*437

IDEA: The Journal of Law and Technology
1995

AUTHENTICATION OF COMPUTER-GENERATED EVIDENCE IN THE UNITED STATES

FEDERAL COURTS

Stanley A. Kurzban [n.a]

I. INTRODUCTION

This article discusses the authentication [n.1] of computer-generated evidence in the United States [n.2] federal courts. [n.3] The Federal Rules of Evidence [n.4] specify *438 what must be done to authenticate a document offered into evidence, but make no distinction between computer- generated evidence and other forms of documentary evidence. [n.5]

Businesses use computers to keep records. [n.6] Parties may enter such records into evidence at trials to make or buttress [n.7] points relevant to the issues involved. Business records entered into evidence under an exception to the hearsay rule are one type of computer-generated evidence. [n.8] In cases of computer-related crime or civil wrong, computer-generated evidence may be admissible under some other exception to the hearsay rule or not be hearsay at all; such evidence is a second type of computer-generated evidence. [n.9] A *439 third type of computer-generated evidence occurs in cases involving commercial transactions under computer-generated contracts between the parties. [n.10], [n.11] Parts II and III of this article treat each of the three types of computer-generated evidence in separate sections: A) Business records that are admissible as exceptions to the hearsay rule; B) Evidence in cases of computer-related crime; and C) Evidence of electronic contracts. Part II traces development of relevant law through pre-existing rules, case law, computer-specific rules and statutes, and authoritative treatises, with reference to current technology. Part III deals with the adequacy of current approaches and draws on technological references to project possible remedies for perceived inadequacies. Part IV summarizes the state of the law and its adequacy to meet future challenges.

II. BACKGROUND

Authentication of computer-generated evidence has thus far been governed by the principles, rules and statues that existed before computer usage became widespread. [n.12] The presumption then was that any documentary evidence would exist on paper and authentication lay in the testimony of the document's author or in verification of a signature. [n.13] The Federal Rules of Evidence contain several references to types of evidence that may be computer- generated. Rule 901(b) gives examples of how evidence might be authe nticated. [n.14] Especially pertinent to computer-generated evidence are *440 references to a "witness with knowledge," [n.15] whose testimony is required for admission of evidence, and a "process or system used" [n.16] for maintenance of the evidence. Rule 803(6), in listing an exception to the rule of hearsay, refers to "records . . . kept in the course of a regularly conducted business activity [n.17]. . . substantiated as by the testimony of a custodian or other qualified witness" [n.18] and alludes to the possible "lack of the evidence's trustworthiness" [n.19] that circumstances might connote.

Application of rules of evidence to computer-generated evidence requires analogizing computer-related processes to those that pre-dated the computer's invention. [n.20] When computers generate evidence, it may not actually be necessary that a "witness with knowledge" [n.21] of the record's creation testify [n.22] if a "qualified witness" [n.23] suffices to vouch for the actual *441 knowledge of the person entering data into a computer, [n.24] of the person preparing a record used by a person entering data into a computer, [n.25] or of the computer itself. [n.26]

The "process or system used" [n.27] involves not only procedures, but also computers and the programs that run on them. "Records . . . kept in the course of . . . business" [n.28] are electronic signals rather than pieces of paper. [n.29] Someone who is a "qualified witness" [n.30] may be anyone from someone present when a computer automatically records an event [n.31] to a senior programmer/analyst who uses a business's application program. [n.32] The word "trustworthiness" [n.33] may allude to the instances of error in use of the system [n.34] or to the effectiveness of security measures used to prevent unauthorized computer use. [n.35]

A. Business Records

Extant case law on the issue has dealt almost exclusively with entry of business records, [n.36] and thus has focused on Rule 803(6). In such cases, *442 decisions related to paper records bearing the same information have established precedents whose application has required relatively little strain because the analogy between ordinary paper and computer-generated business records is very straightforward. [n.37]

Business records may be admitted into evidence as exceptions to the hearsay rule if they are "made at or near the time [of the event in question] by . . . a person with knowledge, if kept in the course of a regularly conducted business activity . . . as shown by the testimony of the custodian or other qualified witness, unless . . . circumstances . . . indicate lack of trustworthiness." [n.38] The exception is predicated on, among other things, the reliance that a disinterested [n.39] business places on the record for the conduct of its business activity. [n.40]

In the absence of computers, operation of the rule is straightforward. Someone timely makes a business record and the business relies on the accuracy of its records. [n.41] If a business record is computer-generated, the *443 basic requirements for authentication persist. [n.42] Courts 'have addressed the questions of witnesses' qualifications and trustworthiness of records. [n.43]

In scrutinizing witnesses' qualifications, courts have been mindful that processes involving computers engender considerable trust in preservation of information from the moment of its entry into a computer to the time it is printed out. [n.44] Accordingly, the testimony of a hotel's Director of Communications who was on duty when a computer recorded a call provided sufficient authentication in United States v. Linn. [n.45] Successful challenges to witnesses' qualifications have all involved witnesses who were ignorant of the procedures involved in the processing of the records they were authenticating. [n.46]

As discussed immediately below, each challenge to a computer-generated business record's trustworthiness has addressed one or more of three subissues: general trustworthiness, reliability and security.Those parties *444 who have generally challenged the trustworthiness of record processing have succeeded only where the side offering computer-generated business records has introduced no evidence of computer systems' trustworthiness. [n.47] Some courts, especially state courts and particularly those that were speaking in the years before computer-aided record-keeping became commonplace, have discoursed at length about special tests of trustworthiness [n.48] that litigators could overlook only at their peril. The current federal standard, however, is reflected in United States v. Young Bros., Inc., which rejected any argument that computer-generated records were inherently less reliable, and so in need of greater foundation than paper records, [n.49] and United States v. Briscoe, [n.50] which cited United States v. Croft [n.51] in stating plainly that the proponent of computer-generated business records need only "provide sufficient facts to *445 warrant a finding that the records are trustworthy" to establish trustworthiness, and need not meet specific tests. [n.52] More recently, the court in United States v. Moore [n.53] went on to say that "ordinary business circumstances . . . suggest trustworthiness." [n.54] In holding that niceties of trustworthiness are, absent exceptional circumstances, more a matter of computer-generated evidence's weight than of its admissibility, [n.55] the circuit courts seem to be in general agreement. [n.56]

A few cases have involved specific grounds for challenging computer-generated records' trustworthiness. In United States v. Hayes, [n.57] the defendant alleged that the United States Internal Revenue Service had taken erroneous actions in reliance on its computers and placed the computer system's reliability in question, but the court dismissed the challenge. In United States v. Catabran, [n.58] there was extensive evidence of inaccuracies in processing of sales, but the court held they "affected only the weight of the printouts, not their admissibility." [n.59] In United States v. Glasser, [n.60] the defendant challenged the security that attended the use of the computer system, saying that "teller identification numbers were not kept confidential." [n.61] The court states: "The existence of an air-tight security system is not a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit *446 computer-generated records; the party opposing admission would have to show only that a better security system was feasible." [n.62]

B. Evidence in Computer-Related Cases

Authentication of computer-generated evidence may pose special problems in cases of computer-related crime. [n.63] Computer-generated evidence offered in the prosecution of a defendant accused of perpetrating a computer worm [n.64] or creating and triggering a logic bomb [n.65] within an application program[n.66] may be quite different from a business record. Requirements for such evidence's authentication may therefore be quite different from those for business records, but there is a dearth of relevant case law because while "computer criminals presented in the literature , especially in literature published by computer security specialists, seem to be . . . computer experts who use the most sophisticated modus operandi , " [n.67] " most computer criminals...are not highly qualified . . . experts." [n.68] A genius . . . appears in one of *447 every thousand cases . . . ." [n.69] In cases that involve computer-generated evidence that is not merely collaterally relevant business records, the defendant's rights under the First, Fourth, and Fifth Amendments to the United States Constitution may present impenetrable barriers to the mere collection of evidence, so that its authentication is never an issue. [n.70] In fact, the only federal case law relating to the authentication requirements for, as distinct from weight to be given to, [n.71] such evidence, [n.72] while suggesting that this type of computer-generated evidence may entail special requirements for authentication, [n.73] is merely dicta for lack of the evidence necessary to raise the special concerns involved. [n.74]

