainty" basis. This trend suggests that new scientific discoveries, which have become accepted within the appropriate profession, are proper subject matter for application of the doctrine. This, in turn, implies that the latter aspect of judicial notice may play an important role in computer evidence.

Rule 201 of the Federal Rules of Evidence deals with judicial notice, and there is case authority applying it to data processing by computers. In Neal v. United States, the taxpayer sought a refund of income taxes paid during 1973. The IRS sent him a form which stated that the excess tax paid by him in 1973 had been applied to adjust his account for 1971. No other explanation was given. Each of his three requests for a hearing or explanation was met by a computer print-out equally non-responsive. Neal sued for a refund for 1973. When the Government asserted that the taxpayer's claim lacked a sufficient showing of basis, the court noted that the details of any 1971 deficiency were "in the sole possession of the IRS computer," and that the Government could not require the taxpayer to provide details "which only the government possesses and which its computer will not disclose." The court stated:

Because it is generally known in this district, Fed. Ev. Rule 201(b), the court will judicially notice the fact that in 1974, many taxpayers entitled to refunds . . . were notified that the refund had been credited to taxes due for 1971, when in fact there were no taxes due for that year. This phenomenon, when it occurred, was

55. (a) Scope of Rule. This rule governs only judicial notice of adjudicative facts.
(b) Kinds of Facts. A judicially noticed fact must be one not subject to reasonable dispute in that it is either (1) generally known within the territorial jurisdiction of the trial court or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned.
(c) When Discretionary. A court may take judicial notice, whether requested or not.
(d) When Mandatory. A court shall take judicial notice if requested by a party and supplied with the necessary information.
(e) Opportunity to be Heard. A party is entitled upon timely request to an opportunity to be heard as to the propriety of taking judicial notice and the tenor of the matter noticed. In the absence of prior notification, the request may be made after judicial notice has been taken.
(f) Time of Taking Notice. Judicial notice may be taken at any stage of the proceeding.
(g) Instructing Jury. In a civil action or proceeding, the court shall instruct the jury to accept as conclusive any fact judicially noticed. In a criminal case, the court shall instruct the jury that it may, but is not required to, accept as conclusive any fact judicially noticed.

FED. R. EVID. 201.
57. Id. at 914.
58. Id. at 917.
widely reported and discussed at professional meetings in the dis-
trict, of persons whose work is concerned with the operation of the
income tax laws.

It is not suggested that all 1973 refunds were so treated; but
there was a sufficient number of them to suggest that what was at
work was the GIGO Rule for Computers (Garbage In, Garbage
Out).\textsuperscript{59}

VI. PRIVILEGE

One of the more fascinating things about computer evidence law
is the degree to which it is permeating traditional problems, only to
surface in the most unexpected places. One such unlikely place is
the area of privilege. An evidentiary privilege is a right residing in a
particular party to have certain matters barred from disclosure in a
legal proceeding.\textsuperscript{60} The two privileges most pertinent to computer
evidence are the trade secret privilege and the government secrets
privilege.

A. Trade Secret Privilege

Trade secrets\textsuperscript{61} may be embodied in computer hardware, pro-
grams, computer data bases, computer output, or documents relat-
ing to any of those. In most if not all jurisdictions, a trade secret
qualifies for a conditional privilege.\textsuperscript{62} Where the subject matter of
the trade secret is squarely in issue, disclosure can be compelled,
but the court may impose certain limitations.\textsuperscript{63} Limiting the disclo-
sure of computer-related evidence proprietary to one's client may be
quite important, and an understanding of the relationship of input,
processing, and output, along with the documentation attendant to
each of them, is necessary to ensure that one's opponent gets a min-
imum of proprietary information.\textsuperscript{64}

\textsuperscript{59} Id.

