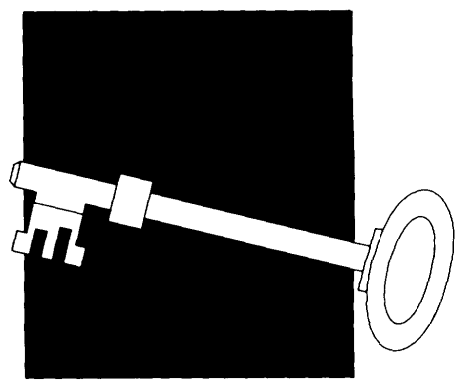
Legal Issues and Information Security 3

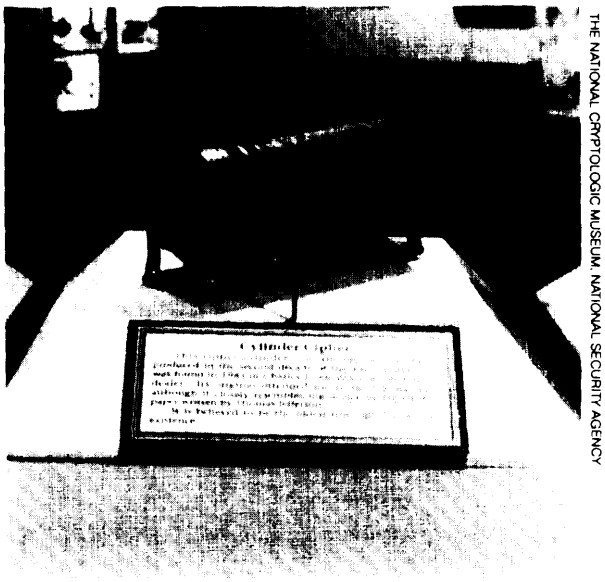
Laws develop in response to society's needs. They evolve in the context of the mores of the culture, business practices, and technologies of the time. The laws currently governing commercial transactions, data privacy, and intellectual property were largely developed for a time when telegraphs, typewriters, and mimeographs were the commonly used office technologies and business was conducted with paper documents sent by mail. Technologies and business practices have dramatically changed, but the law has been slower to adapt. Computers, electronic networks, and information systems are now used to routinely process, store, and transmit digital data in most commercial fields. As the spread and use of information technologies in the business world have quickened, the failure of current laws to meet the needs of a digital, information-based society has become apparent.

This chapter spotlights three areas where changes in communication and information technologies are particularly significant:

1. **Electronic commerce.** As businesses replace conventional paper documents with standardized computer forms, the need arises to secure the transactions and establish means to authenticate and provide *nonrepudiation services for electronic transactions,* that is, a means to establish authenticity and certify that the transaction was made. Absent a signed paper document on which any nonauthorized changes could be detected, a substitute for the signature and a means to prevent, avoid, or minimize the chance that the electronic document has been altered must be developed.



2. **Protection of privacy in data and the international effect of efforts on the part of the European Union** (EU) **to protect personal information.** Since the 1970s, the United States has concentrated its efforts to protect the privacy of personal data on those data collected and archived by the federal government. Rapid development of networks and information processing by computer now makes it possible for large quantities of personal information to be acquired, exchanged, stored, and matched very quickly. As a result, a market for computer-matched personal data has expanded rapidly, and a private-sector information industry has grown around the demand for such data. Although the United States does not comprehensively regulate the creation and use of such data in the private sector, foreign governments (particularly the European Union) do impose controls. The difference between the level of personal privacy protection in the United States and that of its trading partners, who in general more rigorously protect privacy, could inhibit the exchange of data with these countries. [1]
3. **Protection of intellectual property in the administration of digital libraries. The** availability of protected intellectual property in networked information collections, such as digital libraries and other digital information banks, is straining the traditional methods of protection and payment for use of intellectual property. Technologies developed for securing information hold promise for monitoring the use of protected information, and provide a means for collecting and compensating the owners of intellectual property.



19th-century "cipher wheel" believed to be the oldest extant encryption/decryption device.

ELECTRONIC COMMERCE

Businesses are increasingly using electronic messaging, networked computers, and information systems for conducting business that was once transacted solely on paper or by telephone. Electronic commerce is rapid and accurate and can reduce the cost of doing business. Electronic mail, facsimiles, and standardized electronic business forms are transforming the marketplace, changing the way that business is transacted, and causing firms to restructure operations.[2] Distance is no longer a significant barrier. Business can be conducted as quickly and easily halfway around the world as it once was up and down Main Street, USA. For example, automated electronic business

[1] Some commentators suggest that there maybe a subtext in some of the EU activities in this area, including the desire on the part of some to create a "Fro-tress Europe" or to negotiate certain national concerns into law for the entire EU. (Susan Nycum, attorney, Baker & McKenzie, personal communication, June 1994.) Others question whether it is possible to fairly evaluate the motivations for the EU approach to determine whether they are due to cultural differences or economic competition (Richard Graveman, Member of Technical Staff, Bellcore, personal communication, April 1994.)

[2] U.S. Congress, Office of Technology Assessment, *Electronic Enterprises: Looking to the Future*, OTA-TCT-600 (Washington, DC: US. Government Printing Office, May 1994).

transactions, such as Electronic Data Interchange (EDI), enable businesses to contract for sale of goods electronically, process purchase orders, invoice for the transaction, and issue shipping notices in a one-step process. EDI is available to businesses that can access a network with the requisite hardware and software for generating messages and forms with a standard EDI format. EDI has existed since the 1970s; though its use continues to grow, it is only an evolutionary step in the development of the electronic marketplace in the global economy. In the future, data and information will flow freely among international trading partners and firms as electronic commerce displaces the traditional forms of business transactions. However, the universal acceptance of networks for transacting business requires security measures to ensure the privacy needed for commercial transactions in a global competitive environment. Security measures that provide assurance that the authenticity and integrity of a communication have not been compromised will tend to support the enforceability of agreements by the legal system.

While electronic computer messaging technology allows many business transactions to be handled in a paperless fashion, the law of contract and commerce is still based on a paper system paradigm. As a result, businesses confront new legal issues as they implement electronic trading systems. Among these are questions regarding contractual writing requirements, legally binding signatures, and use of electronic communications as evidence of a contract. Government and industry can only make use of these capabilities if electronic transactions are secure and enforceable. The security issues that must be dealt with are: 1) requirements for authentication of the source of a transaction, 2) assurance that the message content is unaltered, 3) prevention of disclosure of the transaction to unauthorized persons, and 4) verification of receipt of the transaction by the intended trading partner.

Statute of Frauds and Electronic Commerce: The Writing and Signature Requirement

The Statute of Frauds was developed primarily to discourage fraud and perjury in proving the existence and content of a contract. Its essential function is to bar proof of certain contracts unless a sufficient writing exists for certain transactions.[5] The Statute of Frauds demands at least some evidence of a contract; a party may not claim that an oral contract or modification was made without submitting some proof. One method of proof is that the contract be memorialized, i.e., set forth with certainty, in a signed writing.

Section 2-201 of the Uniform Commercial Code (U.C.C.) (for discussion of the U.C.C. and security requirements, see box 3-1), which is the U.C.C.'s Statute of Frauds, requires that all contracts for the sale of goods over $500 be in a writing sufficient to indicate that a contract for sale has been made and signed by the party, or the party's

[3]However, oral contracts are binding in many situations.

BOX 3-1: The Uniform Commercial Code and Network Security

Article 4A of the Uniform Commercial Code, which regulates electronic funds transfers, is an example of a provision that creates an incentive for parties to implement commercially reasonable security procedure, to detect fraud.[1] Section 4A-201 defines a security *procedure* as follows.

> [A] procedure established by agreement of a customer and a receiving bank for the purpose of (t) verifying that a payment order or communication amending or canceling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order is that of the customer, or (iii) detecting error in the transmission or the content of the payment order or communication. A security procedure may require the use of algorithms or other codes, identifylng words or numbers, encryption, callback procedures, or similar security devices. [2]

Security procedures are specifically referred to in section 4A-205, which governs erroneous payment orders, and sections 4A-202 and 4A-203, which govern the authorization and verification of payment orders.[3] Although the decisions of whether and to what extent security procedures will be used are left to the parties,[4] these sections are drafted to provide incentive to both parties to the transaction to implement security procedures

Section 4A-205 provides the party sending an order electronically with incentive to bargain for the implementation of security procedures Under section 4A-303, the sender of an erroneous or incorrect order Is, generally, liable [5] Section 4A-205, however, allows the sender to shift the risk of loss to the receiving bank if 1) the sender and receiver have Implemented security procedures, 2) the sender can prove that the sender or the person acting on the sender's behalf compiled with the security procedures, and, (3) had the receiving bank also complied, the errors would have been detected.[6] Section 4A-205 does not apply unless both parties agree to the Implementation of security procedures [7] Security measures are not effective unless both the sender and the receiver comply with the procedure [8]

---

[1] William Lawrence, "Expansion of the Uniform Commercial Code Kansas Enacts Article 4A, " VOI 59, *Kansas Bar Association Journal*, at 27, 33, (September 1990)

[2] Uniform Commercial Code Section 4A-201 (1992)

3 Ibid , sec 4A-201 comment

[4] Ibid , sec 4A-205 comment 1

5 Ibid , sec 4A-303

6 Ibid , sec 4A-205(a)(l) and comment 2 to 4A-205

[7] U C C sec 4A-205 comment 1

8 Ibid , sec 4A-205 comment 2

authorized agent or broker, against whom enforcement is sought.[4] The comment to section 2-201 states that a writing sufficient to satisfy the section must meet only three "definite and invariable" requirements: the writing must evidence a contract for the sale of goods, must be *signed,* which ineludes any authentication identifying the party to be charged, and must specify the quantity.[5]

---

[4] An increasingly important area of inquiry in the discussion of electronic commerce pertains to electronic transactions when the subject matter of the transfer is information. An example of such a question is: what type of contracting will occur when, through use of electronic search tools (e.g., "gophers") information databases can be sought out, entered. and data extracted (for a fee), without any direct human involvement in accepting or rejecting a contract. For further analysis of such issues, see R. Nimmer and P. Krauthaus, "information as Property Databases and Commercial property," *International Journal of Law and Information Technology, vol. 1, No. 1, 1993,* p. 3; and R. Nimmer and P. Krauthaus, "Information as Commodity: New imperatives of Commercial Law," *Law and Contemporary Problems, vol. 55, No.* 3, summer 1992, p. 3.

[5] U.C.C. section 2-201, comment 1 (1 992).

BOX 3-1 (cont'd.): The Uniform Commercial Code and Network Security

Similarly, section 4A-202 provides the receiving bank with an Incentive to use security procedures Under subsection b, the receiving bank can shift the risk of loss to the customer if an unauthorized payment order is accepted by the receiving bank in compliance with commercially reasonable security procedures [9]

Under Article 4A, what constitutes "commercially reasonable" security measures IS a question of law.[10] Factors important in this analysis include the type of customer, the frequency and size of the customer's payment orders, and the security procedures used by similar banks and customers.[11] The purpose of subsection b is not to make banks ensure against fraud, but rather to encourage them to use commercially reasonable safeguards against fraud.[12]

Article 4A also provides parties with an incentive to keep codes and procedures confidential and computer access guarded A person who fraudulently breaches a commercially reasonable security procedure must have knowledge of how the procedure works as well as the codes and identifying devices.[13] Such a person must also have access to the transmitting facilities, either through open computer terminals or other software.[14] If the customer can prove that the person committing the fraud did not receive such confidential Information from the customer or the source controlled by the customer, the loss shifts to the bank.[15]

A receiving bank needs objective criteria in order to determine whether it should act on a payment order.[16] A comment to section 4A-203 suggests types of security measures parties may use.[17] Bank employees may be trained to "test" a payment order, or customers may designate guidelines for the bank's acceptance of payments, such as limiting payments to authorized accounts, amounts or beneficiaries.[18]

9 Ibid, sec 4A-203 comment 5 and sec 4A-202(b)
10 Ibid sec 4A-202(c) and 4A-203 comment 4
11 Ibid, sec 4A-202(c)
12 Ibid sec 4A-203 comment 4
13 Ibid sec 4A-203 comment 5
14 Ibid
15 Ibid sec 4A-203(a)(2) & comment 5
16 Ibid, sec 4A-203 comment 3
17 Ibid
18 Ibid

In evaluating electronic communications, the question arises whether there is a *writing* and a *signature* as required by U.C.C. section 2-201. Section 1-201 (39) defines signed as including any symbol executed or adopted by a party with present intention to authenticate a writing. Section 1-201 (46) defines *written* as including printing, typewriting, or any other intentional reduction to tangible form.[6]

One of the primary goals of electronic messaging is the elimination of paper transactions, which ultimately means the elimination of conventional writings. Maintaining a paper trail to guard against possible problems with the Statute of Frauds diminishes the objectives of computer contracting. No judicial decision answers the question of whether electronic communication

6 Electronic Messaging Services Task Force, Committee on the Uniform Commercial Code, "The Commercial Use of Electronic Data Interchange-A Report," 45 *Business Lawyer* 1645, at 1682 (June 1990).

satisfies the Statute of Frauds writing and signing requirements.[7]

In addition, no clear conventions or rules control the formation of contracts via electronic messaging. Statutes and regulation governing the enforceability and recording of business transactions generally refer to documents, writings, and signatures—not electronic messages, data logs, and authorization codes.[8] To eliminate any question about writing requirements and the legality of signatures, parties can enter into a trading partner agreement. With respect to writing requirements, such an agreement may adopt one or more of several different provisions. The agreement may: 1) redefine the term writing; 2) provide that the parties not challenge the validity of electronic messages merely on the basis that they are in electronic form; and 3) provide that the parties accord electronic messages the same status as paper messages. Trading partner agreements can also eliminate questions about the legality of electronic signatures, by providing that specified electronic codes serve as effective signatures.[9] (One means by which this can be accomplished involves what are called *digital signatures. See below* and chapter 4).