Heightened authentication requirements would have to address the strength of computer security mechanisms, which address specific threats to data's integrity. [n.75] Michael S. Baum [n.76] and Peter N. Weiss, Esq., [n.77] address the value of conventional security mechanisms such as access control and passwords [n.78] as well as incremental improvements thereon. [n.79] These, like locks on front doors of houses, are effective mechanisms for preventing *448 people with no extraordinary skills or privileges from effecting unauthorized access, the mechanisms entirely appropriate to business environments. [n.80] Their presence would bear on any challenge to computer-generated evidence's authenticity that might be based on prevention of unauthorized acts by a business's employees. [n.81] But such mechanisms do not provide protection from:

1. Data processing personnel who are authorized, because of their responsibilities for information processing systems, to modify the basic systems program, called an "operating system," that controls the computer in question; [n.82] or
2. Individuals who can gain electronic access to the computer in question and exploit lacunae, if there are any, in its operating system's defenses against modification. [n.83]

In cases that involve authorized individuals, either as accused perpetrators or as interested parties, conventional security mechanisms may be inadequate to establish computer-generated evidence's trustworthiness. [n.84] In cases that involve interested parties capable of gaining electronic access to computers that generate proffered evidence, the court may have to consider the effectiveness of mechanisms in place to eliminate or avoid unauthorized access. [n.85]

C. Electronic Contracts

The most challenging problem of authentication of computer-generated evidence involves commercial transactions. [n.86] Immense sums may hinge on establishing the authenticity of computer-generated evidence of the existence of a contract which one party seeks to repudiate. [n.87] While in most cases authentication of electronic contracts poses no special problems, there is a dearth of case law on this topic. Although many legal treatises, due to the *449 immense economies involved in digitizing contracts, have touched upon the subject, they have not kept up with technological developments that may affect cases where authentication is an issue of great financial moment. [n.88]

The history of authentication of binding writings, now called "contracts," is a long one. Oliver Wendell Holmes wrote of the use of a mark to authenticate a document in England prior to the Norman invasion. [n.89] The U.S. Supreme Court discussed authenticating seals with wax in Pillow v. Roberts. [n.90]

Courts adapted paper-derived rules for authentication to the telegraph and teletype. [n.91] As each medium came into greater use, courts came to accept the documents transmitted by those media as signed documents in the sense of relevant laws. [n.92]

The use of the handwritten signature to authenticate contracts has been commonplace for centuries. [n.93] What is most significant here is that "it is relatively insecure" [n.94] compared to a computer-generated signature. Whereas "only an expert may be able to detect a careful forgery," [n.95] the unfeasibility of forging computer-generated cryptographic signatures, called "digital signatures," is a matter of mathematical certainty. [n.96]

While detailed discussion of digital signatures appears in section III.C, a brief overview is appropriate here. In the general case, one who digitally signs a contract, or any other collection of digitized information, uses for the purpose a quantity called a "secret key," known only to the signer. [n.97] The *450 signer uses the secret key, two publicly known algorithms (called a "public key encrypting algorithm" and a "hashing function"), and the full text of the contract to create a digital signature that only someone knowing the secret key could possibly create. [n.98] Anyone can, by using a publicly known "public key" that corresponds in some mathematical way to the signer's secret key and a public key decrypting algorithm to recreate a hashed value from the contract, verify (and demonstrate to an impartial third party) that only one who knew the signer's secret key could have sent the contract. [n.99]

Baum indicates a continuing lack of case law regarding authentication of electronic contracts. [n.100] Concern that the rules of evidence were deficient in this regard [n.101] led to a number of efforts, described in brief immediately below, to remedy the deficiencies.

Baum's ABA committee [n.102] is addressing various intersections ofEDI and the law, including this article's focus. Baum, Linking Security and the Law, [n.103] is the best documentation of material related to the work of that committee. Baum also led the Electronic Messaging Services Task Force of the American Bar Association's Subcommittee on Electronic Commercial Practices, Uniform Commercial Code Committee, and Section of Business Law, which developed the Model Agreement, [n.104] for use by parties who thereunder agree to transact business electronically, and provides for cryptographic means of ensuring messages' integrity [n.105] and restricts the parties' right to contest the admissibility of digitally signed *451 documents. [n.106] The Task Force's report [n.107] and Model Agreement "were . . . submitted to the Secretary of the United Nations Commission on International Trade Law ('UNCITRAL')," [n.108] about which more appears immediately below.

The ABA's Section on Science and Technology's study of the authentication of computer-generated evidence in the context of the Uniform Commercial Code (UCC) [n.109] led to a panel discussion, "Evidentiary Challenges in the Global Electronic Environment," [n.110] at the ABA convention in New York City in August 1993. UNCITRAL continues similar work. [n.111]

The Association for Information and Image Management (AIIM) organized and sponsored a task force on the admissibility of records stored on computers as digitized images of paper records. Its guidelines [n.112] depend on the state of the law with respect to computer-generated evidence of other types. Its Section II-B-2 [n.113] addresses Rule 901(b)(9).

III. ANALYSIS

Authorities [n.114] cite no cases in which the rules governing authentication of computer-generated evidence have been so inadequate to their purposes that courts' holdings were inappropriate or unhelpful. Yet, one can easily argue [n.115] that there is substantial danger that existing precedents for authentication of computer-generated evidence will prove deficient in specific and foreseeable cases unless knowledgeable individuals work to ensure that advances are made in the field. The National Research Council argues that computers face growing risks, [n.116] which, if not taken into account, could render evidentiary standards obsolete.

*452 A. Business Records

By and large, computer-generated evidence in the form of business records is "like any other" such evidence. [n.117] Because the strictures applied to other paper apply so well to computer printouts, there is little reason to be concerned [n.118] that rules of evidence are inadequate to deal with their authentication for admission into evidence.

Establishment of standards for authentication of computer-generated evidence is like selection of methods for protection of data in that both depend on the value of the data involved and the likelihood that harm, whether accidental or malicious, will befall the data. [n.119] Thus far, the business records whose authenticity has most often been challenged when they were introduced into evidence havebeen records of telephone calls. [n.120] These records are typical in that the businesses that keep such records, in this case, telephone companies, have no reason to expend much of their resources ensure the accuracy of any individual record. Therefore, they protect entire files of records by creating redundant copies of the files from time to time and resorting to these if they have reason to suspect that the primary files are inaccurate. [n.121] This conduct is justified because, until the records appear at issue in particular cases, no one places very great value on any one record. Thus, one cannot assess the trustworthiness of the records by considering only the precautions taken against modifications of individual records. The business's whole procedure for maintaining records is relevant. But the very fact that the business relies on the accuracy of the records provides the assurance the court needs that the records are trustworthy. [n.122] This reinforces the Glasser court's assertion that "air-tight security . . . is not . . . a prerequisite to the admissibility of computer printouts." [n.123]

*453 Also justifying companies' decisions as to how much to invest in protecting individual records is the low risk of deliberate modification of such records to render them inaccurate. [n.124] Companies take minimal steps to protect themselves from such an act because they realize that its likelihood is low. [n.125] This is so because it is rare than an individual would have much to gain from modifying a record and such an individual is likely to lack the access and skill necessary to effect fraudulent modification. [n.126]

All the above leads to companies' affording business records less protection than might be apt in other circumstances, [n.127] such as those that attend the other two classes of computer-generated evidence this paper considers. However, the relatively low level of protection is commensurate with the risk that records will not be authentic. [n.128] Accordingly, standards for authentication should also be lower than might be appropriate for other types of computer-generated evidence. [n.129] The best guideline for such standard is that they should mirror the standards for proper equivalents except as the differences between paper and computer-generated records dictate. [n.130] One should expect businesses to take no better care to assure the authenticity of computer-generated records than they would to assure the authenticity of the paper equivalents.