\textsuperscript{60} See generally C. McCormick, \textit{supra} note 13, §§ 72 \textit{et seq.}

\textsuperscript{61} "A trade secret may consist of any formula, pattern, device or compilation
of information which is used in one's business, and which gives him an opportunity to
obtain an advantage over competitors who do not know or use it." \textsc{Reformation of
Torts} § 757, comment b (1939).

\textsuperscript{62} See, e.g., \textsc{Fed. R. Civ. P. 26(c)(7)}; A.H. Robins Co. v. Fadely, 299 F.2d 557, 561
(5th Cir. 1962).

\textsuperscript{63} For example, an independent impartial expert may be interposed between
the parties. Or \textit{in camera} proceedings, with a sealed record, may be used. Protective
orders, preventing disclosure or use except for the litigation, are also commonly en-
tered.

\textsuperscript{64} A party with a right to disclosure of the ingredients of another's product is
not necessarily entitled to disclosure of the process for making that product. Baker v.
Proctor & Gamble Co., 17 F.R. \textsc{Serv.} 30b.352, Case 1, at 460 (S.D.N.Y. 1952). Similarly,
One aspect of this topic is whether software embodying trade secrets need be disclosed in agency proceedings. In certain cases, statutes or agency rules govern the situation, and the Freedom of Information Act applies to all federal agencies. Where deletion of certain matters would divest the material of its trade secrets, disclosure of non-privileged portions may be proper.

Instances where computer evidence may be sought in agency proceedings are legion. In Federal Trade Commission proceedings, for example, computer data bases and print-outs representing such confidential information as costs, sales, inventories, and customer lists may be demanded. In a Food and Drug Administration proceeding directed toward ascertaining the safety of a drug, statistical analyses of a large number of laboratory experiments may be necessary. Conversion of the raw data into useful numbers may well have been done by computer, with the validity of the investigation depending directly on the accuracy of the computer calculations. Or, computer calculations may play a role in determining the proper quality controls for a particular manufacturing process. Other agency situations involving the application of the trade secret privilege to computer evidence are also easily identifiable.

B. Government Secrets Privilege

There are three branches of this doctrine:

1. the privilege which applies to military and diplomatic "secrets of state";
2. the executive privilege which attaches to high officials and their papers; and,
3. the residual privilege which applies to certain other official information.

The scope of this privilege has been significantly impacted by the Freedom of Information Act. This privilege is pertinent to computer evidence because of the extensive scientific and techno-
logical research and development work carried on by government contractors and by the government itself, an ever increasing amount of which is performed with the aid of computers. 69 Many of the data bases (which may reflect in mathematical form the physical characteristics of military systems), programs (which may be designed to simulate such systems), and output (displaying system capabilities) may be classified. The privilege may be asserted when computer-related documents are sought. 70 In one computer-related case involving a claim of governmental secrets privilege, a third party attempted to secure documents relating to a license between a publisher and the Air Force for the use of the publisher's copyrighted material in the Air Force's computer legal retrieval system. 71

VI. CONCLUSION

Certain aspects of computer evidence law are emerging from the mist and beginning to assume faintly defined form. Most of the technical aspects of the admissibility of business record print-outs have been well litigated. The probative value of computer evidence and simulations appear to be areas which, in the near future, will see great activity. The past five years have seen a dramatic upsurge in the degree to which the importance of computer evidence generally has been appreciated, the next five years promise more of the same.

69. In 1970, for example, research and development expenditures in the United States amounted to $18 billion, with the federal government funding eighty percent of this. Barber, The American Corporation 134 (1970).

70. There are many situations where such a claim might arise. After a nuclear reactor accident, can parties obtain secret government computer output representing simulations of the reactor, and showing that the design was unsafe, and the accident foreseeable? When a new fighter plane crashes, can an injured party obtain secret government computer output indicating that the manufacturer knew the plan suffered from poor stability? If a destroyer of novel design breaks up on the high seas, can a party obtain secret government computer output showing that computer simulations were not properly conducted? Can a government security clearance file on tape be obtained in an employment discrimination action?