In the absence of trading partner agreements, contracting parties must await court decisions of changes in laws to assure trading partners that electronic contracts would not be rendered unenforceable. Legislative modifications have been proposed.[10] Among these are:

- change the U.C.C. 's definition of a *writing* to include properly communicated electronic communications as reduced to tangible form;
- change the definition of *signed to* include proper, nonreputable electronic signatures;
- define electronic signatures;
- delete the use of the word *authenticate* from the definition of *signed* or define it; and
- define *identify* in the definition of *signed.*[11]

The National Conference of Commissioners on Uniform State Laws is currently undertaking a revision of U.C.C. Article 2. Among the current draft proposals is to eliminate the Statute of Frauds entirely for sales of goods. The basis for this proposition includes the conclusion that the Statute of Frauds does not protect the important interests in the modem contractor commercial environment, but does prevent assertion of some otherwise valid claims.

Electronic Commerce and the Rules of Evidence: Data Integrity and Nonrepudiation

For an electronic message to survive a challenge to its authenticity, a party must prove the message originated from the sender and was not altered after dispatch from the sender. Evidence of adequate safeguards enhance the reliability of records, the ability to prove substantive terms of the commercial transaction, and the likelihood that the computer record will be admitted into evidence to

---

7 D.L. Wilkerson, "Electronic Commerce Under the U.C.C. Section 2-201 Statute of Frauds: Are Electronic Messages Enforceable?" 41 *Kansas* Law Review 407-408 (1992).

8 Ibid.

9 An United Nations Commission on International Trade Law (UNCITRAL) Working Group on Electronic Data Interchange is currently drafting a set of Uniform Draft Rules on these issues (see A/CN.9/WG.IV/WP.60, Jan. 24, 1994) for adoption by national legislators when reviewing legislation. The American Bar Association Section of Science and Technology, Information Security Committee is also drafting rules of practice and commentary on certification authorities for a global public key infrastructure.

10 While some would suggest wholesale elimination of the statute, doing so would affect more than electronic contracts and would constitute a significant change in the U.C.C. It would also require support form the legal community. Modifying the statute to address a subset of electronic communications is believed by some to be a more pragmatic approach.

11 M. Baum, "Electronic Contracting in the U. S.: The Legal and Control Context," *EDI and the Law, 1.* Walden (cd.) (London: Blenheim Online, 1989), p. 135.

12 Raymond T. Nimmer, University of Houston Law Center, persona] communication, July 1994.

show a *writing* in accordance with U.C.C. section 2-201. If a party fails to show that it has reasonably protected its business records and data, its credibility would be damaged should it assert its records to be superior to the records of another party that properly guarded its records. Without proper controls, a recipient or other third party can alter electronic mail messages, which renders the computer printout unreliable as evidence. However, the burden of proof of establishing that messages have been properly handled may be imposed on different parties in different circumstances, whether sender, recipient, or third-party challenger. The characteristics associated with the evidentiary value of electronic documents are often asserted to be essentially the same as those associated with maintaining the security of the information. This need to show adequate controls is similar in the field of trade secret law.] [3]

Case law concerning the admissibility of computer printouts supports the proposition that computer data can be sufficiently reliable to provide trustworthy evidence of the existence of a contract. For instance, courts rarely have excluded reliable computer evidence under the best evidence rule, which generally requires that only the original writing be admitted into evidence. Rule 1001 (3) of the Federal Rules of Evidence states: "If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'"

Computer data compilations are admissible as business records under rule 803(6) if a party establishes the proper foundation for the reliability of the records. Business records must be kept in the course of regularly conducted business activity. In addition, records are reliable only to the extent they are compiled conscientious] y and consistently.[14] Rule 803(6) requires that an opposing party has an opportunity to inquire about production, maintenance, and accuracy of the records, to ensure that records admitted into evidence are trustworthy.

Electronically filed federal records are often offered as business records prepared in the ordinary course of business. [15] The proponent offering the evidence seeks to demonstrate the authenticity and reliability of the information, and the opponent tries to challenge those assertions:

> [T]he foundation for admission of (computer records) consists of showing the input procedures used, the tests for accuracy and reliability and the fact that an established business relies on the computerized records in the ordinary course of carrying on its activities. The (opposing) party then has the opportunity to cross-examine concerning company practices with respect to the input and as to the accuracy of the computer as a memory bank and retriever of information . . . [T]he court (must) ● 'be satisfied with all reasonable certainty that both the machine and those who supply its information have performed their functions with utmost accuracy . . . [T]he trustworthiness of the particular records should be ascertained before they are admitted and . . . the burden of presenting an adequate foundation for receiving the evidence should be on the parties seeking to introduce it rather than upon the party opposing its introduction."[16]

Thus, the law of evidence in this context requires the following:

---

13 Assertion of a trade secret "often entails establishing that affirmative and elaborate steps were taken to insure that the secret claimed would remain so." *Amoco Production Company v. Lindley*, *609* P. 2d 733 (Okla. 1980)

14 The defendant in *United States v. Briscoe*, 896 F.2nd 1476 (7th Cir. 1990) argued that, as shown in *United States v. Weatherspoon*, *581* F.2nd 595 (7th Cir. 1978) computers must be tested for internal programming errors on a monthly basis. The Briscoe court held that, although such evidence was presented in *Weatherspoon*, the admission of computer records does not require such a showing.

15 P.N Weiss, "Security Requirements and Evidentiary Issues in the Interchange of Electronic Documents: Steps Toward Developing a Security Policy," *Worldwide Electronic Commerce—Conference Proceedings (New* York, NY: Jan. 16-18, 1994), p. 220.

16 *United States* v. *Russo*, 480 F. 2d 1228 (6th Cir. 1973).

1. proof that an electronic communication actually came from the party that it purports to come from;
2. proof of the content of the transaction, namely, the communications that actually occurred between the parties during the contract formation process;
3. reducing the possibility of deliberate alteration of the contents of the electronic record of the transactions; and
4. reducing the possibility of inadvertent alteration of the contents of the electronic record of the transactions. [17]

These concerns about the authenticity of the identification of the originator, with the integrity of the content of the communication, and reducing the likelihood of alteration, which are at the heart of the law of evidence, are the same concerns that must be addressed in the context of electronic commerce. Security measures that provide assurance that the authenticity and integrity of a communication have not been compromised will also provide a high degree of confidence that the contents of the communication will be admissible as evidence. [8]

Nonrepudiation

A paper contract typically provides identification of the parties executing the contract, incorporating their *wet* signature, thus verifying their identity and intent to be bound to particular terms. The document is typically dated, and each party receives a copy of the document with both his or her signature and that of the other party. [19] In the world of electronic commerce, authenticity and integrity services generally do not provide all of the guarantees to both parties that they normally receive in the world of paper transactions. Most electronic messaging mechanisms for integrity and authenticity provide identification of the parties only in a fashion suitable for verification by the other contractual party, not by an independent third party such as a court.[20]

Nonrepudiation is an attempt to match the assurances provided by a well-executed, paper-based contract,[21] prevent a document's originator from denying the document's origin, and provide proof of authenticity.[22]

Nonrepudiation maybe provided in whole or in part through the use of one or more of mechanisms such as digital signatures, data integrity, and certifying authorities, with support from other system services such as time stamping. The nonrepudiation can be achieved by using a combination of these mechanisms and services to satisfy the security requirements of the application in question. The goal is to collect, maintain, make available, and validate nondeniable proofs regarding data transfers between the originator and recipient, thus establishing legal obligations that serve electronic practices.

Time-Stamping

The time a transaction is initiated or is submitted to an electronic messaging system, as well as the

---

17 M. Baum *and* H. Perritt, *Electronic Contracting, Publishing & ED/ Law (New* York, NY: John Wiley & Sons, Inc., 1991), section 6.23.

18 P.N. Weiss, op. cit., footnote 15, p. 221.

19 Steven Kent, Chief Scientist, Security Technology, Bolt Beranek and Newman, Inc., personal communication, May 1994.

20 Some express the concern that more demands will be placed on the electronic media than is expected of non-electronic media, since in modem commerce the idea of a well-executed paper transaction is often not met, irrespective of the influence of electronics. For example, the current Statute of Frauds is not applicable to cases where goods contracted for have been delivered. Similarly, in the absence of a "writ ing," entirely oral evidence is admissible about the tenor and terms of a contract. Finally, in many modem cases, even if a writing claims to bc the integrated statement of the agreement and is signed and available, the parties are often allowed to enter evidence outside the writing to reflect the meaning of the contract. (Raymond T. Nimmer, University of Houston Law Center, personal communication, July 1994.)

21 Ibid.

22 M. Baum, "Linking Security and the Law," *Worldwide Electronic Commerce—Conference Proceedings (New* York, NY: Jan. 16-18, 1994), p. 295.

time when a message is received by a third party or acted upon by a recipient, may be critical in some instances. Examples of such cases include electronic submission of bids or cases where the first to file a response wins. Some contend that there is little need for a trusted third party in such instances, since the recipient would be the trusted entity and the time would be determined by the recipient (e.g., the moment the message entered the recipient electronic mailbox), others believe that the audit trail maintained may not be sufficiently trustworthy, since internal clocks in the system are subject to inaccuracies, failures, or tampering.

For example, two parties to a contract could use the Data Encryption Standard Message Authentication Code (DES MAC)[23] function and suitable key management to achieve authenticity and integrity for their EDI messages, but each could change his or her local record of the transaction and neither could, on purely technical grounds, prove who tampered with the transaction (also see discussion in box 4-4). 24 Moreover, some argue that because digital signatures are created using *secret* keys that can be disclosed, either accidentally or maliciously, a time context must be associated with any digital signature if it is to be treated as authentic and comparable to a paper-based signature. Time context is not an added feature relevant only to time-sensitive transactions, they contend, but an essential aspect of all digital signatures used for nonrepudiation.[25] However, others contend that certification authorities can provide this assurance of authenticity.[26]

The inherent limitation of the use of digital signatures is their inability to provide *time-related* nonrepudiation. While a digital signature attached to a message will have a time-stamped audit trail through the network, digital signatures cannot, in the absence of a trusted entity, provide an unforgeable, trusted time stamp. To achieve full nonrepudiation, certification must be undertaken by a disinterested party beyond the control of the parties to a transaction or record. Such a third party is called a *trusted entity*.[27]

The key attributes of a trusted entity are that it is a disinterested third party trusted by the parties to the transaction and subject to the dispute resolution mechanisms relevant to a transaction or record. A trusted entity's administrative, legal, operational, and technical infrastructure must be beyond question. A trusted entity can perform any of a variety of functions to facilitate electronic contracts. Among these functions are: 1) producing a document audit trail, 2) storing a record copy of electronic documents,[28] 3) providing time and date stamps, or 4) generating authentication certificates to ensure the identity of the communicating

---

[23] The Data Encryption Standard (DES) is a published, federal information processing standard (FIPS) for use in protecting unclassified computer data and communications. It has also been incorporated in numerous industry and international standards. The encryption algorithm specified by the DES is called the Data Encryption Algorithm (DEA). This algorithm is what is called a symmetric, private-key algorithm, also referred to as a *secret key* algorithm (see box 4-3). The DES (FIPS PUB 46-2) can be used in message authentication to create a *message authentication code* (MAC) that is appended to the message before it is sent. Use of DES in what is called the Data Authentication Algorithm is specified in FIPS PUB 113 ("Computer Data Authentication," 1985). Message authentication (e.g., of electronic funds transfers) using the DEA is standard in banking and the financial community.

[24] Steven Kent, Chief Scientist, Security Technology, Bolt Beranek and Newman, Inc., personal communication, May 1994.

[25] Ibid. Some commentators disagree with this approach, contending that what is important is to know when a message is made, so that the time of its making can be compared to a list of revoked keys. However, if that revocation list is automatically queried upon receipt of the message, actual time would not matter, only relative time (revocation I isting versus message receipt). (Charles Miller, attorney, San Francisco, CA, personal communication, June 1994.)

[26] Charles Miller, attorney, San Francisco, CA, personal communication, June 1994.

[27] M. Baum, op. cit., footnote 22, p. 296

[28] Some commentators argue that storage of record copies of electronic documents is not necessarily a good idea; some might not favor allowing a third party to hold documents independently and subject to subpoena. (Charles Miller, attorney, San Francisco, CA, personal communication, June 1994.)

parties.[29] These functions maybe provided by different entities, some of whom are trusted by all parties, and some trusted by only some parties.[30]

Some suggest that the functions ascribed to the trusted third party can be provided by the value--added network providers;[31] however, the extent to which these responsibilities and the attendant liability will be assumed by such enterprises is unclear. Other entities that might take on these responsibilities include the U.S. Postal Service and the banking industry. In contrast to the courts' treatment of conventional, paper-based transactions and records, little guidance is offered as to whether a particular safeguard technique, procedure, or practice will provide the requisite assurance of enforceability in electronic form. This lack of guidance concerning security and enforceability is reflected in the diversity of security and authentication practices used by those involved in electronic commerce.