Existing standards arguably not only meet but exceed that standard. Some courts' concern for standard equipment, reliable operation, correct repair, and the use of error-resistant procedures with computers [n.131] probably reflects jurists' unease with computers more than any need for increased vigilance necessitated by their use. Peritz [n.132] seems to infer untrustworthiness from his personal experience from around 1970, [n.133] newspaper-inspired misconceptions about personal computers, [n.134] and *454 congressional testimony that "only 1% of computer crimes are even detected." [n.135] The statement makes no sense. [n.136]

Donn Parker, who studies computer crime, after describing a business' computerization of its records, admitted that the "business is probably safer from crime in many ways after installing the computer." [n.137] This statement from an expert consulted for advice by those who fear for their data's security confirms the courts' view [n.138] that, as the Young Bros. court held, there is no reason to consider computer-generated evidence any less reliable than evidence on paper. [n.139]

Nonetheless, businesses increasingly permit access to their computers via open networks and telephone lines. [n.140] Before accepting computer- generated records into evidence as authentic, courts may demand evidence that the records are secure from attack by interested people outside the presumably disinterested business that maintains them. [n.141]

B. Evidence in Computer-Related Cases

Courts should be especially concerned about the authenticity of direct, rather than incidental, computer-generated evidence of wrongdoing, whether business records or not. [n.142] If evidence is germane to the issues of a case, successful counterfeiting of data may have a greater and more predictable effect on the outcome of a proceeding. In such cases, the defendants may be sophisticated users of computers. They may know how to tamper with computers and may assert, with cause, that others may have fabricated *455 computer- generated evidence to their detriment. For example, evidence that a particular individual created a damage-causing program [n.143] might be crucial to successful prosecution of a computer-related crime. This is a problem that may greatly expand in scope in the next few years and one which case law and the legal literature have not yet addressed in any but the most rudimentary fashion. Moreover, production of such evidence may involve creation of a paper record of data such as programs and logs, in detail that is not required for normal, day-to-day operations of business and so not considered part of the business's routine procedures. Such production may require skills that relatively few people have, and, most significantly, skills that would also make it possible for those same people to counterfeit data. Finally, those who produce the data may be employees or principals of a business that claims to have been victimized in the matter at issue and are therefore motivated to influence the case in a manner detrimental to the accused. [n.144] In such a case, heightened concern for the authenticity of computer-generated evidence is clearly warranted and may indicate court appointment of a disinterested expert.

In cases that involve production of evidence or even mere contact with evidence by persons who might not be disinterested parties, courts must consider the fact that such parties might be able to tamper with computer- generated evidence because of protection lapses [n.145] in evaluating the authenticity of computer-generated evidence.

C. Electronic Contracts

The immense economic potential of electronic contracting bespeaks a need to develop superior rules for the authentication of computer-generated evidence of valid electronic contracts. While the greatest volume of such contracts may involve parties accustomed to dealing with one another who require no special safeguards against repudiation, extraordinary means of authentication may be justified for those contracts that involve great sums, especially those in electronic funds transfer systems. [n.146] The appropriate mechanism is cryptographic digital signatures. [n.147] The following discussion *456 adds technological gloss and extensions to the treatment in section II. C above.

A contractor can append a cryptographic digital signature to a digital contract to provide the other party with practically irrefutable evidence of the contract's origin and contents. "Public key cryptography" (PKC) [n.148] makes this possible. Authentication for electronic documents can be "better than traditional handwritten signatures." [n.149] A United Nations report goes so far as to be dismissive of the authentication afforded by manual signatures. [n.150]

Cryptography involves a means for transforming information in such a way that the original information can be recovered only by performing a particular calculation. For example, if A transformed a number, 89, by multiplying it by 7, getting 89 x 7 = 623 as a result, A could get 89 back from 623 only by dividing by 7: 623 divided by 7 equals 89. The word "cryptography" comes from a root meaning "secret" and involves more than just a transformation; it must involve a secret of some sort as well. In the example above, the rule "divide by 7" might be a secret known only to the persons whom A wishes to be able to learn that "623" means "89." Alternatively, A might let everyone know that the type of transformation A performs, called "encryption," is multiplication and that the type of transformation needed to recover the original information, called "decryption," is division, but A tells only certain people that the number A uses, and the one they must use as well to recover the original information, is "7." In that case, the pair of processes, multiplication and division, is A's cryptographic "algorithm" and "7" is the (single) "key." That is, the secret information A shares with the people A authorizes to recover information A encrypts.

In PKC, each cryptographic communication, that is, each encryption-decryption pair, involves two keys, not one, and an algorithm that is quite complicated, far different from multiplication-division. One key, called a "private key," is a secret known to only one person and is used for either *457 operation, encryption or decryption; the other key, called a "public key," is not secret at all, but is associated openly with that person's name in a published register and is used for the inverse operation, decryption or encryption, respectively. That is, using first one key of the pair and then the other, in whichever order, will always result in recreation of the original data. If A encrypts information with A's secret key, anyone can decrypt it with A's non- secret public key and be certain that A encrypted the information, because A is the only person who knows the secret key that must have been used to encrypt the information.

If A sends someone a contract encrypted with A's secret key, the recipient can later demonstrate that A sent it and that it is unchanged because only A knows the secret key used to encrypt it and only the original contract would yield the precise encrypted value that A sent. [n.151]

PKC is relatively expensive to perform, [n.152] so one would like to use it on pieces of information far smaller than entire contracts. "Hashing" is a word that means transforming a large amount of information into a far smaller amount in such a way that very few items of information would yield the same result if similarly hashed. [n.153] For example, if every letter of A's contract were replaced by the number indicated its place in the alphabet and every line then by the sum of the values of the letters in it, those line numbers would represent the contract in a useful way: Very likely, no other contract would have the same value in terms of its line numbers. If A were to encrypt those line numbers with A's secret key and send the result to B, B could decrypt them with A's public key and demonstrate that A sent B that contract and not some other one, but A needed to encrypt far less than all of A's contract to accomplish the objective.

To permit signing of electronic contracts, the Unites States Department of Commerce's National Institute of Standards and Technology has, with the help of the National Security Agency, developed a Digital Signature Standard (DSS) [n.154] and a Digital Hashing Standard (DHS) [n.155], [n.156], [n.157] This *458 work demonstrates existing interest in digital signatures, which serve only to authenticate data, so may presage their appearance in, and possibly encourage their acceptance as a standard by, the courts.

The fact that only A knows A's secret key is what prevents A from repudiating a contract A sends B. If A tells others A's secret key, A can then claim that one of them might have created the information that B claims proves A sent B the contract. One way of preventing people from repudiating contracts by revealing their secret keys to others is to give them secret keys whose values even they do not know.

One can do that by placing the secret key and the machinery that uses it in an epoxy device that accepts input values and produces output values, encrypted with a secret key, but can be demonstrated to resist perfectly any attempt to determine the key itself. [n.158] In that case, the actual contract is tied to the device because only it can perform the necessary encryption.

One might try to repudiate a contract by denying possession of the device. [n.159] This would not be possible, however, if the device will encrypt only for its owner. Such a restriction can be built into a device that employs a biometric mechanism (for example, signature dynamics; that is, verifying that a signature is created by moving a pen just as the legitimate owner of a signature does when signing his or her name [n.160]) to verify that its owner is requesting encryption before performing same. [n.161]

Whether there is a market for the rather expensive and not-yet- marketed device described above, presumably for handling very large and sensitive transactions, is conjectural. [n.162] Only if such a market exists would *459 consideration of its legal implications in terms of authentication of computer-generated evidence be appropriate.

IV. CONCLUSION

Rules for authentication of computer-generated evidence are evolving from rules that apply to documents whose only existence was always on paper. This is appropriate and, in the case of business records that are incidental to a case, wholly adequate. Such records are admitted into evidence because of the trust that disinterested businesses place in them and that trust is independent of the record's medium, be it paper or computer storage device.

When cases involve individuals who are capable of tampering with computer- generated evidence, authentication that suffices for business records may well be inadequate. The presence in the case of individuals alleged to be capable of tampering with computers requires that courts consider the possibility of tampering in deciding whether proffered computer-generated evidence is authentic.

Electronic contracts present unique challenges of authentication. If authentication of such contracts remains a matter of contractual agreement between the parties, as per recent ABA work, [n.163] there is no obvious need for new law. If, however, the problem enters the legal area, law should be ready to deal with it.