Legal standards for electronic commercial transactions have not been fully developed and these issues have undergone little review in the courts. Therefore, action by Congress may not be warranted now. However, Congress may wish to monitor this issue, so that these concerns are considered in future policy decisions about information security.

PROTECTION OF INFORMATION PRIVACY AND THE PROBLEM OF TRANSBORDER DATA FLOW

Development of a Right to Information Privacy in the United States

Although a right to privacy is not set forth in the Bill of Rights, the U.S. Supreme Court has protected various privacy interests. The Court found sources for a right to privacy in the First,[32] Third,[33] Fourth,[34] Fifth,[35] Ninth,[36] and 14th

29 M. Baum, op. cit., footnote 11, p. 135.

30 For example, time-stamping requires a widely trusted entity. However, that entity need not archive the documents it time-stamps and it is often held that the time-stamper should not even have access to the original documents for any purpose beyond hashing values of the documents. In the paper world, under U.S. law, copies of contracts are retained by the parties to the contract, but not by mutually trusted third parties. The Latin Notaraire approach to contracts is different and would have the third party hold the documents, but this is not a universal approach. Similarly the generation of (public-key) certificates can be undertaken by a set of entities completely separate from those who support the time-stamping function.

31 Ian Walden, Tarlo Lyons Information" Technology Law Research Fellow, Centre for Commercial Law Studies, Queen Mary and Westfield College, University of London, personal communication, April 1994.

32 The First Amendment provides: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances. "

33 The Third Amendment provides: "No Soldier shall, in time of peace be quartered in any house, without the consent Of the Owner, nor in time of war, but in a manner to be prescribed by law."

34 The Fourth Amendment provides: "The right Of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

35 The Fifth Amendment provides: "No person shall be held to answer for a capital, or otherwise infamous crime, unless On a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb, nor shall be compelled in any criminal case to be a wimess against himself, nor be deprived of life, liberty, or property; without due process of law; nor shall private property be taken for public use without just compensation."

36 The Ninth Amendment provides: "The enumeration in the Constitution of certain rights shall not be construed to deny ordisparage others retained by the people."

Amendments.[37] The concept of privacy as a legal interest deserving an independent remedy was first enunciated in an article coauthored by Samuel Warren and Louis Brandeis in 1890, which describes it as "the right to be let alone."[38] Since the late 1950s, the Supreme Court has upheld a series of privacy interests under the First Amendment and due process clause, for example "associational privacy,"[39] "political privacy, ''wand the "right to anonymity in public expression."[41] The Fourth Amendment protection against "unreasonable searches and seizures" also has a privacy component. In *Katz v. United States,* the Court recognized the privacy interest that protected an individual against electronic surveillance. But the Court cautioned that:

> . . . the Fourth Amendment cannot be translated into a general constitutional "right to privacy." That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further and often have nothing to do with privacy at all. Other provisions of the constitution protect personal privacy form other forms of government invasion. 42

The Fifth Amendment protection against self-incrimination involves a right to privacy against unreasonable surveillance by the government or compulsory disclosure to the government.[43]

Until *Griswold v. Connecticut, 381* U.S. 479 (1965), any protection of privacy was simply viewed as essential to the protection of other more well-established rights. In Griswold, the Court struck down a Connecticut statute that prohibited the prescription or use of contraceptives as an infringement on marital privacy. Justice William O. Douglas, in writing the majority opinion, viewed the case as concerning "a relationship lying within the zone of privacy created by several fundamental constitutional guarantees," that is, the First, Third, Fourth, Fifth and Ninth Amendments, each of which creates "zones" or "penumbras" of privacy. The majority supported the notion of an independent right of privacy inherent in the marriage relationship. Not all agreed with Justice William O. Douglas as to its source; Justices Arthur Goldberg, Earl Warren, and William Brennan preferred to locate the right under the Ninth Amendment.

In *Eisenstadt v. Baird, 405* U.S. *438 (1972),*[44] the Court extended the right to privacy beyond the marriage relationship to lodge in the individual:

> If the right of the individual means anything, it is the right of the *individual,* married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child.

Roe v. Wade, 410 U.S. 113 *(1973),*[45] further extended the right of privacy "to encompass a woman's decision whether or not to terminate her pregnancy." The Court argued that the right of privacy was "founded in the Fourteenth Amendment's concept of personal liberty and restrictions on State action." The District Court had argued that the source of the right was the Ninth Amendment's reservation of the right to the people.

---

37 The 1 4th Amendment provides in pertinent part, "No State shall deprive ant person Of life, liberty, or property, without due process Of law; nor deny to any person within its jurisdiction the equal protection of the laws."

38 Warren & Brandeis, "The Right to Privacy," 4 *Harvard Law Review 193 (1890).*

39 *NAACP* v. *Alabama, 357* U.S. 449 (1958).

40 *Watkins* v. *United States,* 354 U.S. 178 (1957); and *Sweezy* v. New *Hampshire,* 354 U.S. 234 (1957).

41 Talley v. *California,* 362 U.S. 60 (1960).

42 *Katz* v *United States,* 389 U.S. 347, 350 (1967).

43 See *Escobedo* v. *Illinois,* 378 U.S. 478 (1964); *Miranda* v. *Arizona,* 384 U.S. 436 (1966); and *Schmerber* v. *California,* 384 U.S. 757 (1%6).

44 In Which the Court struck down a Massachusetts law that made it a felony to prescribe or distribute contraceptives to single persons.

45 In Which the court struck down the Texas abortion statute.

To this point, the Supreme Court addressed the question of privacy only as it applied to very specific kinds of human conduct. In the earliest case that raised the issue of the legitimate uses of computerized personal *information* systems, the Supreme Court avoided the central question of whether the Army's maintenance of such a system for domestic surveillance purposes "chilled" the first amendment rights of those whose names were contained in the system.[46] In two cases decided in 1976, the Court did not recognize either a constitutional right to privacy that protected erroneous information in a flyer listing active shoplifters[47] or one that protected the individual's interests with respect to bank records. In *Paul v. Davis,* the Court specified areas of personal privacy considered "fundamental":

> ... matters relating to marriage, procreation, contraception, family relationships, and child rearing and education.

Respondent Davis' claim of constitutional protection against disclosure of his arrest on a shoplifting charge was "far afield from this line of decision" and the Court stated that it "declined to enlarge them in this manner."[48] In *United States v. Miller,*[49] the Court rejected respondent Miller claim that he had a Fourth Amendment reasonable expectation of privacy in the records kept by banks "because they are merely copies of personal records that were made available to the banks for a limited purpose," and ruled instead that checks are not confidential communications but negotiable instruments to be used in commercial transactions." In response to *United States v. Miller,* Congress enacted the Financial Privacy Act of 197850 (Public Law 95-630), providing bank customers with some privacy regarding records held by banks and other financial institutions and providing procedures whereby federal agencies can gain access to such documents. Congress effectively overruled the *Miller* holding by requiring the government to obtain a subpoena in order to access bank records. Because the focus of the constitutional right to privacy has traditionally not been on privacy of information, statutory provisions have been enacted to protect specific kinds of information, including the Family Educational Rights and Privacy Act of 1974 (popularly known as the Buckley Amendment)[51] to protect the privacy of records maintained by schools and colleges; the Fair Credit Reporting Act, to protect the privacy of consumers in the reporting of credit information;[52] and the Federal Videotape Privacy protection Act.[53]

The Privacy Act

Congress enacted the Privacy Act of 1974 (Public Law 93-579) to provide legal protection for and safeguards on the use of personally identifiable information maintained in federal government record systems. (See box 3-2 for discussion of privacy and confidentiality.) The Privacy Act established a framework of rights for individuals whose personal information is recorded and the responsibilities of federal agencies that collect and maintain such information in Privacy Act record systems. The Privacy Act embodies principles of fair information practices set forth in *Computers and the Rights of Citizens,* a report published in 1973 by the former U.S. Department of Health, Education, and Welfare. These principles are as follows:

~ *Laird* v. *Tatum,* 408 U.S. 1 (1972).

47 *Paul* v. *Davis,* 424 U.S. 693 (1976).

48 Ibid., p. 713.

49 *United States* v. *Miller,* 425 U.S. 435 (1976).

50 Public Law 95-630, title XI, 92 Stat, 3697, Nov. 10, 1978, *et seq.*

51 Public Law 93-380, title V, sec. 513, 88 Stat. 571, Aug. 21, 1974.

52 Public Law 91-508, title VI, sec. 601, 84 Stat. 1128, Oct. 26, 1970, *et seq.*

53 Public Law 100-618, sec. 2(a)(1),(2), 102 Stat. 3195, Nov. 5, 1988, *et seq.*

1. There must be no secret personal data record-keeping system.
2. There must be a way for individuals to discover what personal information is recorded and how it is used.
3. There must be a way for individuals to prevent information about themselves, obtained for one purpose, from being used or made available for other purposes without their consent.
4. There must be a way for individuals to correct or amend a record of information about themselves.
5. An organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for its intended use and must take reasonable precautions to prevent misuses of the data.

The Privacy Act gives individuals the right to access much of the personal information about them kept by federal agencies. It places limits on the disclosure of such information to third persons and other agencies. It requires agencies to keep logs of all disclosures, unless systems of records are exempt from the Privacy Act.[54]

The Privacy Act also gives an individual the right to request an amendment of most records pertaining to him or her if he or she believes them to be inaccurate, irrelevant, untimely, or incomplete. The agency must acknowledge the request in writing within 10 days of its receipt. It must promptly (though no time limit is specified) make the requested amendment or inform the individual of its refusal to amend, the reasons for the refusal, and the individual's right to request a review by the agency head. If the individual requests such a review, the agency head has 30 days to render a decision. Should the agency head refuse to amend the information, the individual can file a concise statement of his or her disagreement with the agency decision. Thereafter, the agency must note the dispute in the record and disclose this fact, along with the individual's statement, whenever the record is disclosed.

The Privacy Act further provides that the individual can pursue his disagreement, and indeed any noncompliance by an agency, with a civil suit in Federal District Court. He or she can obtain an injunction against a noncomplying agency, collect actual damages for an agency's willful or intentional noncompliance, and also be awarded attorney's fees and costs if he or she "substantially prevails" in any such action. Agency personnel are criminally liable for willful noncompliance; the penalty is a misdemeanor and a fine of up to $5,000. There have been few cases in which a complainant has recovered damages.

The federal agencies also have a responsibility to collect only relevant information on individuals, to get the information directly from the individual whenever possible, and to notify the individual of several facts at the time the information is requested. Willful failure to comply with the notification requirement may result in civil and criminal liability.

The Privacy Act also covers agencies' "system of records" and requires an annual, nine-point report to be published in the *Federal Register. The* report must contain information such as categories of records maintained; their routine use; policies on their storage and retrieval; and other agency procedures relating to the use, disclosure, and amendment of records. Agencies also have extensive rulemaking duties to implement each component of the law.

The Privacy Act is limited, however, in several significant ways. Some believe that a system of notification through the *Federal Register is* cumbersome and burdensome to the individual who, practically speaking, does not regularly review the publication, so that notification is not effective. The act also places the burden of monitoring privacy in information and redressing

[54] The Privacy Act exempts from this provision records pertaining to law enforcement. The Privacy Act of 1974 (Public Law 93-579, sec. 552a(A)(2)).

BOX 3-2: The Problem of Definition—Privacy and Confidentiality

In discussions about privacy and information policy, the terms *privacy* and *confidentiality* are often used interchangeably Neither term possesses a single clear definition, and theorists argue variously that privacy and confidentiality (and the counterpart to confidentiality, secrecy) may be concepts that are the same, completely distinct, or in some cases overlapping,

While definitions of privacy and confidentiality and distinctions between the two cannot be tightly drawn (as indeed, the two terms are not necessarily exclusive of one another) for purposes of this report, the Off Ice of Technology Assessment will attempt to use the terms in the following ways, largely mirroring approaches to the subject matter taken by Alan Westin and Charles Fried, *Confidentiality* will refer to how data collected for approved purposes will be maintained and used by the organization that collected it, what further uses will be made of it, and when individuals will be required to consent to such uses It will be achieved, as Anita Allen states, when designated information is not disseminated beyond a community of authorized knowers.[1] According to Allen, confidentiality is distinguished from secrecy, which results from the intentional concealment or withholding of information Privacy will refer to the balance struck by society between an individual's right to keep information confidential and the societal benefit derived from sharing the Information, and how that balance is codified into legislation giving individuals the means to control information about themselves.

Privacy can be viewed as a term with referential meaning, it typically is used to refer to or denote something But privacy has been used to denote many quite different things and has varied connotations As Edward Shils observed 20 years ago:

> Numerous meanings crowd in the mind that tries to analyze privacy the privacy of private property, privacy as a proprietary interest in name and image; privacy as the keeping of one's atfairs to oneself, the privacy of the internal affairs of a voluntary association or of a business, privacy as the physical absence of others who are unqualified by kinship, affection or other attributes to be present, respect for privacy as the respect for the desire of another person not to disclose or to have disclosed information about what he is doing or has done; the privacy of sexual and familial affairs, the desire for privacy as the desire not to be observed by another person or persons, the privacy of the private citizen as opposed to the public official, and these are only a few

Definitions of privacy may be narrow or extremely broad One of the best known definitions of privacy is that set forth by Samuel Warren and Louis Brandeis in a 1890 article that first enunciated the concept of privacy as a legal interest deserving an independent remedy Privacy was described as "the right to be let alone [2] "In spite of its breadth, this view has been influential for nearly a century [3] In the 1960s, 1970s and 1980s, the proliferation of information technology (and concurrent developments in the law of reproductive and sexual liberties) has inspired further and more sophisticated inquiry into the meaning of privacy. [4]

In his work, *Privacy and Freedom,*[5] Alan Westin conceived of privacy as "an Instrument for achieving individual goals of self realization, " and defined it as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to

---

[1] A L Allen, *Uneasy Access Privacy for Women in a Free Society* (Totowa, NJ Rowman & Littlefield, 1988), p 24

2 The term "the *right* to be let alone" was borrowed from the 19th century legal scholar and jurist Thomas Cooley See T Cooley, Law *of Torts* (2nd Ed , 1888)

3 Allen argues that if privacy simply meant "being let alone, " any form of offensive or harmful conduct directed toward another person could be characterized as a violation of personal privacy

[4] Allen, op cit footnote 1, p 7

5 A F Westin, *Privacy and Freedom (New* York, NY Ateneum, 1967)

BOX 3–2 (cont'd.): The Problem of Definition: Privacy and Confidentiality

others, " approaching the concept in terms of informational privacy WA Parent defined privacy in terms of information as "a condition of not having undocumented personal information about oneself known by others"[6]

In contrast, Ruth Gavison defines privacy broadly as "limited access in the senses of solitude, secrecy, and anonymity" In her view, privacy is a measure of the extent to which an individual is known, the extent to which an individual is the subject of attention, and the extent to which others are in physical proximity to an individual Her definition of privacy was to include

> such "typical" invasions of privacy as the collection, storage, and computerization of information, the dissemination of information about individuals, peeping, following, watching, and photographing individuals intruding or entering '(private" places, eavesdropping, wiretapping, reading of letters, drawing attention to individuals, required testing of individuals, and forced disclosure of information. [7]

In *Computers, Health Records and Citizens Rights,* Westin draws a clear distinction between the concepts of privacy and confidentiality in the context of personal information

> Privacy is the question of what personal information should be collected or stored at all for a given social function It Involves issues concerning the legitimacy and legality of organizational demands for disclosure from individuals and groups, and setting of balances between the individual's control over the disclosure of personal information and the needs of society for the data on which to base decisions about individual situations and formulate public policies Confidentiality is the question of how personal data is collected for approved social purposes shall be held and used by the organization that originally collected it, what other secondary or further uses may be made of it, and when consent by the individual will be required for such uses It is to further the patient's willing disclosure of confidential information to doctors that the law of privileged communications developed In this perspective, security of data Involves an organization's ability to keep its promises of confidentiality.

Allen notes the unsettled relationship between secrecy and privacy in the privacy literature In her view, secrecy is a form of privacy entailing the Intentional concealment of facts She claims that it does not always involve concealment of negative facts, as is asserted by other privacy scholars [8] She points to the work of Sissela Bok, who defines secrecy as the result of intentional concealment and privacy as the result of "unwanted access "g Since privacy need not involve Intentional concealment, privacy and secrecy are distinct concepts Privacy and secrecy are often equated because "privacy is such a central part of what secrecy protects " Bok viewed secrecy as a device for protecting privacy.[10]

Charles Fried also discusses the relationship between privacy and secrecy He states that at first glance privacy seems to be related to secrecy, to limiting the knowledge of others about oneself He argues for refinement of this notion, stating that it is not true that the less that is known about us the more privacy we have He believes, rather, that privacy is not simply an absence of Information about us in the minds of others, it is the control we have over Information about ourselves It is not simply control over the quantity of Information abroad, it is the ability to modulate the quality of the knowledge as well We may not mind that a person knows a general fact about us, and yet we feel our privacy invaded if he or she knows the details.[11]

---

6 W A parent "Recent Work on the Conceptlon of Privacy" *American Philosophical Quarterly,* vol 20, 1983, p 341
7 R Gavison, 'Privacy and the Limits of the Law, " *Yale Law Journal,* VOI 89 1980, p 421
8 Ibid
9 S Bok Secrets *On the Ethics of Concealment and Revelation (New* York, NY Oxford University Press, 1984) p 10
10 Ibid
11 C Fried, "Privacy," *Yale* Law *Journal,* vol 77.1968, pp 474 782

SOURCE Off Ice of Technology Assessment, 1994

wrongs entirely with the individual, providing no government oversight mechanism for the system. In addition, the act itself is limited in its application to "routine use" of the record, which refers to disclosure of records, not how the collecting agency uses those records internally.55 Many commentators have noted that the penalties prescribed in the act are inadequate, and others comment that the act contains no specific measures that must be in place to protect privacy so that it cannot be used to describe what technical measures must be taken to achieve compliance.

Other criticism arises from technological challenges to the act's effectiveness and workability. When the act was debated and enacted, federal agency record systems were still based largely on paper documents and stand-alone computer systems that were not 1 inked together. Computers and telecommunication capabilities have expanded the opportunities for federal agencies to use, manipulate, and peruse information. There has already been a substantial increase in the matching of information stored in different databases as a way of detecting fraud, waste, and abuse. Networked systems will further enhance this ability. The Computer Matching Act requires that every agency conducting or participating in matching programs establish a Data Integrity Board. Among the responsibilities of these Boards is to oversee matching programs in which the agency has participated during the year and to determine compliance with applicable laws, regulations, and guidelines. The are also to serve as a clearinghouse for receiving and providing information on the accuracy, completeness, and reliability of records used in matching programs.[56]

More recent use of federal agency information, in such programs as the Credit Alert Interactive Voice Response System, involve more cooperative interconnection of information across agencies (see box 3-3). The ability to share databases and access systems between federal and state governments is also being developed. All 50 states can electronically access Social Security Administration (SSA) data.[57] While the Internal Revenue Service (IRS) currently sends magnetic tapes to the states in order to share federal tax data, electronic access is expected by 1997 or 1998.[58] ('See box 3-4 for discussion of privacy concerns at the Internal Revenue Service.)

Because of these uses and the ease with which they can be accomplished through networked computers, the Privacy Act has come under additional criticism for its agency-by-agency approach to addressing privacy protections. The act places responsibility for data protection separately on each federal agency. Given the increased sharing of data, if privacy protection fails, it is difficult under this approach to determine who must bear responsibility and who is liable when abuses of information occur. Some commentators suggest that the act be overhauled to reflect the technological changes that have occurred since the 1970s and the new uses of information enabled by those changes. (See below for a discussion of the development and capabilities of computer and network technology.) Others believe that clearer

---

55 For a discussion of the government's "routine use" of personal information, see P. Schwartz, "The Computer in German and American Constitutional Law: Towards an American Right of Information Self Determination," *The* American *Journal of Comparative Law*, vol. 37, No. 4, fall 1989, pp. 694-698.

56 5 U.S.C. 552a(u).

57 Among the major SSA data exchanges with the states is the Beneficiary Earnings and Data Exchange (BENDEX), which extracts information from the Master Beneficiary Record earnings information for the entire nation. Most states check BENDEX before sending a payment to a surviving spouse claiming retirement benefits. Another common exchange is the Supplemental Security Income/State Data Exchange (SDX). This exchange is an extract of the Supplemental Security Record, the database that stores a person's history on public assistance. Case workers use SDX to verify eligibility for public assistance.

58 26 USC 6103 enumerates 28 instances in which the IRS can disclose taxpayer information.

policy decisions must be made regarding when the sharing of information between agencies is appropriate, and stronger partitions between agency data must be established. To facilitate these changes, it is suggested that a better forum for privacy policy decisions be established to replace the data integrity boards already existing in agencies that participate in computer matching programs.

Increased computerization and linkage of information maintained by the federal government is arguably not addressed ***by the Privacy Act, which approaches privacy issues on an agency-by-agency basis.***

To address these developments:

- ***Congress could and allow each agency to address privacy concerns individually, through its present system of review boards.***
- ***Congress could require agencies to improve the existing data integrity boards, with a charter to make clearer policy decisions about sharing information and maintaining its integrity.***
- ***Congress could amend the existing law to include provisions addressing the sharing and matching of data, or restructure the law overall to track the flow of information between institutions.***
- ***Congress could provide for public*** *access for* ***individuals to information about themselves, and protocols for amendment and correction of personal information. It would also consider providing for online publication of the Federal*** **Register** ***to improve public notice about information collection and practices.***

In deciding between courses of actions, Congress could to exercise its responsibility for oversight through hearings and/or investigations, gathering information from agency officials involved in privacy issues, as well as citizens, in order to gain a better understanding of what kinds of actions are required to implement better custodianship, a minimum standard of quality for privacy protection, and notice to individuals about use and handling of information.

BOX 3–3: The CAIVRS Program

The Credit Alert Interactive Voice Response System (CAIVRS) is a screening program aimed at preventing people who do not repay federal loans from obtaining new loans CAIVRS includes delinquent debtor data from the departments of Agriculture, Education, Housing and Urban Development (HUD) and Veterans Affairs (VA) and the Small Business Administration Begun by HUD in 1987, it contains information on home, property, and mobile home loans, and is now used by the VA for screening loan applications in its housing program CAIVRS allows lenders such as mortgage bankers to phone in to the database The lenders enter a password, then punch in the Social Security number of the person seeking credit The system reviews its data and responds

The system is comparable to a credit-card check before a buyer makes a credit purchase in a store If the lender gets a "hit, " he or she cannot grant a new loan and must ask HUD to review the loan application In the first 10 months of 1993, CAIVRS handled 23 million inquiries and recorded 30,000 "hits" on applicants with problem credit histories.

SOURCE Off Ice of Technology Assessment, 1994

Privacy and Computerization

American legal scholars first considered the impact of computerization on privacy more than 20 years ago. Soon after, the U.S. Privacy Protection Study Commission, under a congressional charter, extensively studied privacy rights in the emerging information society. The commission focused on eight sets of recordkeeping relationships and found that privacy was not protected satisfactorily from either government or industry intrusions. While the commission noted privacy

BOX 3–4: Security and Privacy Concerns at the Internal Revenue Service

The Internal Revenue Service's (IRS'S) long-term project to modernize its computer system, the Tax Systems Modernization (TSM) Program, began in 1988 and is projected to require a net capital investment of over $8 billion by 2008 Information security has been a major issue in this process; the IRS has been faulted for privacy violations in its existing system and has been charged with showing little progress in addressing privacy concerns about the confidentiality of taxpayer records as it proceeds with TSM The IRS counters that it is aggressively addressing these but additional safeguards could potentially make the system more cumbersome to operate. [1]

In a recent review of general controls over IRS computer systems, the General Accounting Office found that the IRS did not adequately restrict access to computer programs and data files or monitor the use of these resources by staff As a result, IRS employees who did not need taxpayer data could access and/or use it, and unauthorized changes to the taxpayer data could be made inadvertently or deliberately. In addition to confidentiality and integrity problems, these actions could result in fraud.[2]

The National Research Council (NRC) has also been studying the IRS and its progress in implementing the TSM initiative In its report of a two-year study requested by the IRS, NRC found that the IRS needed a more integrated, comprehensive, and internally consistent security architecture and that it should investigate the use of modern cryptographic techniques such as public-key cryptography and digital signatures in electronic filings NRC also found that the IRS privacy policy development should include a stronger and more effective integration of privacy principles and techniques in TSM system designs [3] In a follow-on letter report to the IRS in 1993, NRC found, "The IRS has increased its awareness of privacy issues and has tackled several security issues over the last three years However, serious concerns remain about the privacy and security issues engendered by TSM. In particular, rapid development of a comprehensive privacy and security policy is needed."[4] According to the NRC committee, the new technologies being provided through TSM can lead to a wide range of potentially disastrous privacy and security problems for the IRS unless the IRS develops effective, integrated privacy and security policies. [5]

---

1 Stephen Barr, "IRS Computer Revamp Faulted by Study Panel, " *Washington Post*, Aug 20, 1993, p A21

2 u s General Accounting Office, *IRS in formation Systems Weaknesses Increase the Risk of Fraud and Impair Reliability of Management Information, GAO/AIMD-93-34,* September 1994

3 Computer Science and Telecommunications Board, National Research Council, *Review Of the Tax Systems Modernization of the Internal Revenue Service* (Washington, DC National Academy Press, 1992)

4 Lette report from Robert p Clagett (Chair, Committee on Review of the Tax Systems Modernization Of the Internal Revenue Service, National Research Council) to Margaret Richardson (Commissioner, IRS), July 30, 1993

5 Ibid

SOURCE. Office of Technology Assessment, 1994

problems in the private sector, it believed that the real threat existed with government collection and use of information, which is the concern that the Privacy Act of 1974 addresses.[59]

Since the 1970s, however, computer and communications technology has enabled the growth of an information industry within the private sector. The dramatic advances in telecommunications

---

[59] J R Reidenberg, "Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?" *Federal Communications Law Journal*, *vol. 44, No. 2,* March 1992, pp. 1%- 197.

and information technology changed the relationship between individuals and corporations with respect to the circulation of personal information.[60] Information technology, networking, and proliferation of computers have encouraged extensive gathering and dissemination of personal information through sophisticated data collection techniques, corporate outsourcing of data processing, and the establishment of information service providers and clearinghouses.[61] Vast quantities of personal information containing greater detail than ever before about an individual financial status, health status, activities, and personal associations became readily available through commercial information services and list brokers. Information that once had to be laboriously assembled by hand or using punched-card methods could be bought in machine-manipulable form.[62]

These new capabilities and the increased circulation of personal information to private-sector, resale companies raise significant privacy concerns. A joint Lou Harris/Equifax survey conducted in 1992 indicated that 79 percent of Americans feel their personal privacy is threatened. Most Americans acknowledge the danger to privacy from present computer uses.63 Privacy and information processing have also generated substantial interest overseas: in many European countries, statutes provide a broad set of privacy rights applicable to both the public and private sectors.