[n.a]. The author has published numerous works on computer security since 1979, founded (in 1981) and later chaired the Association for Computing Machinery's Special Interest Group for Security, Audit, and Control (SIGSAC), serves on the Editorial Boards of two professional journals in the field of computer security, and is a student at Pace University School of Law. He chairs the Evidentiary working group of the Information Security Committee of the ABA's EDI and Information Technology Division in the Section of Science and Technology.

[n.1]. Fed. R. Evid. (hereinafter Rule) 901 states that "authentication" is "a condition precedent to admissibility" and "is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." That provides the context for this paper. Accordingly, this paper omits discussion of other considerations (e.g., hearsay and best evidence) that bear on the admissibility of computer-generated evidence and also of considerations that bear on the weight, as opposed to the admissibility, of computer-generated evidence's admissibility, see, e.g., Transport Indemnity v. Seib, 132 N.W.2d 871 (Neb. 1965) [hereinafter Seib]; Irving Younger, Computer Printouts in Evidence: Ten Objections and How to Overcome Them, in The Litigation Manual (1st Ed. 1983 American Bar Ass'n.) 204, 207, to be cited to the second edition in the material described infra in the text accompanying note 110; and Kevin J. Kotch, Addressing the Legal Problems of International Electronic Data Interchange: The Use of Computer Records as Evidence in Different Legal Systems, Temp. Int'l and Comp. L. J. 451, 459 (1992).

Note that there is a distinction between authentication for demonstrating evidence's admissibility and authentication of admitted evidence as part of a case. (See, e.g., Seib at 875.) This article addresses only the former, but the latter is a significant and closely related matter.

[n.2]. For information on other countries' treatment of the topic, see: England's English Civil Evidence Act, 1968, § 5 (Eng.) (cited in Younger, supra note 1, at 207); "The South Australia Evidence Act Part VI A, § 59a-c, as amended through 1975, reproduced in Computer Law Service, at app. 5-4. la (R. Bigelow ed. 1977)" (as cited in Rudolph J. Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 Nw. U.L. Rev. 956, 963, n31 (1986); see also Younger, supra note 1, at 207); Ken Chasse, "Legal Admissibility of Electronic Images as Documentary Evidence in Canada," presented at Imaging Canada, November 24, 1992, (a discussion of the relevant law and circumstances, similar to those in the United States, in Canada); Kotch, supra note 1, at 459 n.70; and Annex to Automatic Data Processing, Part V of United Nations Commission on International Trade Law Yearbook, Volume XVI: 1985, 351 [hereinafter UN], 362-65.

[n.3]. This article focuses on federal law in the United States, where there is no nationwide comprehensive law on the admissibility of computer-generated evidence. (Younger, supra note 1, at 207; Kotch, supra note 1, at 459.) Because state laws generally comport with the relevant federal laws of evidence, state cases are used hereinafter (see infra notes 6, 9, 17, 24, 26, 39, 42, 43 and 45) to illustrate some points. See N.C. Gen. Stat. § 55A-27.1 (1965) (cited in Monarch Federal Sav. and Loan Ass'n v. Genser, 383 A.2d 475, 483 (N.J. 1995) [hereinafter Monarch]; for less sweeping state laws specific to admission of computer-generated evidence, see Cal. Evid. Code § 1500.5 (West Supp. 1993) (computer-generated evidence as "best evidence") and Mo. Ann. Stat. § 659.094 (Vernon Supp. 1993) ("printouts shall be competent evidence") for admissibility of computer-generated evidence in computer crime trials; Iowa Code Ann. § 622.28 (West Supp,. 1993) ("including electronic means") for a state law applying to business records; and Iowa Code Ann. § 622.30 (West 1993) for a state law derived by adding "electronic data processing" to the Uniform Photographic Copies of Business and Public Records as Evidence Act, 14 U.L.A. 145 (1986), § 1.

[n.4]. Fed. R. Evid.

[n.5]. Michael S. Baum, Linking Security and the Law of Computer-Based Commerce, in United States Department of Commerce National Institute of Standards and Technology (NIST), Workshop on Security Procedures for the Interchange of Electronic Documents:

Selected Papers and Results (NISTIR 5247), (August 1993) [hereinafter NISTIR 5247] 27, 33 [hereinafter Baum, Linking Security and the Law].

[n.6]. United States v. Russo, 480 F.2d 1228, 1239 (6th Cir.), cert. denied, 414 U.S. 1157 (1973); see also King v. State ex rel. Murdock Acceptance Corp., 222 So. 2d 393, 398 (Miss. 1969).

[n.7]. The word is from State v. Ortiz, 448 A.2d 1241, 1246 (R.I. 1982).

[n.8]. United States v. Scholle, 553 F.2d 1109, 1125 (8th Cir.), cert. denied, 434 U.S. 940 (1977). See infra sections II. A and III. A. See infra text accompanying note 17 for the relevant portions of Rule 803(6), which embodies the exception.

[n.9]. Note, Appropriate Foundation Requirements for Admitting Computer Printouts into Evidence, Wash. U. L.Q. 59, 66 (Winter 1977). See e.g., United States v. Morris, 928 F.2d 504 (2d Cir. 1991) (defendant loosed a computer worm inside a collection of computer networks); see also Burleson v. State, 802 S.W.2d 429 (Tex. Ct. App. 1991) (defendant set and triggered logic bombs within his former employer's application programs). See infra sections II. B and III. B.

[n.10]. Michael S. Baum and Henry Perritt, Electronic Contracting, Publishing, and EDI Law (1991) [hereinafter Baum, Electronic Contracting]. See infra sections II. C and III. C.

[n.11]. Ronald L. Johnston, A Guide for the Proponent and Opponent of Computer-Based Evidence, 1 Computer/L.J. 667, 667 (1979) identifies only two types of computer-generated evidence, business records and simulations, and does not address authentication of the latter type. Our typology is more apt for contemporary cases.

[n.12]. John Robinson Thomas, Legal Responses to Commercial Transactions Employing Novel Communications Media, 90 Mich. L. Rev. 1145, 1147 (1992).

[n.13]. Id. at 1152; David Bender, Computer Evidence Law: Scope and Structure, 1 Computer/L.J. 699, 714 (1979). See infra text accompanying notes 89-93 for a discussion of means of validating authorship. Note that Rule 1001(3) ("[I]f data are stored in a computer . . . , any printout . . . is an 'original'.") obviates, for the present purposes, any distinction between evidence as it exists in a computer system and its representation on paper that is a printout from that system.

[n.14]. Rule 901(b) has many parts; only those relevant to computers are addressed here.

[n.15]. Rule 901(b)(1). In the case of paper, the witness needed knowledge of the creation, storage, and retrieval of the paper, but in the case of computer-generated evidence, the knowledge required of the witness extends to the domain of the computer involved, something which is more complex than a file cabinet.

[n.16]. Rule 901(b)(9). In the case of paper, the "process or system" is simply a way of maintaining records, but in the case of computer-generated evidence, it involves computer programming as well.

[n.17]. Rule 803(6). For discussion of distinctions between such business records and computer-generated evidence specially prepared for trial, see Peritz, supra note 2, at 959, and the cases discussed thereat: United States v. Russo, 480 F.2d 1228 (6th Cir. 1973) (annual report is a business record), cert. denied, 414 U.S. 1157 (1974); and Perma Research & Dev. v. Singer Co., 542 F.2d 111, 125 (2d Cir.) (Van Graafeiland, J. dissenting), cert. denied, 429 U.S. 987 (1976). See also United States v. Hernandez, 913 F.2d 1506, 1512-13 (10th Cir. 1990) (computer-generated evidence specially prepared for trial admissible under the hearsay exception for business records if the evidence merely represents admissible business records).

[n.18]. Rule 803(6). The "custodian" of evidence on paper requires no special skill, but the "custodian" of computer-generated evidence must be a person who is qualified to work with computers. See infra notes 30 and 44-46, and accompanying text.