International Privacy Concerns: Transborder Data Flow

Development of sophisticated telecommunications systems, coupled with the increased use of computing technologies, has resulted in a growing, international market in information and associated services. Computer and telecommunications technology delivers news, science, education, industry, manufacturing, medical, and national defense information. These technologies and their ability to transmit information and services over distances are not constrained by national borders .64

Transborder data flow is the transfer of data across national borders. The media may be ordinary text on microfilm, punched cards, or computer listings transmitted by ordinary mail. Data may also be transmitted electronically via telephone lines, cables, specific data networks, or satellite. Such data may be transmitted from a terminal to a computer system as part of an international network. They are then processed in the system and sent back to the terminal. The data alternatively may be accessed and processed online in a network by anyone who is able to enter the system.

Foreign countries, particularly European nations, have taken steps to address the problem of data flows to destinations perceived to lack sufficient privacy protection. In the mid- 1970s, European lawmakers recognized that data technology

---

60 Concerns raised by the computerization of health care information, cited by the Krever Commission of Canada, reflect those raised by computerization generally. The commission stated that: 1) computer technology makes the creation of new databases and data entry easy, so that databases can be created and maintained readily; 2) computerization allows for storage of large amounts of data in a very small physical medium. An intruder into a database can retrieve large amounts of data once access is gained; 3) computers provide for the possibility of "invisible theft' '—stealing data without taking anything physical—so that persons are unaware that data has been altered, stolen or abused, and 4) computers allow for the possibility of "invisible" modification, deletion, or addition of data. Ontario Commission of Inquiry into the Confidentiality of Health Information, "Report of the Commission," 1980, vol. II, Pp. 160-166.

61 J.R. Reidenberg, op. cit., footnote 59, pp. 201'2W.

62 W Ware, "The New Faces of Privacy, " *The information Society, vol. 10,* 1993, pp. 195, 200.

63 Harris-Equifax Consumer Privacy Survey 1992, conducted for Equifax by Louis Harris and Associates in association with Alan F. Westin, Columbia University.

64 I Walden and N, Savage, "Transborder Data Flows," *Information Technology & the Law*, 2nd Ed., 1. Walden (cd.) (Great Britain: MacMillan Publisher, Ltd., 1990), p. 121.

could lead to invasions of privacy and that this should not be regarded as simply a national concern. They realized that the economic and social relationships of many countries were closer than before, and that the emergence of a global market led to an increased movement of information across borders. Since information is often of a personal nature, and based on the premise that the needs of the market should not undermine the legal protection for citizens, it was deemed necessary to regulate the use of personal data similarly in all countries.[65] A number of countries prohibit the transmission of personal information to countries with little or no computer privacy protection.[66] Data protection and security requirements established by countries outside the United States may have a significant impact on transborder data flow because of the limited legal standards in the United States.

While the Privacy Act of 1974 addresses the protection of data maintained by the federal government through principles of fair information practices (for enumeration and discussion of fair information practices, see page 81), American law does not contain a comprehensive set of privacy rights or principles that adequately address the acquisition, storage, transmission, use, and disclosure of personal information within the private sector. Legal protection is accorded through privacy rights created by federal or state legislation or state common laws. In addition, self-regulatory schemes have been adopted by some industries and various companies. Although these schemes may offer privacy protect ion, the y are not enforceable by law. Europe is sensitive to a need to protect privacy, particularly the threat of technology that may easily transmit data to a country where corresponding legal protections may not be afforded it.[67]

The European approach to addressing privacy concerns is a comprehensive one; most European countries have adopted omnibus legislation governing private-sector data processing. Among these broad national laws are a number of important differences relating to the scope of coverage and the regulatory enforcement mechanisms. The European Union believes that the effect of these differences is likely to impede the development of the single European market and has proposed a directive to harmonize these laws and establish a community standard of privacy protection.[68]

Two sets of international norms have traditionally established standards for data protection: the Organization for Economic Cooperation and Development's (OECD's) voluntary Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data , and the Convention of the Council of Europe for the Protection of Individuals with Regard to Automatic Processing of Personal Data (No. 108/1981).69 Each attempted to assure that transborder data could flow across borders in an acceptable way and to provide the data with a certain level of protection. Later, in July 1990, the European Economic Community Commission proposed a draft directive '"concerning the protection of individuals in relation to the processing of personal data."

The Organization for Economic Cooperation *and Development Guidelines*

The OECD guidelines were drafted in 1979 and adopted in September 1980 as the Guidelines on the Protection of Privacy and Transborder Flows

65 p Blume "An EEC Policy for Data Protection," *Computer/Law Journal*, vol. 1 I, 1992.

66 J.R. Reidenberg, op. cit. footnote 59, p. 238.

67 Ibid.

68 Ibid.

69 OECD is a United Nations intergovernmental institution, established in 1961 with the stated objectives of effective use of economic resources of member states, development of scientific and technical research, training of personnel, maintenance of stable finances in external and internal turnover, liberalization of commodity exchange and flow of capital, and technical assistance to developing countries.

of Personal Data. They were developed in response to growing national movements to regulate transborder data flows and the discussion about the Council of Europe proposal. The specific mandate was:

> . . . to develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate the harmonization of national legislation, without this precluding at a later date the establishment of an international convention.

The OECD guidelines are based on principles of data protection to govern the protection of personal data in transborder data flows. These principles are:

- Data should be obtained lawfully and fairly.
- Data should be relevant to their purposes, accurate, complete, and current.
- The purpose for which data will be used must be identified and data must be destroyed if it is no longer necessary to serve that purpose.
- Use of data for purposes other than those specified is authorized only with the consent of the data subject or by authority of law.
- Procedures must be established to guard against loss, destruction, corruption, or misuse of data.
- Information about collection. storage, and use of personal data and personal data systems should be available.
- The data subject has a right of access to his or her data and the right to challenge the accuracy of that data.
- A data controller should be designed and accountable for complying with measures established to implement these principles.[70]

These principles mirror the elements of fair information practices that form the basis of much of U.S. law related to government information. In the private sector, however, these principles are not consistently applied.[71] Since 1980 over 177 U.S. corporations and trade associations publicly endorsed the OECD guidelines and issued policy letters on privacy and data security in recognition of the importance of this subject, though few U.S. companies have publicly implemented the guidelines.

The guidelines balance the requirements for the free flow of data with the need to provide basic data protection. They also specifically require that data flow be secured. Part 3 of the guidelines deals specifically with transborder data flow:

- Member countries should take into consideration the implications for other member countries of domestic processing and re-export of personal data.
- Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a member country, are uninterrupted and secure.
- A member country should refrain from restricting transborder flows of personal data between itself and another member country, except where the latter does not yet substantially observe these guidelines or where export of such data would circumvent its domestic privacy legislation. A member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data, and for which the other member country provides an equivalent protection.
- Member countries should avoid developing laws, policies, and practices in the name of the protection of privacy and individual liberties,

70 OECD Doc. No. C(80)58 final.

71 Some argue that the discussion about privacy rights should focus on property-rights issues. at least m part. They contend that information is "property" and that information-control issues should be viewed as allocating (creating, denying, or conditioning) property rights in in formation. (R. Nimmer and P. Krauthaus, op. cit., footnote 11.)

that would create obstacles to transborder flows of personal data that would exceed requirements for such protection.[72]

While the OECD guidelines are voluntary and are not a legally binding instrument, they have been endorsed by all **24** member countries.

The Council of Europe has interpreted the convention on data protection for specific kinds of data processing. The principles at the foundation of this convention are virtually identical to those of the OECD guidelines. The Council of Europe has also defined fair information practices under other circumstances and issued recommendations for areas such as direct marketing and employment records.[73] The U.S. business community views these initiatives as reflecting an appropriate balance between privacy protection and free flows of information .[74]

European Community Council Directive

In July 1990 the Commission of the European Economic Community published a draft Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (*'The Council Directive' ').75 The Council Directive is part of the European Union's (EU's)[76] program to create a "common market and an economic and monetary union, and. . . the implementation of certain common policies . . . "7[7] (For discussion of the European Union's analysis of information security systems, see box 3-5.)

On March 11, 1992, the European Communities Parliament advised amending the commission's proposal to eliminate the distinction between public and private-sector data protection, and then amended and approved the draft Council Directive. On October 15, 1992, the commission issued its amended proposal, which is being considered by the Council of Ministers.

Under the Council Directive, each of the EU member states must enact laws governing the "processing of personal data."[78] *Processing is* defined broadly as "any operation or set of operations," whether or not automated, including but not limited to "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[79] Personal data is defined equally broadly as "any information relating to an identified or identifiable natural person."[80] The only "processing of personal data" not covered by the Council Directive is that performed by a "natural

---

72 OECD Doc. *No.* C(80) *58* final.

73 See Council of Europe Committee of Ministers, Recommendation R985(920) on the Protection of Personal Data for Purposes of Direct Marketing (1985); and Council of Europe Committee of Ministers, Recommendation R989(2) on the protection of Personal Data Used for Employment Purposes (1989).

74 M N DiTosto, Manager, Telecommunications/Economic and Financial Policy, U.S. Council for International Business, International Data Protection Landscape, remarks to the State of Virginia's Committee on Information Policy, July 23, 1993.

75 Analysis of the Provisions of the Council Directive was assisted by personal communication with and material provided by Fred H. Cate, Senior Fellow, The Annenberg Washington Program.

76 The European *community* officially became the European Union in November 1993.

77 European Economic Community Treaty of 1957, art. 2 (as amended by the Single European Act of 1986 and the Treaty on European Unity (Maastricht, 1992)).

78 Council Directive, Com(92)422 Final SYN 287 (October 15,1992).

79 Ibid.

80 Ibid., art. 2(a). "[A]nidentifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

BOX 3–5: The Green Book on the Security of Information Systems

The Commission of the European Communities' *Green Book on the Security of information Systems* ("Green Book")[1] IS the result of a European Council decision adopted in May 1992 establishing a Senior Official's Group to advise the commission on action to be undertaken, and to develop strategies for the security of Information systems or "Action Plan " As a step toward this Action Plan, the Green Book examines the issues involved, the range of options resulting from an analysis of the issues, and requirements for action The Green Book attempts to outline the background to the development of a consistent approach to information security in Europe [2]

The intention of the Commission in preparing the Green Book was to set out and promote a better understanding of information security issues and to develop a consensus on information system security strategies to be considered on an EC-wide basis. The Green Book represents an intermediate step toward the formulation of an Action Plan foreseen in the Council Decision. [3]

The Green Book, m its section on Proposed Positions and Actions, identifies areas where initiatives are needed EC-wide These require a concerted approach within Europe and where possible, internationally. The general position taken by the document is that societies engaged in the global economy need to provide for adequate levels of Information security With the growing diversity of services and applications of telematics, the security of information systems must evolve with the growing demand and reduce the risks to security and safety while avoiding obstruction of renovation or economic and social developments [4]The document examines and sets forth a proposed position and action for three major areas trust services, International developments, and technical harmonization [5]

The Green Book addresses issues surrounding *trust services,* Including electronic alternates to traditional techniques of securing Information, such as signatures, envelopes, registration, sealing, depositing and special delivery. It raises the issue of information crime and rules governing the use of electronic evidence in civil and criminal court proceedings including the need to harmonize these wlthin the EC The absence of such harmonization could create, it asserts, "safe havens" for illegal activities. It addresses the need to cater to the needs for seamless information security for business, the general public, video and multimedia communications, and telecommuting in nonclassified Information The report suggests that trust services be established, including digital signature, nonrepudiation, claim of

[1]Commission of the European Communities, Directorate General XIII, Telecommunications, Information Market and Exploitation of Research, Green *Book on the Security of Information Systems,* Draft 40, Oct 18, 1993

[2]Ibid

3 Ibid p 1

[4]Ibid at p 2

[5]Ibid at 3-6

(continued)

person in the course of a purely private and personal activity."[81]

Individual national laws enacted in compliance with the Council Directive must guarantee that "processing of personal data" is accurate, up-to-date, relevant, not excessive, used only for the legitimate purposes for which it was collected, and kept in a form that permits identification of individuals no longer than is necessary, for that pur-

81 Ibid., art. 3(2).

BOX 3–5 (cont'd.): The Green Book on the Security of Information Systems

origin, claim of ownership in negotiable documents, fair exchange of values, intractability, and time stamping It suggests establishment of Europe-wide confidentiality services for nonclassified information, establishment of a network of Trusted Third Parties for the administration of the service provisions such as for name assignment, key management, certifications and directories, and liability principles for network providers, intermediates, and value-added service providers, It suggests establishment of common principles for legislation covering communication crime and for electronic evidence, development of generic codes of practice for handling nonclassified information, including rules for security labeling, and development of sector-specific codes of practice and base line controls.[6]

The Green Book discusses rapidly developing *international/ communication* and security concerns, and recognizes that security needs of European organizations and individuals must be safeguarded and the competitiveness of the European industry maintained. It points out the need to avoid creation of barriers to trade and services based on the control over security mechanisms and digital signature schemes. It proposes that if acceptable international solutions cannot be agreed to, a European option should be considered In response to these positions it suggests efforts toward international solutions for information security, strengthened support for international standardization, and consideration of a European security option offering confidentiality and digital signature services internationally [7]

On the subject of *technical harmonization,* the paper points out that electronic products, systems, services, and applications must be secure and safe, and must operate to generally recognized levels of trust The International character of service and product supply requires the establishment of mutual recognition of testing, validation, auditing, and liability assessment To accomplish this, the Green Book suggests establishment of an international scheme for evaluation, certification, and mutual recognition that provides for security, safety, and quality evaluations for applications, services, systems, and products. It also proposes establishment of principles for incident reporting obligations, incident containment, schemes for service provider and vendor self-evaluations and declarations, and communitywide quality criteria for safety of systems, including methodologies for the assessment of threats, vulnerabilities, and hazards for safety critical systems [8]

[6] Ibid at p 3-4
[7] Ibid , at p 5
[8] Ibid , at p 5-6

SOURCE Off Ice of Technology Assessment, 1994

pose.[82] personal data maybe processed only with the consent of the data subject when legally required or to protect "the public interest" or the "legitimate interests" of a private party, except where (hose interests are trumped by the "interests of the data subject."[83] The processing of data revealing "racial or ethnic origin, political opinions, religious beliefs, philosophical or ethical persuasion . . . [or] concerning health or sexual life" is severely restricted and in most cases forbidden without the written permission of the data subject."[84]

82 Ibid., art. 6(I).

83 Ibid., art. 7.

84 Ibid., art. 8.

Persons from whom data is to be collected must be informed of the purposes of the intended processing; the obligatory or voluntary nature of any reply; the consequences of failing to reply; the recipients of the data; the data subject right of access to, and opportunity to correct, data concerning her or him; and the name and address of the "controller."[85] This same disclosure, except for that concerning the obligatory or voluntary nature of any response and the consequences of failing to reply, must be provided to anyone about whom data is collected without their consent.[86]

The Council Directive requires member states to enact laws guaranteeing each individual access to, and the opportunity to correct, processed information about her or him. This right of access may be limited only to protect national security, defense, criminal proceedings, public safety, a "duly established paramount economic and financial interest of a member state or of the [European] Community . . ." or a similar interest.

National laws under the Council Directive must also permit data subjects to correct, erase, or block the transfer of "inaccurate or incomplete data,"[87] and the opportunity to object to the processing of personal data.[88] The Council Directive requires that data subjects be offered the opportunity to have personal data erased without cost before they are disclosed to third parties, or used on their behalf, for direct mail marketing.[89]

The Council Directive establishes basic requirements for protecting personal data from "accidental or unlawful destruction or accidental loss and against unauthorized alteration or disclosure or any other unauthorized form of processing."[90]

In keeping with most European data protection legal regimes, the Council Directive requires that controllers' notify the applicable national ● 'supervisory authority" before beginning any data processing.[91] At minimum, member States' national laws must require that the notification include: the name and address of the controller, the purpose for the processing, the categories of data subjects, a description of the data or categories of data to be processed, the third parties or categories of third parties to whom the data might be disclosed, any proposed transfers of data to other countries, and a description of measures taken to assure the security of the processing.[92]

Each supervisory authority is required to investigate data processing that "poses specific risks to the rights and freedoms of individuals."[93] For certain routine processing that does not pose significant threat to individuals rights (e.g., the production of correspondence, consultation of documents available to the public, etc.), the Council Directive permits members states to simplify or even eliminate the notification requirements.[94] Each supervisory authority is required to keep and make available to the public a '*register of notified processing operations."[95]

Under the Council Directive, each member state must establish an independent public author-

85 Ibid., art. 11 (1).
86 Ibid., art. 8.
87 Ibid., art. 14(3).
88 Ibid., art. 15(1).
89 Ibid., art. 15(3).
90 Ibid., art. 17(1).
91 Ibid., art. 18(1).
92 Ibid., art. 18(2).
93 Ibid., art. 18(4).
94 Ibid., art. 19.
95 Ibid., art. 21.

ity to supervise the protection of personal data,[96] which has the power to investigate data processing activities, to intervene and order the destruction of data that has infringed on personal rights, to order that processing cease, and to block transfer of data to third parties. The supervisory authority must also have the power to deal with complaints from data subjects and is required to issue a publicly available report at least annually.[97]

Each member state's law must provide for civil liability against those that control data for unlawful processing activities,[98] and impose penalties for noncompliance with the national laws adopted pursuant to the Council Directive.[99] National laws must provide both for enforcement by a supervisory authority and for remedies for breach of rights.[100]

Finally, although forbidden to restrict the flow of personal data among themselves because of national data protection or privacy concerns, member states will be required to enact laws prohibiting the transfer of personal data to nonmember states that fail to ensure an "adequate level of protection.''[101] The prohibition is of particular concern to U.S. business interests. The basis for determining the adequacy of the protection offered by the transferee country "shall be assessed in the light of all circumstances surrounding a data transfer," including the nature of the data, the purpose and duration of the proposed processing, the "legislative provisions, both general and sectoral," in the transferee country, and the "professional rules which are complied with" in that country.[102] However, the Council Directive does not spell out standards for making evaluations.

Because the United States lacks comprehensive laws on fair information practice, the Council Directive prompts increased scrutiny of U.S. private-sector activity in the area of data protection. U.S. business has some serious concerns about the EU proposal, as it relates to the data subject's consent and the transfer of data to non-EU countries.

With respect to issues surrounding transborder data flows, the initial version of the proposed Council Directive required all member states to prevent the transfer of personal data to a non-European Union country unless that country ensured an "adequate level of protection," where adequacy appeared to be determined by an EU evaluation of the third countries' national data protection laws. The first draft of the proposed Council Directive allowed EU level coordinating committees to establish a blacklist of countries, but did not require it. There was great concern about how the United States would be treated.

Business was especially concerned with this provision because of its potential to erect barriers to the free flow of information. This was also perceived as indirectly imposing EU standards on third-party countries, including the United States, where the approach to privacy protection is different. The business community prefers to rely on the existing structure of federal, state, and industry-specific laws in this area and on self-regulation rather than broad legislation. The business community sees the revised Council Directive as placing more emphasis on the importance of the free flow of information. It now states that the adequa-

96 Ibid., art. 30(1).

97 Ibid., art. 30(3).

98 Ibid., art. 23.

99 Ibid., art. 25.

100 Ibid., art. 22.

101 Ibid., art. 26(1). The prohibition is subject to exemptions where the transfer is necessary 1) to the performance of a Contract in which the data subject has consented to the transfer; 2) to serve an "important public Interest"; or 3) to protect "the vital interest of the data subject."

102 Ibid., art. 26(2).

cy of protection in a non-EU country "shall be assessed in the light of all the circumstances surrounding the data transfer operation," including nature of the data, purpose and duration of processing, laws, and professional rules, but believes it should go further and recognize self-regu1atory practices, such as a company's internal code of conduct.[103] The EC has commissioned an extensive study of U.S. law and practice in connection with an interest in better understanding the scope of information practices in the United States.[104]

In addressing the sufficiency of existing U.S. legal standards for privacy and security in a networked environment for the private sector:

- ***Congress could legislate to set standards similar to the OECD guidelines; or, alternatively,***
- ***Congress could allow individual interests, such as the business community, to advise the international community on its own of its interests in data protection policy.*** *However, because the EU's protection scheme could affect U.S. trade in services and could impact upon individuals, Congress may also wish to monitor and consider the requirements of foreign data protection rules as they shape U.S. security and privacy policy to assure that all interests are reflected.*

One means of assuring that a diversity of interests is reflected in addressing the problem of maintaining privacy in computerized information—whether in the public or private sector—would be for Congress to establish a Federal Privacy Commission. Proposals for such a committee or board were discussed by the Office of Technology Assessment (OTA) in its 1986 study of *Electronic Record Systems and Individual Privacy.* OTA cited the lack of a federal forum in which the conflicting values at stake in the development of federal electronic systems could be fully debated and resolved. As privacy questions will arise in the domestic arena, as well as internationally, a commission could deal with these as well. Data protection boards have been instituted in several foreign countries, including Sweden, Germany, Luxembourg, France, Norway, Israel, Austria, Iceland, United Kingdom, Finland, Ireland, the Netherlands, Canada, and Australia.

The responsibilities and functions suggested for a privacy commission or data protection board are:

1. to identify privacy concerns, that is to function essentially as an alarm system for the protection of personal privacy;
2. to carry out oversight to protect the privacy interests of individuals in information handling activities;
3. to develop and monitor the implementation of appropriate security guidelines and practices for the protection of health care information;
4. to advise and develop regulations appropriate for specific types of information systems;
5. to monitor and evaluate developments in information technology with respect to their implications for personal privacy in information; and
6. to perform a research and reporting function with respect to information privacy issues in the United States.

Debate continues as to whether such a body should serve in a regulatory or advisory capacity. In the 103d Congress, legislation has been introduced that would establish a Privacy Protection Commission.[105]

---

[103] M N Di Tosto, Manager, Telecommunications/Economic and Financial Policy, United States Council for International Business, "International Data Protection Landscape," remarks to the State of Virginia's Committee on Information Policy, July 23, 1993.

[104] The study, directed by Professor Spiros Simitis, Wolfgang Goethe College of the University of Frankfurt and conducted by Professors Paul Schwartz, University of Arkansas School of Law and Joel R. Reidenberg, Fordham University School of Law, is expected to bc released in 1994.

[105] S. 1735, the Privacy Protection Act, was introduced by Senator Paul Simon on Nov. 20, 1993.

DIGITAL LIBRARIES

Digital libraries, or networked information collections, allow online access to books, journals, music, images, databases, and multimedia works. Digital libraries rely upon technological advances in net working—ranging from advanced data storage technologies and processes to widespread use of interoperable devices and development of a National Information Infrastructure. Digital libraries would integrate networked information resources of all kinds into new collaborative environments.[106]

Digital libraries make available to institutions online versions of journals and magazines, text and graphics from books, and other print resources. Digital libraries might also include resources such as linked libraries for software, collections of human genome data sequences, and global climate data.[107] Others envision the digital library as a network of publishers, vendors, libraries, other organizations, and individuals (public, commercial and private), any of which can offer an item or collection of items.[108] These libraries will affect the way that library users obtain and report research information, and promise to provide researchers with easy access to a wide array of information resources.[109]

One example of ways in which these libraries bring together texts from a variety of sources is the Electronic Text Center, an online collection at the University of Virginia in Charlottesville. The humanities collection held at the center contains the *Oxford English Dictionary,* a wide range of Old English writings, several versions of Shakespeare's works, the complete works of 1,350 English poets, and hundreds of other literary, social, historical, philosophical, and political materials in various languages.[110] These data are stored on large-capacity magnetic disk drives, while computers in the library and elsewhere on campus can search and view all materials, including color images of manuscript pages. A text-only version of the database can be viewed over a network using desktop computers. Access to the system, which has been used increasingly since its implementation in August 1992, is limited to university students, faculty, and staff.[111]

In the area of science, an analogous system is disseminated over Cornell University's local area network called Chemistry On-line Retrieval Experiment, a prototype electronic library of 20 American Chemical Society journals. Four participants collaborate in the project: the American Chemical Society and its Chemical Abstracts Service division; Bell Communications Research (Bellcore) of Morristown, New Jersey; Cornell University's Mann Library; and the Online Computer Library Center, a database resource service

---

106 The Corporation for National Research *Initiatives* (CNRI) outlines one proposal for components of a digital system, which could include: 1) personal library systems for the users; *2)* organizational library systems for serving groups of individuals or activities; 3) new as well as existing local or distant databases; 4) database servers to handle remote requests, and 5) a variety of system functions to coordinate and manage the entry and retrieval of data. The system components are assumed to be linked by means of one or more interconnected computer networks. They assume use of active intelligent computer programs such as "knowbot" programs, that act as agents traveling within a network and accessing network resources on behalf of end users. The programs would be capable of exchanging messages with other such programs and moving from one system to another carrying out the wishes of the users.

107 Robert A iken, Network Research Program Director, U.S. Department of Energy, Livermore National Laboratories, personal communication, May 1994.

108 U S Department of Commerce, Technology Administration, *Putting the Information Infrastructure to Work: Report of the Information Infrastructure Task Force Committee on Applications and Technology,* NIST Special Publication 857 (Gaithersburg, MD: National Institute of Standards and Technology, May 1994) , p. 95.

109 Stu Berman, "Advances in Electronic Publishing Herald Changes for Scientists," *Chemical & Engineering News,* vol. *71,* No. *24,* J une 14, 1993, pp. 10, 16.

110 [bid.

111 Ibid.

for libraries, based in Dublin, Ohio. This system enables student and faculty access to a database that will eventually include more than 10 years' worth of 20 chemical journals and information from scientific reference texts. Users can electronically retrieve articles, complete with illustrations, tables, mathematical formulas, and chemical structures. They can also switch to articles on related topics, or to reference articles, using hypertext-type links. [112]

Ways in which digital information differs from information in more traditional forms include the following:

1. Digital works are easily copied, with no loss of quality.
2. They can be transmitted easily to other users or be accessed by multiple users.
3. They can be manipulated and modified easily and changed beyond recognition.
4. Works treated very differently under current copyright law are essentially equivalent: text, video, or music are all reduced to a series of bits and stored in the same medium.
5. Works are inaccessible to the user without hardware and software tools for retrieval, decoding, and navigation.
6. Software allows for new kinds of search and linking activities that can produce works that can be experienced in new ways, e.g., interactive media.[113]

The nature of digital works changes how authors create, the kinds of works they create, and the ways that readers or users read or use the works. These changes in the nature of creative works affect the operation of copyright law. (For a discussion of copyright law and the related issue of fair use, see boxes **3-6** and 3-7.) In an earlier work, OTA suggested several options for dealing with these issues. Among these were to clarify the status of mixed-media works with respect to their copyright protection and to create or encourage private efforts to form rights clearing and royalty collection agencies for groups of copyright owners.[114] However, the application of intellectual property law to protect works maintained in digital libraries continues to be uncertain; concepts such as *fair use* are not clearly defined as they apply to these works, and the means to monitor compliance with copyright law and to distribute royalties are not yet resolved.