[n.19]. Id. Courts have historically assumed the "trustworthiness" of records kept on paper, but the courts' assessments of the "trustworthiness" of computer-generated business records have varied greatly. See infra notes 33 and 47-62, and accompanying text.

[n.20]. Jerome J. Roberts, A Practitioner's Primer on Computer-Generated Evidence, 41 U. Chi. L. Rev. 254, 272 (1974).

[n.21]. Rule 901(b)(1).

[n.22]. Before codification of the Rules, 28 U.S.C. § 1732 (1989) read: "In any court . . . , any . . . record of any act . . . shall be admissible as evidence . . . if made in regular course of business . . . if [made] at the time of such act . . . . All other circumstances . . . , including lack of personal knowledge by the entrant or maker, may be shown to affect its weight, but ... not its admissibility." (Cited in Annotation, Business Record - Electronic Computer, 11 A.L.R. 3d 1377, 1378 n.6 (1965) superseded by Admissability of Computerized Private Business Records 7 A.L.R. 4th 8, (1994).) Congress adopted Rule 803(6) with the "understanding that its use of the phrase 'person with knowledge' preserved the meaning of the earlier statue, that is, that ... in light of the complex nature of modern business organizations[,] it is "coterminous with the custodian of the evidence or other qualified witness." (1974 United States Code Congressional and Administrative News 7051, 7063-64, (Senate Report No. 93-1277 on Pub. L. No. 93-595, 88 Stat. 1926, 1939 (1975), Oct. 11, 1974)); Conference Report of Dec. 14, 1974, made no mention of the phrase. (Id. at 7104.).

[n.23]. Rule 803(6).

[n.24]. Younger, supra note 1, at 206, citing King v. State ex rel. Murdock Acceptance Corp., 222 So.2d 393 (Miss. 1969).

[n.25]. Id.

[n.26]. See State v. Armstead, 432 So. 2d 837, 839 (La. 1983) (a computer automatically recorded the making of a telephone call). Interestingly, the court ruled that because the evidence was automatically recorded, it was relevant and therefore need not meet the standards for admission into evidence as a business record under the exceptions to the hearsay rule. Id.

[n.27]. Rule 901(b)(9).

[n.28]. Rule 803(6).

[n.29]. Roberts, supra note 20, at 274.

[n.30]. Rule 803(6); cf. Rule 901(b)(1). See infra text accompanying notes 44-46.

[n.31]. See United States v. Linn, 880 F.2d 209, 216 (9th Cir. 1989) (witness a hotel's Director of Communications).

[n.32]. See Burleson v. State, 802 S.W.2d 429, 440 (Tex. Ct. App. 1991); infra notes 65-66 and accompanying text.

[n.33]. Rule 803(6).

[n.34]. See United States v. Hayes, 861 F.2d 1225, 1228-29, (10th Cir. 1988) (defendant presented evidence that the United States Internal Revenue Service relied on its computer-generated records in making some incorrect refunds).

[n.35]. See United States v. Glasser, 773 F.2d 1553, 1559 (11th Cir. 1985) ("[T]eller identification numbers were not kept confidential.").

[n.36]. Halina S. Dziewit et al., The Quest for the Paperless Office - Electronic Contracting: The State of the Art Possibility but Legal Impossibility, 5 Santa Clara Computer and High Tech. L.J., 75, 82 (1989); Kotch, supra note 1, at 459; See Johnston, supra note 11, at 668-69; and Bender, supra note 13, at 715, for dated discussions on authentication of computer-generated business records.

[n.37]. See Rosenberg v. Collins, 624 F.2d 659, 665 (5th Cir. 1980); and United States v. Vela, 673 F.2d 86, 90 (5th Cir. 1982).

[n.38]. Rule 803(6). See parenthetical of United States v. Catabran, 836 F.2d 453, 457 (9th Cir. 1988), in United States v. Moore, 923 F.2d 910, 914- 15 (1st Cir. 1991); Central Fidelity Bank v. Denslow (In re Denslow), 104 B.R. 761, 764 (Bankr. E.D. Va., 1989).

[n.39]. Rosenberg, 624 F.2d at 665. Were the business not disinterested, the assumptions underlying the exception would be invalid. See People v. Lugasi, 205 Cal. App. 3d 434, 440 n.4 Cf. English Civil Evidence Act, 1968 § 6(3)(c) (Eng.), which calls for the admission of computer-generated evidence, but mandates regard for the question whether any person concerned had any incentive to conceal or misrepresent the facts. The same concern for disinterestedness might be inferred from Rule 803(6)'s allusion to "lack of trustworthiness." See supra, text accompanying note 19.

[n.40]. See Rosenberg, 624 F.2d at 665 and McCormick on Evidence, § § . 281, 286, and 287, cited in United States v. Fendley, 522 F.2d 181, 187 (5th Cir. 1975) (Godard, J. dissenting); see also United States v. Russo, 480 F.2d 1228, 1239, (6th Cir.), cert. denied, 414 U.S. 115 (1973).

[n.41]. See Rosenberg, 624 F.2d at 665; United States v. Russo, 480 F.2d 1228, 1239 (6th Cir.), cert. denied, 414 U.S. 1157 (1973).

[n.42]. United States v. DeGeorgia, 420 F.2d 889, 893 n.11 (9th Cir. 1969); See also Rosenberg, 624 F.2d at 665, citing United States v. Fendley, 522 F.2d 181, 184 (5th Cir. 1975). See United States v. Russo, 480 F.2d 1228, 1240 (6th Cir.), cert. denied, 414 U.S. 1157 (1973) and United States Fidelity & Guaranty v. Young Life Campaign, Inc., 600 P.2d 79, 81 (Colo. App. 1979) [hereinafter U.S. Fidelity] for discussions of how timely entry of data into computers meets the requirement for timely recording of data in business records.

[n.43]. King v. State ex rel. Murdock Acceptance Corp., 222 So. 2d 393, 398 (Miss. 1969), citing Annotation, supra note 22, at 1378 11 A.L.R. 3d 1377.

[n.44]. For example, the court in Olympic Insurance Co. v. H. D., Harrison, Inc., 418 F.2d 669, 670 (5th Cir. 1969) went so far as to say that computer-generated evidence had a "prima facie aura of reliability." This apparently reflected an overly credulous view that has led some to suggest that the familiar expression, GIGO, has come to stand not so much for the original "garbage in, garbage out," as for "garbage in, gospel out." (DanielT. Brooks, Computer Law: Current Trends and Developments, 272 PLI/Pat 515, 527 (1989).)

[n.45]. United States v. Linn, 880 F.2d 209, 216 (9th Cir. 1988). See also Kennedy v. LAPD, 901 F.2d 702, 717 (9th Cir. 1990) (widow of lawyer whose time records she entered into the computer an adequate witness); United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985) ("a billing supervisor" sufficed); DeGeorgia, 420 F.2d at 891 ("security officer"); Rosenberg, 624 F.2d at 665 ("comptroller"); United States v. Croft, 750 F.2d 1354, 1364 (7th Cir. 1984) ("Director of Payroll and Benefits Services"); and United States v. Young Bros., Inc., 728 F.2d 682, 694 (5th Cir. 1984), cert. denied, 469 U.S. 881 (1984); and state cases: D & H Auto Parts v. Ford Marketing Corp., 57 F.R.D. 548, 551 (E.D.N.Y. 1973) ("assistant controller"); State v. Armstead, 432 So. 2d 837, 841 (La. 1983) ("security manager"). For many additional examples, see Johnston supra note 11, at 672 n.19.

[n.46]. People v. Bovio, 455 N.E.2d 829, 833 (Ill. App. 2d Dist. 1983) (no testimony about computer equipment): U.S. Fidelity, 600 P.2d at 82 (no testimony about input); People v. Boyd, 384 N.E.2d 414 (Ill. 1978) (inter alia, no knowledge of equipment); and Arnold D. Kamen & Co. v. Young, 466 S.W.2d 381, 387 (Tex. Civ. App. 1971) (no personal knowledge of input). Note especially the view of the court in Zayre Corp. v. S. M. & R. Co., 882 F.2d 1145, 1149 (7th Cir. 1989), expressed in dicta while dismissing an appeal because the relevant point was not timely preserved, that the witness's title (here, "Controller") did not suffice to show the requisite knowledge; cf. supra note 45.