Findings from OTA's 1992 Study of Software and Intellectual Property

In an earlier work, *Finding a Balance: Computer Software, Intellectual Property and the Challenge of Technological Change,* [115] OTA examined fundamental copyright issues raised by collections of digital information. OTA's findings still apply, and bear mentioning here.

---

112 Ibid.

113 U.S. *congress,* Office of Technology Assessment, *Finding a Balance: Computer Software, Intellectual Property and the Challenge of Technological Change,* OTA-TCT-527 (Washington, DC: U.S. Government Printing Office, May 1992). These differences were also cited in *Putting the Information Infrastructure to Work: Report of the Information Infrastructure Task Force Committee on Applications and Technology,* op. cit., footnote 108, p. 96. The report stated that "[t]he advanced information infrastructure presents three significant and qualitatively new challenges to protecting intellectual property, First, digitization offers an unprecedented, easy, and inexpensive method to produce an indefinite number of perfect copies. Second, information in disparate media can be converted into a single digital stream and can be easily manipulated to create a variety of new works. Third, digitized information can be instantaneously distributed to and downloaded by thousands of users of the network."

114 Ibid., p. 36 However, some commentators believe that an approach more appropriate to present technological capabilities would allow for direct payments. (Oliver Smoot, Executive Vice-President, Computer and Business Equipment Manufacturers Association, personal communication, May 1994.) At the same time, efforts to arrive at a standard licensing contract for online information have confronted problems. (Laurie Rhoades, Attorney Advisor, U.S. Copyright Office, personal communication , May 1994.)

115 *Finding a Balance,* op. Cit., footnote 113.

What Is a "Work"

Copyright protection attaches to an "original work of authorship" when it is "fixed in any tangible medium of expression." Thus, when an author writes a novel on a computer or word processor, it is clear that a printout is fixed and tangible and protected by copyright. It is also fairly clear that the words on the cathode-ray tube disappear when it is turned off and therefore are unprotectable.

The electronic mail message is a new type of "work" that usually exists only in digital form until it is printed out. Most messages are of a temporary nature and their authors may or may not care whether their rights under copyright are protected. Other users of electronic mail use this medium to contact and collaborate with colleagues, to express ideas, and to exchange drafts of works in progress. In these cases, people would likely wish to retain the rights to their writings.

The technology of electronic messages also raises questions about the definition of publishing for purposes of copyright. A person can forward an electronic message received from someone else very easily to any number of other people. Is this kind of distribution the same *as publishing,* a right that copyright law grants exclusively to the author? A message can also be modified before forwarding: does this create a derivative work, for which permission from the author should be gained? Whether or when an infringement of copyright occurs in these cases has not yet been tested.

A further complication in the definition of a work arises because computers make collaboration and multiple authorship easy. Many electronic mail messages are generated as a part of *computer conferences,* whereby people communicate about topics of mutual interest, even though they are geographically separated. Conferencing software on the host computer records and reorganizes incoming messages so that each participant can read what has been written by others and then add his or her own responses.

Are the proceedings of a computer conference a joint or collective work, or many separate works? If it is a collective work with many contributors, the individual contributors can claim authorship in their respective contributions, but who can claim authorship in the collection as a whole? If it is not a joint work, does each individual message constitute a separate work, or do all the contributions of one author constitute a work? The question of what constitutes the work, and the identity of the author or authors, will determine the rights that pertain thereto.

The question of the size of a work might be important in determining if infringement has taken place and if a *fair-use defense* against infringement is appropriate. Fair use is determined by four criteria (discussed in box 3-7), one of which is the amount and substantiality of material used with respect to the whole.

Special Concerns of Libraries

Many of the rules under the copyright law regarding lending and sharing library materials or making preservation copies or replacement copies of damaged works were developed with printed books and journals in mind.

Some provisions in the copyright law also deal with copying and other use of "computer programs," but do not specifically extend to digital information. The copyright law gives the owner of a computer program the right to make an archival copy under certain conditions. The library may not be the owner of the computer program. Vendors often say that programs are licensed, not sold. The library, as a licensee rather than an owner, does not have the rights described in the copyright law; these are abrogated by the terms of the license. There is considerable controversy over the enforceability of many of these contracts in which the vendor has enough bargaining power to force terms on the user. At present, there is a wide variety in the terms and conditions of software and database licenses. An institutional user like a library or university computer center often uses hundreds of different program and data packages, and ensuring compliance with all of the packages different requirements is difficult.

The copyright law also currently refers only to computer programs and not to data or digital information. Since computer data is stored in the

BOX 3-6: What Is Cc

Copyright law in the United States protects the rights of an author to control the reproduction, adaptation, public distribution, public display, and public performance of original works of authorship of every kind, ranging from books to sound recordings.

A fundamental goal of U.S. copyright law is to promote the public interest and knowledge—the "Progress of Science and useful Arts."[1] Although copyright is a property Interest, its primary purpose was not conceived of as the collection of royalties or the protection of property, rather, copyright was developed primarily for the promotion of intellectual pursuits and public knowledge As the Supreme Court has stated

> The economic philosophy behind the clause empowering the Congress to grant patents and copyrights is the conviction that encouragement of individual efforts by personal gain is the best way to advance public welfare through the talents of authors and inventors in Science and the useful Arts [2]

Much of the structure and basis for American law is derived from its British legal antecedents After the Introduction of the printing press in England in the late 1400s, the Crown's first response was to control what writings were printed or copied The earliest British copyright laws were enacted in the 1500s to promote censorship by the government to cooperation with a monopolistic group of printers known as the Stationer's Guild This system collapsed when the company failed to exercise discretion as a censor, but used its monopoly power to set high prices. Parliament's response in 1695 was to allow the Stationer's copyrights to expire, but this resulted in a period of anarchical publication. In 1709 Parliament responded to the situation by enacting legislation known as the Statute of Anne This statute granted a copyright to authors, as opposed to printers, for a period of 14 years The copyright was renewable for an additional 14 years if the author was still alive After the expiration of the copyright, the writing became part of the public domain available for use by anyone This first modern copyright law became the model for subsequent copyright laws in English-speaking countries [3]

After severing ties with Great Britain, the former American colonies sought means to secure copyright laws in 1783, the Continental Congress passed a resolution encouraging the various states to enact copyright legislation All of the states except Delaware enacted some form of copyright statute, although the various State laws differed greatly [4] Because of the differences in the State copyright laws and the ensuing difficulties, the Framers of the Constitution, notably James Madison, asserted that the copyright power should be conferred upon the legislative branch [5] This concept was ultimately adopted, and Congress was granted the right to regulate copyright (art 1, sec. 8, cl 8). [6]

---

[1] The Constitution provides that "Congress shall have power to Promote the Progress of Science and useful Arts, by securing form limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries "

[2] *Maser* v Stein, 347 US 201219 (1954)

[3] See U S Congress, Off Ice of Technology Assessment, Intellectual *Properly Rights m an Age of Electronics and Information,* OTA-CIT-302 (Washington, DC U S Government Printing Office, April 1986)

[4] R P Lyman, *Copyright in Historical Perspective* (Nashville TN Vanderbilt University Press 1968), p 183

[5] Ibid

[6] Congress's constitutional grant of copyright regulation is more restricted than its English antecedents

BOX 3-6 (cont'd): What Is Copyright?

The First Congress in 1790 enacted the first federal copyright act This legislation provided for the protection of author's rights [7] Commentators have written that the central concept of this statute is that copyright is a grant made by a government and a statutory privilege, not a right. The statute was substantially revised in 18318 to add copyright coverage to musical compositions and to extend the term and scope of copyright. A second general revision of copyright law in 1870[9] designated the Library of Congress as the location for administration of the copyright law, including the deposit and registration requirements. This legislation extended copyright protection to artistic works The third general revision of American copyright law in 1909[10] permitted copyright registration of certain types of unpublished works The 1909 legislation also changed the duration of copyright and extended copyright renewal from 14 to 28 years A 1971 amendment extended copyright protection to certain sound recordings.[11] The fourth and most recent overhaul of American copyright law occurred in 1976, after years of study and legislative activity The 1976 legislation modified the term of copyright and, more significantly, codified the common law fair-use concept as a limitation on the exclusive rights of the copyright holder In 1980, following recommendations made by the National Commission on New Technological Uses of Copyrighted Works, legislation explicitly extended copyright to computer programs.[12]

The copyright statute interprets the constitutional term "writings" broadly, defining it as:

> works of authorship fixed in any tangible medium of expression now known or later developed, from which they can be perceived, reproduced or otherwise communicated, either directly or with the aid of a machine or device.[13]

Copyright protection is expressly provided for eight categories of a works literary; musical, dramatic, pantomimes and choreographic, pictorial, graphic and sculptural; motion picture and other audiovisual works, sound recording, and architectural, however, the legislative history indicates that these categories are not meant to be exhaustive Computer programs are copyrightable as "literary works" as defined in 17 U.S.C 101.[14]

The term *computer program* IS also defined in section 101 as "a set of statements or instructions used directly or indirectly in a computer in order to bring about a certain result. "

Copyright protection subsists from the time work of authorship is created in a fixed form. The copyright in the work becomes the property of the author immediately upon creation. Only the author or one deriving rights through the author, can rightfully claim copyright.

---

[7] Ch 15, Sec 1, 1 Stat 12 See, OTA- CIT-302, op. cit footnote , p.64

84 Stat 436

9 Act of July 8, 1879, c 230, 16 Stat198

10 Act of March 9, 1909 c 320, 35 Stat1075

11 Public law 92-14 r), Oct 15, 1971, 85 Stat [91]

1217 USC107, 11 7

13 17 U S C 102(a)

1417 U S c 101 provides in pertinent part "Literary works" are works, other than audiovisual works, expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, periodicals, manuscripts, phonorecords, film, tapes, disks or cards, in which they are embodied

(continued)

BOX 3-6 (cont'd.): What Is Copyright?

In the case of works made for hire, the employer rather than the employee is presumptively considered the author A work made for hire is define as

1 a work prepared by an employee within the scope of his other employment, or
2 a work specially ordered or commissioned for use in a variety of circumstances enumerated by the statute

Copyright does not protect ideas, but rather the expression of ideas Copyright protection does not extend to any

> procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, Illustrated, or embodied [15]

Copyright protects the writings of an author against unauthorized copying, distribution, and so forth, and protects the form of expression rather than the subject matter of the writing Unlike patents, it does not protect against independent creation Copyright grants the owner the exclusive right to do and to authorize others to do the following:[16]

- reproduce copies of the copyrighted work,
- prepare derivative works based on the copyrighted work;
- distribute copies of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease or lending,
- perform the copyrighted work publicly, and
- display the copyrighted work publicly.[17]

The statute does, however, specify certain Imitations to the copyright owner's exclusive rights that are noninfringing uses of the copyrighted works These limitations Include the "fair use" of the work (17 U S C 107(1988)), certain kinds of reproduction by libraries and archives (17 U S C 108 (1988)), certain educational performances and displays (17 U S C 110 (1988)), and certain other uses (17 U S C 117 (1980))

It is an Infringement of the copyright for anyone to engage in any of the activities enumerated above without the authorization of the copyright owner The copyright statute provides that the copyright owner may institute an action for Infringement against the copyright infringer to prevent further infringement of the copyright (17 U S C 502 (1988)) An Infringer of a copyright may be subject to the payment of actual damages and profits to the copyright owner (17 U S C 504 (b)(1988)), or in certain circumstances the copyright owner may elect specified statutory damages within specified ranges in lieu of actual damages and profits (17 U S C 504 (c)(1988)) In addition, in certain cases the court may permit the recovery of legal fees and related expenses involved in bringing the action (17 U S C 505 (1988)) Criminal sanctions may also be imposed for copyright infringement in certain cases (17 U S C 506 (1988))

---

15 17 U S C 102(b)

16 Not all works, however, enjoy all rights For example, sound recordings have no public Performance right 17 USC 106(4)

17 17 u s c 106

SOURCE U S Congress, Off Ice of Technology Assessment, *Copyright and Home Copying Technology Challenges the Law* OTA-CIT-422 (Washington, DC U S Government Printing Off Ice, October 1989).