[n.47]. Bovio, 455 N.E.2d at 833; O'Shea v. International Business Machines, Inc. 578 S.W.2d 844 (Tex. Civ. App. 1st D. 1979); and Monarch, 383 A.2d at 488.

[n.48]. See, e.g., Burleson, 802 S.W.2d at 441; Note: In addition to proof that a computerized business record was made in the regular course of business at or near the time of the occurrence of the act, condition, or event recorded therein, proof may be required of the type of computer used and its acceptance as standard and efficient equipment, its methods of operation, the competency of its operators, and the method and circumstances of preparation of the record, including the sources of information on which it is based, the procedures for entering and retrieving information [into and] from the computer, and the controls and checks used, as well as checks made, to [e]nsure the accuracy and reliability of the record. (Donald M. Zupanec, M.D., J.D., Annotation, Admissibility ofComputerized Private Business Records, 7 A.L.R. 4th 8 § 2(a) at 13 (1981).) Many cases (id. § 3 at 15) illustrate the points listed. Rules vary widely in different jurisdictions; compare King, 222 So. 2d at 398 and Bovio, 455 N.E.2d at 833, which referred to a requirement for "standard equipment," with United States v. Hayes, 861 F.2d 1225, 1228-30 (10th Cir. 1988); and U.S. Fidelity, 600 P.2d at 81 (Colo. App. 1979), which dealt in few or no particulars. United States v. Scholle 553 F.2d 1109, 1125 (8th Cir.) cert denied, 434 U.S. 940 (1977) cited United States v. Russo, 480 F.2d 1228, 1229 (6th Cir.), cert. denied, 414 U.S. 1157 (1973) in referring to "the original source of the computer program . . . and the procedures for input control including tests used to assure accuracy and reliability" and the latter referred as well to "properly functioning equipment" (id.), but while the points stand 15 or more years later in those two circuits, no later decisions in those or any other federal districts stipulated such a requirement and the court in United States v. Vela, 673 F.2d 86, 90 (5th Cir. 1980), citing Rosenberg at 665, specifically declined to follow Scholle. See also United States v. Briscoe, 896 F.2d 1476 (7th Cir.), cert. denied sub nom., United States v. Usman, 498 U.S. 863 (1990) which placed no absolute condition on proof of "trustworthiness" and text accompanying notes 51-55. See Monarch, 383 A.2d at 481 for an exhaustive discussion of state standards as of 1975. See generally Roberts, supra note 20, at 276-79, for older cases beginning with Seib, 132 N.W.2d 871 (Neb. 1965); and Kotch, supra note 1, at 459.

[n.49]. Young Bros., 728 F.2d at 693.

[n.50]. 896 F.2d 1476 (7th Cir.), cert. denied sub nom., United States v. Usman, 498 U.S. 863 (1990).

[n.51]. 750 F.2d 1354, 1365 n.7 (7th Cir. 1984).

[n.52]. Briscoe, 896 F.2d at 1494-95. See: Association for Information and Image Management (AIIM), Performance Guidelines for Admissibility of Records Produced by Information Technology Systems as Evidence, in Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems, Part I, (May 1992), 2-5 [hereinafter AIIM], which, inter alia, quotes United States v. Downing, 753 F.2d 1224 (3rd Cir. 1985) as follows: "[W]hether a particular machine works as intended is a question distinct from one directed at a process generally." See also United States v. Liebert, 519 F2d 542, 547 (3rd Cir. 1975).

[n.53]. 923 F.2d 910 (1st Cir. 1991).

[n.54]. Id. at 915. See also Bender, supra note 13, 16 714. In focusing properly on businesses' reliance on records as evidence of their trustworthiness, courts have justifiably declined to accept Peritz's call (Peritz, supra note 2) for "an expanded foundation for admitting computerized business records into evidence . . . " (Id. at 960.) Even Peritz acknowledges that "records are seen as reliable evidence because of the business community's day-to-day reliance on them" (Id. at 957) and that "[t]he area of disagreement, if any, has shifted to the domain of probative value" (rather than authentication) (Id. at 972). See also infra text accompanying notes 122-139 and supra note 22.

[n.55]. Peritz, supra note 2, at 972.

[n.56]. Id. at 970.

[n.57]. 861 F.2d 1225, 1228-29 (10th Cir. 1988).

[n.58]. 836 F.2d 453, 458 (9th Cir. 1988).

[n.59]. Id.; See supra note 22 and text accompanying note 55.

[n.60]. 773 F.2d 1553 (11th Cir. 1985).

[n.61]. Id. at 1559.

[n.62]. Id.; See Schalk v. state, 823 S.W.2d 633, 637 and 643 (Tex. Ct. App. 1991), cert. denied, 112 S.Ct. 1763 (1992), for a discussion, citing Alois Valerian Gross, J.D., Annotation, What is Computer 'Trade Secret' Under State Law, 53 A.L.R. 4th 1046, § 7[a] (1987), of passwords' adequacy as a protective mechanism for trade secrets; and section III. A, infra, for further discussion of this point.

[n.63]. Mark Tantam, Investigating Computer Abuse, in Zella Ruthberg and Hal Tipton, eds., The Handbook of Information Security Management, 705, 710 (1993). See United States v. Khoury, 901 F.2d 948 (11th Cir. 1990) (law enforcers created false computer records in the hope of detecting illicit access thereto); and Burleson v. State, 802 S.W.2d 429 (Tex. Ct. App. 1991) (defendant maliciously modified his former employer's files). Note specialized computer crime statutes relating to the admissibility of computer-generated evidence: Iowa Code Ann. § 716A.16 (West 1993) ("printouts shall be admitted as evidence") and Mo. Ann.Stat. § 569.094 (Vernon Supp. 1993) ("printouts shall be competent evidence").

[n.64]. A "worm" is a program that places copies of itself in computers connected electronically to the one in which it is running. While a worm can simply take advantage of unused processing power in the remote computers to perform many similar computations simultaneously on different sets of data, a worm can be used less benignly. See United States v. Morris, 928 F.2d 504 (2d Cir. 1991); Eugene H. Spafford, The Internet Worm Program: An Analysis, Purdue Technical Report CSD-TR-823, Department of Computer Science, (1989); Cornell University, The Computer Worm: AReport to the Provost from the Commission of Preliminary Inquiry, (1989). The latter two are reprinted in the more extensive work, Peter J. Denning, Computers Under Attack: Intruders, Worms, and Viruses, 191 (part on "Worms," devoted almost exclusively to the Morris case) (1990).

[n.65]. A "logic bomb" is a program segment that suddenly begins to perform in a destructive way.

[n.66]. See Burleson, supra note 9; Buck BloomBecker, Spectacular Computer Crimes, 97 (1990).

[n.67]. Arthur Solarz, Lessons from a Swedish Study of Computer Crimes, 11 Computer Fraud & Security Bulletin, Number 2, 6, 11 (Dec. 1988).

[n.68]. Id. Accord John Taber, A Survey of Computer Crime Studies, 2 Computer/L.J. 275, 298-99 (Number 2, Spring 1980); National Research Council (N.R.C.), Computers at Risk: Safe Computing in the Information Age [hereinafter N.R.C.], 61 (1991).

[n.69]. BloomBecker, supra note 66, at 37.

[n.70]. Michael Gemignani, Viruses and Criminal Law, in Denning, supra note 56, at 489, 493. Gemignani refers to "a reasonable expectation that . . . computer files are private" (Id.), "search[] and seiz[ure]" (Id.), and requiring self-incriminating decryption of a file (Id.).

[n.71]. See supra, last paragraph of note 1.

[n.72]. See, e.g., United States v. Morris, 928 F.2d 504 (2d Cir. 1991) and Burleson v. State, 802 S.W.2d 429 (Tex. Ct. App. 1991), which involved detective work that could only have been done by people who clearly have all the skills and access they would need to fabricate evidence. See infra section III. B.

[n.73]. United States v. Bonallo, 858 F.2d 1427, 1436 (9th Cir. 1988).

[n.74]. Id. at 1436 (defendant, accused of altering bank records, which were admitted into evidence against him, alleges that someone else might theoretically have altered them, but the court held that he did "not provide any evidence to support that theory" (Id.)).

[n.75]. Ronald Paans, A Close Look at MVS Systems: Mechanism, Performance, and Security, 97-108 (1986).

[n.76]. Baum, Linking Security and the Law, supra note 5; Michael S. Baum, EDI and the Law [hereinafter Baum, EDI and the Law]; and Baum, Electronic Contracting, supra note 10, generally. Baum is Chairman of the Information security Committee of the EDI and Information Technology (EDI/IT) Division of the ABA's Section of Science and Technology. "EDI" stands for "electronic data interchange."

[n.77]. Peter N. Weiss, Security Requirements and Evidentiary Issues in the Interchange of Electronic Documents: Steps Toward Developing A Security Policy, in NISTIR 5247, supra note 5, 155, 165-66. Weiss is with the United States Office of Management and Budget.

[n.78]. See supra a text accompanying note 61 and, for a primer on such mechanisms, Appendix hereto, infra.

[n.79]. See, e.g., text accompanying and sources cited in note 162, infra.

[n.80]. See Baum, Linking Security and the Law, supra note 5, at 37.

[n.81]. See, e.g., United States v. Glaser, 773 F.2d 1553, 1559 (11th Cir. 1985).

[n.82]. Paans, supra note 75, at 98; Peter D. Goldis, Comparing MVS and UNIX Security: The View from the Glass House, 2 Information Systems Security, Numbers 3, 38, 44 (Fall 1993).

[n.83]. Ira H. Witten, Computer (In)security: Infiltrating Open Systems, in Denning, supra note 64, at 105; Paans, supra note 75.

[n.84]. Id.

[n.85]. See Id.; and generally, Goldis, supra note 82.

[n.86]. See generally Benjamin Wright, EDI and American Law (1989) [hereinafter Wright, EDI and Law] and Benjamin Wright. The Law of Electronic Commerce--EDI, Fax, and E-Mail: Technology, Proof, and Liability [hereinafter Wright, Law of Electronic Commerce] (1991); Baum, EDI and the Law (1989).

[n.87]. Baum, Electronic Contracting, supra note 10, at § 6.24, 345.

[n.88]. Id.

[n.89]. Oliver Wendell Holmes, The Common Law (1881), 272-30, cited in Baum, Linking Security and the Law, supra note 5, at 28 n.1.

[n.90]. 54 U.S. (13 How.) 472, 473-4 (1851), (court upheld the validity of a Wisconsin deed stamped on paper, in the face of an applicable Arkansas law requiring a seal on wax or wafer) cited in Baum, Linking Security and the Law, supra note 5, at 28 n.2.

[n.91]. See generally Douglas Robert Morrison, The Statute of Frauds Online: Can a Computer Sign a Contract for the Sale of Goods?, 14 Geo. Mason U. L. Rev., 637 (1992), which refers to Selma Savings Bank v. Webster County Bank, 206 S.W. 870 (Ky. 1918); and Thomas, supra note 12, at 1154-55, which refers to Hall v. Western Union Tel. Co., 162 F.657 (7th Cir. 1908) and Guynn v. Corpus Christi Bank & Trust, 589 S.W.2d 764 (Tex. 1979) for the respective media.

[n.92]. Thomas, supra note 12, at 1151-52.

[n.93]. See, e.g., Thomas, supra note 12, at 1150 (referring to the Statute of Fraudes, citing 29 (Car.2, ch. 3, § 17 (1677) (Eng.) (Id., n.25); and Stephen M. Lipton and Stephen M. Matyas, Making the Digital Signature Legal - and Safeguarded, Data Communications 41, 42 (Feb. 1978).

[n.94]. UN, supra note 2, at para. 55.

[n.95]. Id.

[n.96]. Lipton and Matyas, supra note 93, at 71; See also Baum, Linking Security and the Law, supra note 5, at 62.

[n.97]. Dziewit, supra note 36, at 93-94.

[n.98]. Id.

[n.99]. Whitfield Diffie and Martin Hellman, New Directions in Cryptography, IEEE Transactions on Information, Volume 22, Number 6, 644; See also Lipton and Matyas, supra note 68. Dziewit, supra note 36, at 94, cites O'Brien, A Signature for the Electronic

Letter, Telecommunications, Oct. 1985, 58bb, for the proposition that "the probability of two documents['] producing the same signature is less than one in 1,000 trillion." For example, if some number, N, is a function of every character of the contract, K, and of the secret key, S, of the sender, A, then the fact that the receiver, B, knows N is evidence that A, the only person who knows S, must have computed it, because neither B nor anyone else ignorant of S could possibly have computed N. The fact that A bothered to compute N and to send it to B is evidence of A's desire to enter into contract K with B.

[n.100]. Baum, Linking Security and the Law, supra note 5, at 32.

[n.101]. See generally Henry Peritz, supra note 2.

[n.102]. See supra note 76 for the full name of the committee. This author chairs its Evidentiary working group, which is preparing a proposed ABA resolution on the subject of the evidentiary treatment of digital signatures.

[n.103]. Supra note 5.

[n.104]. 45 Bus. Law. 1717 (1990) [hereinafter Model Agreement].

[n.105]. Electronic Messaging Services Task Force, The Commercial Use of Electronic Data Interchange--A Report and Model Trading Partner Agreement, 45 Bus. Law. 1645, 1696 n.209 [hereinafter EMSTF]. See Model Agreement, supra note 104, § § . 1.4, 1.5 and Comments thereto.

[n.106]. EMSTF, supra note 105, at 1695.

[n.107]. Id.

[n.108]. Jeffrey B. Ritter, Scope of the Uniform Commercial Code: Computer Contracting Cases and Electronic Commercial Practices, 45 Bus. Law. 2533, 2537 n.14.

[n.109]. Baum, Electronic Contracting, supra note 10, at § 6.20, 339.

[n.110]. Publication of the American Bar Ass'n; copy of material distributed at the convention on file with the author.

[n.111]. UN, supra note 2.

[n.112]. AIIM, supra note 52.

[n.113]. Id. at 2-4.

[n.114]. E.g., Younger, supra note 1, at 207.

[n.115]. See Baum, Linking Security and the Law, supra note 5, at 31.

[n.116]. N.R.C., supra note 68, at 10.

[n.117]. Rosenberg v. Collins, 624 F.2d 659, 665 (5th Cir. 1980).

[n.118]. Peritz, supra note 2, per supra note 54, notwithstanding.

[n.119]. Baum, Linking Security and the Law, supra note 5, at 45. See generally Robert V. Jacobson, The Need for Risk Analysis, in NISTIR 5247 supra note 5, at 77.

[n.120]. See, e.g., United States v. Briscoe, 986 F.2d 1476, 1494 (7th Cir. 1990); United States v. Linn, 880 F.2d 209, 216 (10th Cir. 1988); United States v. Miller, 771 F.2d 1219 (9th Cir. 1985); United States v. Vela, 673 F.2d 86, 90 (5th Cir. 1982); Rosenberg v. Collins, 624 F.2d 659, 665 (5th Cir. 1980); and State v. Armstead, 432 So. 2d 837 (La. 1983).

[n.121]. Paula Noyes Singer, Proposed Changes to the Federal Rules of Evidence as Applied to Computer-Generated Evidence, 7 Rutgers Computer & Tech. L.J. 157, 164 n.15.

[n.122]. See supra note 545 and text accompanying notes 39-40. See also Comment, Admissibility of Computer Business Records as an Exception to the Hearsay Rule, 48 N.C. L. Rev. 687, 689 (1970), as cited in Note, supra note 9, at 72-73 n.72.

[n.123]. United States v. Glasser, 773 F.2d 1553, 1559 (11th Cir. 1985); see supra note 62 and accompanying text.

[n.124]. But see Armstead, 432 So. 2d at 841 for a court's consideration of such a possibility.

[n.125]. Baum, Linking Security and the Law, supra note 5, at 47; and Baum, Electronic Contracting, supra note 10, at 184.

[n.126]. See Paans, supra note 75, at 100.

[n.127]. Baum, Linking Security and the Law, supra note 5 at 47 n.85.

[n.128]. Id; Wright, EDI and Law, supra note 86, at 5.

[n.129]. Baum, Linking Security and the Law, supra note 5, at 48.

[n.130]. See supra notes 15, 16, and 18.

[n.131]. See supra note 48 and accompanying test.

[n.132]. Peritz, supra note 2, at 990-99. See also Comment, supra note 122, at 76; Singer, supra note 121, at 171.

[n.133]. Id. at 990-91. Peritz refers without citing sources to "less knowledgeable users" (Id. at 990) and "great problems" (Id. at 991) than he saw earlier, but takes no account of improvements in security mechanisms and security administrators' techniques.

[n.134]. Id. at 991 n.183. Peritz states without citing a source that "intrusions occur regularly." (Id. at 991). For an authoritative and corrective view, see Witten, supra note

83. Note that what Peritz calls the "Milwaukee 14" (Id.) is the 414 Club, named for Milwaukee's telephone area code. (Peter J. Denning, Intruders, in Denning, supra note 64, at 143).

[n.135]. Id. at 992 n.184: The Federal Computer Systems Protection Act: Hearings on § 766 Before the Subcomm. on Criminal Laws and Procedures of the Judiciary, 95th Cong., 2d Sess. 4 (1978) (statement of Senator Biden) (estimate attributed to Professor August Bequai of American University Law School).

[n.136]. S. A. Kurzban, letter to the Editor, 5 ACM SIGSAC Review, vi (no. 1, 1987); see Robert V. Jacobson, letter to the Editor, 5 ACM SIGSAC Review iii (No. 2, 1987).

[n.137]. Small Business Computer Crime Prevention Act, H.R. 3075: Hearing Before the Subcomm. on Antitrust and Restraint of Trade Activities Affecting Small Business of the House Comm. on Small Business, 98th Congress., 1st Sess. 28 (1983) (testimony of Donn Parker).

[n.138]. See supra notes 48-56 and accompanying text.

[n.139]. United States v. Young Bros., Inc., 728 F.2d 682, 693 (5th Cir. 1984), cert. denied, 469 U.S. 881 (1984).

[n.140]. N.R.C. supra note 68, at 10; Ralph Spencer Poore, Security in Open Networks: A Contradiction in Terms, 2 Information Systems Security, No. 3, 18 (Fall 1993).

[n.141]. See United States v. Morris, 928 F.2d 504 (2d Cir. 1991); Clifford Stoll, the Cuckoo's Egg (1991) and sources cited supra note 64 for a case in which a perpetrator penetrated the defenses of systems attached via networks, as many business systems are; and N.R.C., supra note 68, at 11, and Witten, supra note 83.

[n.142]. See supra section II.B.

[n.143]. See Morris, supra note 9; United States v. Bonallo, 858 F.2d 1427 (9th Cir. 1988); and Burleson v. State, 802 S.W.2d 429 (Tex. Ct. App. 1991).

[n.144]. See Burleson, supra note 143.

[n.145]. See e.g., Ruthberg and Tipton, eds., supra note 63, generally; Paans, supra note 75, at 111-21; and Goldis, supra, note 82, generally.

[n.146]. Henry H. Perritt, The Electronic Agency and the Traditional Paradigms of Administrative Law, 44 Admin. L. Rev. 79, 102 (1992).

[n.147]. See supra text accompanying notes 97-99. See also Baum, EDI and the Law, supra note 62, at 202; Electronic Contracting, supra note 10, at 43, 57, 58, 70 and 71; Wright, EDI and Law, supra note 62, 97; and Wright, Law of Electronic Commerce, supra note 62, at § 1.3.2.

[n.148]. See supra, note 99.

[n.149]. Weiss, supra note 104, at 158 n.6, quoting Perritt, supra note 111, at 94. See also Stasia M. Williams, Something Old. Something New: The Bill of Lading in the Days of EDI, 1 Transnat'l L. & Contemp. Probs. 555, 575 n.146 ('written signatures can be forged more easily than a [public key cryptography] digital signature," citing Chris Reed, Authenticating Electronic Mail Messages - Some Evidentiary Problems, 4 Software L. J. 161, 172.

[n.150]. UN, supra note 2 § 55: "Even where a specimen of the authorized signature is available for comparison, only an expert may be able to detect a careful forgery. Where large numbers of documents are processed, signatures are sometimes not even compared except for the most important transactions."

[n.151]. Dziewit, supra, note 36, at 95, contains another discussion of the subject.

[n.152]. Miles E. Smid, Cryptography, in Ruthberg and Tipton, eds., supra note 63, at 653, 655.

[n.153]. 58 Fed. Reg. 27712-02 (1993).

[n.154]. See 56 Fed. Reg. 42980-02 (1991).

[n.155]. See 58 Fed. Reg. 27712-02 (1993) and, generally NIST, Security Issues in the Use of Electronic Data Interchange (EDI) in Bulletin of the National Institute of Standards and Technology Computer Systems Laboratory (June 1991).

[n.156]. Baum, Electronic Contracting, supra note 10, at § 4.29, 202 n.202 n.210; and Dziewit, supra note 36, at 95 n.101, citing O'Brien, supra, note 74, refer to the fact that a patent, U.S. Patent No. 4,405,829, covers a public key cryptosystem. This author cannot say whether DSS is covered thereby.

[n.157]. As to PKC-less digital signatures, see Ralph C. Merkle, A Certified Digital Signature, in Advances in Cryptology - CRYPTO '89 Proceedings, 218 (1990).

[n.158]. See Steve H. Weingart, Physical Security for the [micro] ABYSS System, in Proceedings of the 1987 IEEE Symposium on Security and Privacy, 52, 55 (1987); and D. G. Abraham et al., Transaction Security System, 30 IBM Systems Journal 206, 218 and 215.

[n.159]. "Failure of one of the principles to notify other parties that his digital signatures have been compromised and may be subject to use by unauthorized agents may be deemed his own negligence, and might defeat any defenses he may later raise as to the authority of his agents." (Lipton and Matyas, supra note 68, at 48.) A report due soon from the Commission of the Common Market on "Legal Aspects of Authentication, Storage and Coding" will take the position that anyone surrendering the device is legally responsible for anything it encrypts. (Peter Landrock, private communication on file with the author.)

[n.160]. See United States Congress office of Technology Assessment, Defending Secrets, Sharing Data - New Locks and Keys for Electronic Information, 80 [hereinafter OTA]; and Brian J. B. Cope, Biometric Systems of Access Control, 18 Electrotechnology (No. 2) 71 (April-May 1990).

[n.161]. See Raymond Wong et al., Polonius: An Identity Authentication System, Proceedings of the 1986 IEEE Symposium on Security and Privacy, 101 (1986); and Addison Fischer, Public Key Cryptography in Action, 3 Information Systems Security No. 1 (Spring 1994), at 57, 66, for owner-authenticating smart cards; and D. G. Abraham et al., Transaction Security System, 30 IBM Systems Journal 206, 221 for a description of a biometric device.

[n.162]. But see id. at 210, 211 for a discussion of market exploration conducted by International Business Machines Corporation.

[n.163]. See supra text accompanying note 106.

*460 APPENDIX

"Access control" is the association of every user of a computer with every privilege those in control of the computer have authorized the user to exercise. If a computer controls access, there is assurance, to the extent that the control is effective, that no unauthorized access takes place.

Computers identify users by some authenticating act the users perform when they begin a series of interactions with the computer. The prototypical act is the entry of a secret piece of information, called a "password," presumed to be known only to them. More reliable authenticating acts include supplying a device, called an "artifact" in the technical literature, and manifesting a characteristic, such as a signature or a fingerprint. [n.164] For a thorough discussion of security mechanisms, see relevant chapters in The Handbook of Information Security Management. [n.165]

[n.164]. See OTA supra note 160, at 77-83.

[n.165]. William H. Murray and Stanley A. Kurzban, Chapters II-4-1 through II-4-3, in Ruthberg and Tipton, eds., supra note 63, 515-550 (1993).