BOX 3-7: Fair Use

The tension between the stimulation of intellectual pursuits and the property interests of the copyright owner has been a central issue in the development, implementation, and interpretation of American copyright laws Moreover, the concept of copyright presents a seeming paradox or contradiction when considered within the context of the first amendment freedom of speech guarantees while the first amendment guarantees freedom of expression, it can be argued that copyright seems to restrict the use or dissemination of Information. It can be argued, however, that copyright, to the degree that it stimulates expression and encourages writing and other efforts, furthers first amendment expression values by encouraging the quantity of "speech" that is created. [1] In attempting to resolve these conflicting interests, the courts have adopted a test that weights the interests of freedom of expression and the property interests of the copyrightholder to arrive at an acceptable balance [2] An extensive body of case law has been developed that weighs and counterbalances first amendment concerns and the rights of the copyright holder [3]

Hence, the American copyright system is based on dual interests intellectual promotion and property rights Combined with these factors is the first amendment freedom of expression concern, Courts have balanced and assessed these seemingly conflicting elements, and Congress has considered them in enacting copyright legislation

Much of the historical balancing has occurred in the context of the fair-use doctrine The doctrine of fair use as codified in the Copyright Act of 1976 has antecedents in British law of the 18th and 19th centuries and in 19th century U S case law Various approaches have been adopted to interpret the fair-use doctrine It has been said that the doctrine of "fair use" allows the court to bypass an inflexible application of copyright law, when under certain circumstances it would impede the creative activity that the copyright law was supposed to stimulate Indeed, some commentators have viewed the flexibility of the doctrine as the "safety valve" of copyright law, especially in times of rapid technological change Others have considered the uncertainties of the fair-use doctrine the source of unresolved ambiguities.

In codifying the fair-use exception in the Copyright Act of 1976, Congress did not formulate a specific test for determining whether a particular use was to be construed as a fair use Rather, Congress created statutory recognition of a list of factors that courts should consider in making their fair-use determinations The four factors set out in the statute are

1 the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
2 the nature of the copyrighted work;
3 the amount and substantiality of the portion used in relation to the copyrighted work as a whole, and
4 The effect of the use on the potential market and value of the copyrighted work (17 U.S.C. 107)

---

[1] HIS also argued that freedom of speech guarantees the speaker the right to speak his or her own expression, and that it does not give him the right to speak) or copy someone else's expression Nor does it prevent a speaker from using the ideas or information in someone else's ideas, facts, or information Copyright requires the speaker to arrive at his own expression from the ideas he wishes to express The resulting conflict or balance between these interests is part of copyright Itself —limited protection, with the limitations specifically designed to encourage publication and access to information The remaining conflict, it is argued, maybe resolved by fair use Mary Jensen, University of South Dakota School of Law, personal communication, Sept 29, 1991

[2] Melville Nimmer, *Nimmer on Copyright (New* York, NY Bender, 1991), VOI 1, sec 1 10

[3] See *Harper& Row Publishers, Inc v Nation Enterprises, 471* U S 539 (1985)

(continued)

BOX 3–7 (cont'd.): Fair Use

Congress realized that these factors were "in no case definitive or determinative" but rather "(provided some gauge [SIC] for balancing equities " It appears that Congress developed a flexible set of criteria for analyzing the circumstances surrounding each fair-use case, and that each case would be judicially analyzed on an ad hoc basis Therefore, courts seem to have considerable latitude in applying and evaluating fair-use factors [4] Courts have given different weight and interpretation to the fair use factors in different judicial determinations The following Illustrations demonstrate how some courts have interpreted certain fair-use factors

In evaluating the first factor, the purpose and character of the use, courts have not always held that the use '(of a commercial nature" precludes a fair-use finding, nor does a "nonprofit educational" purpose mandate a finding of fair use A defense of fair use on the basis of the first criterion will more often be recognized, however, when a defendant uses the work for educational, scientific, or historical purposes

Consideration of the second factor, the nature of the copyrighted work, must be based on the facts and circumstances of each particular case For instance, courts have Interpreted the scope of the fair use doctrine narrowly for unpublished works held confidential by their authors

In examining the third factor, the amount and substantiality of the portion of the work used, courts have looked at both the quantitative aspect—how much of the work is used—and the qualitative factor—whether the "heart" or essence of the work is used The fair-use doctrine is usually not considered to be applicable when the copying is nearly a complete copy of the copyrighted work, or almost verbatim. Before the Court of Claims decision in *Williams & Wilkins Co v United States,* [5] courts as a rule did not allow fair use for copying of entire works or substantial portions of a work However, the issue of copying entire works was the topic of significant debate prior to passage of the 1976 act The result of this debate, which allows for this kind of copying under limited circumstances, is found in section 108, which sets out guidelines for classroom copying, and in interpretation of fair use in the legislative reports. [6]

In assessing the fourth factor, courts have examined the defendant's alleged conduct to see whether it poses a substantially adverse effect on the potential market for, or value of, the plaintiff present work These considerations are used with great care by the courts in applying the fair-use doctrine on a case-by-case basis

Congress looked to the issue of copyright fair use at some length in 1991, examining whether the fair use doctrine and the First Amendment permit biographers to make unauthorized use of their subject's unpublished letters and manuscripts The courts have decided this issue on the basis of the specific facts of each case, but emphasizing the unpublished nature of the work in denying fair use

In 1991 the Senate passed S 1035 to clarify that the unpublished nature of a copyrighted work does not per se preclude applicability of the fair use defense to infringement A similar measure was deleted from H R 2372 when a district court ruled in favor of a biographer in *Wright v Warner Books* [7]

---

[4] For a historical analysis of the fair use factors, see William Patry, *The Fair Use Privilege in Copyright Law* (Washington, DC The Bureau of National Affairs 1985) ch 17

[5] *Williams & Wilkins Co v United States*, 172 US P Q 670 (Ct Cl 1972), 487 F 2d 1345, 180 US P Q 49 (Ct Cl 1973), *aff'd by an equally divided court*, 420 U S 376 184 U S P Q 705 (1975)

[6] Patry op cit footnote 4, PP 449450

[7] Wright v Warner *Books,* 748 F Supp 105 (DC SNY 1990) The Second Circuit affirmed

SOURCE U S Congress, Off Ice of Technology Assessment, *Copyright and Home Copying Technology Challenges the Law,* OTA-CIT-422 (Washington, DC U S Government Printing Off Ice, October 1989) and cited sources

same medium as computer programs, it would seem logical to treat them in the same way. However, the argument remains that digital data does not fit the definitions currently set out in section 101 of the Copyright Act so owners have no right to make archival copies. The two points raised here become even more complicated for libraries in the case of mixed-media works in which printed material, digital data, computer programs, microfiche, and other forms might be packaged and used together.

Libraries have long participated in resource sharing whereby several libraries cooperatively purchase material, and some libraries don't make certain purchases in the knowledge that the material can be obtained through interlibrary loan. Resource sharing practices have long been viewed as prudent use of both funds and storage space, especially for low-demand items. Interlibrary loans of collections among libraries is institutionalized by tradition and acceptable under the provisions of the Copyright Act (section 108). Interlibrary loan exchanges have increased dramatically in recent years. However, sharing of other information resources has recently come under fire from some publishers, who see them as depriving information providers of sales. Publishers protect their interests by leasing, instead of selling materials, thus denying libraries the rights that ownership (e.g., of printed works) permits under the *first-sale doctrine*. Contracts with electronic information providers sometimes limit or forbid sharing or lending of materials. Libraries, particularly public ones, have an obligation to balance the interests of users and publishers—a balance that the Copyright Act is intended to maintain. The growing use of electronic information, and the tendency of information providers to control the uses of this material through contracts, may lead to distinctions between for-profit and not-for-profit libraries, in terms of their operations, cost differentials, and access.

Other issues to be resolved are policies about the use of material obtained by library patrons. Some libraries offer online information and other services such as access to electronic bulletin boards to their patrons. These libraries become an additional link in a complex of transactions. To what extent are libraries responsible if users make unauthorized copies, post copyrighted material on electronic bulletin boards, send obscene messages, or otherwise infringe copyrights, violate contracts, or break laws? These problems are not new. The photocopier eventually caused libraries to adopt a policy of providing copiers, posting a notice about the copyright law, and then leaving users unsupervised to follow their own consciences. Policies regarding digital information—what can be downloaded, number of printouts allowed, etc.—will also be developed. The development of policies for digital information may be more complex since contracts with information vendors will also be involved.

Authorship and Compilations

Copyright attaches to "original works of authorship.. . ." *Original* in this case means that the work was independently created by the author and not copied from another work. The U.S. Supreme Court has defined *author* as "he to whom anything owes its origin; originator; maker." Because much of digital information is in the form of compilations of facts, which are not original, how much of the publisher's contribution to selection, arrangement, and organization of facts should be protected by copyright is sometimes controversial.[116]

---

116 The U.S. Supreme Court *addressed this* issue *in Feist Publications v. Rural Telephone Service Co., Feist* v. *Rural Telephone*, 499 U.S. 340 *(1991), finding that* telephone White Pages are not copyrightable, and that copying them into another compilation was not an infringement. The Court held that the proper test for copyrightability of a compilation is originality-not "sweat of the brow" or "industrious collection" as courts had previously held.

Use of Digital Information

Like print publishing, electronic publishing is about delivering works to readers and returning royalties to copyright holders. Several characteristics of digital information make the delivery system different and lead copyright owners and their publishers to want more control over the readers' uses of the information.

In using an online information service, a reader buys access to the electronic information. Once that access is permitted, the information is out of the control of the copyright owner and the publisher. For the most part, publishers have no way of knowing how the material is finally used or disposed of. For this reason, publishers consider information as used as soon as it reaches the reader and, as a result, generally require that it be paid for in advance. Schemes for digital libraries usually postulate charging for use of documents based on how much information a user has retrieved.

This means that some amount of useless information is paid for by the user. A partial remedy for this is to improve search and retrieval software and to offer means to browse through information before a reader commits to requesting a whole document. Users generally have to agree to certain limitations on their use of the information, in order to gain access to the database. Copies of a work can be purchased on CD-ROM (Compact disc-read only memory) or disc, but in many instances, the work is leased or licensed in this form, not purchased. The first-sale doctrine does not apply in these instances; the use of the material is subject to the terms of the license agreement. Contracts may also govern the rights and responsibilities at each link of the distribution chain through which digital information comes to the end user.

Traditionally, copyright law does not give copyright owners rights to control the access that readers have to information. Copyright owners in the electronic world use contracts to impose restrictions to ensure that they are paid for every instance of access or use. Still, as a practical matter, these restrictions do not prevent unauthorized copying. Once a user has paid for one legitimate copy of something, little can be done to prevent him or her from making other copies. Digital information is easily copied and easily transmitted to many locations. These characteristics make electronic distribution an attractive publishing medium, but there is a potential for any reader to become a "publisher" of unauthorized copies.

Unauthorized Copying

Unauthorized copying is not a problem unique to digital information, yet digital copies are unique in that, unlike photocopies and facsimiles, each copy is of the same quality as the original. Distribution is easy; the copy can be posted on a computer bulletin board or distributed to a list of users on a computer network. Scanning technology allows one to turn information on paper into digital information so that it can be changed or manipulated, and if one wants to disguise the origins or authorship of the document, format changes can be made with a few keystrokes.

Technological proposals for limiting unauthorized copying generally seem to work only within a closed system. Once a user moves an authorized copy out of the system, there seems to be no way to prevent further copying. Some writers suggest that there is no solution to the problem of unauthorized copying and that the problem is sufficiently grave that electronic publishing will never thrive as an industry because authors and publishers will not release works in digital form. However, it is possible that, as in the case of the photocopying of books or home taping of musical recordings, a viable market will persist despite the presence of unauthorized copies.

OTA Options from the 1992 *Study*

In *Finding a Balance*, OTA offered several options to Congress to address these issues. As Congress has not revisited these fundamental copyright questions, it is worthwhile to bear these in mind when examining computer security issues surrounding networked information collections.

To deal with the issues of ***fair use*** *of works in electronic form, OTA suggested that:*

- *Congress might clarify the fair-use guidelines in the Copyright Act with regard to lending, resource sharing, interlibrary loan, archival and preservation copying, and copying for patron use.*
- *OTA further suggested that Congress might establish legislative guidance regarding fair use of works in electronic form and what constitutes copying, reading, and using. Another option would be to direct the Copyright Office, with assistance from producers and users of electronic information, to develop and disseminate practical guidelines regarding these issues.*

With respect to question raised concerning ***multimedia works,***

- *OTA suggested that Congress clarify the status of mixed-media works with regard to their protection under copyright.*

Multimedia Works and Performances over Networks

Networked information systems will contain an increasing amount of electronic information in multimedia format, causing concern in the library community with respect to copyright protection. The fact that digital storage makes all works essentially equivalent complicates the definition and treatment of digital work under the law of copyright. Current copyright law allocates particular rights according to the category to which the work belongs, including literary works, dramatic works, pictorial, graphic and sculptural works, audiovisual work, motion pictures, musical compositions, computer programs, and sound recordings. These different categories sometimes have different implications for uses and protections of the work. There is no category for a mixed-media work that combines examples from each of these categories.[117]

One approach suggests that a mixed-media work should be considered to be a series of different works, with each type of work treated according to its class. However, enforcement of intellectual property rights in such a system would be complex. Another approach would be to consider the whole package as if all the works were of the same category.[118] This approach would potentially produce what could be argued to be inequitable distribution of intellectual property royalties.

Copyright protects the writings of an author against unauthorized copying, distribution, and so forth, and protects the form of expression rather than the subject matter of the writing. It does not protect against independent creation. Copyright grants the owner the exclusive right to do the following: (and to authorize others to):

- reproduce copies of the copyrighted work;
- prepare derivative works based on the copyrighted work;
- distribute copies of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease or lending;
- in the case of certain works (literary, musical, dramatic and choreographic works, pantomimes, and motion pictures and audiovisual works), perform the copyrighted works publicly; and
- in the case of the certain works, display the copyrighted work publicly.[119]

The statute (17 U. S. C.) does, however, specify certain limitations to the copyright owner's exclusive rights. It grants to others the noninfringing use of the copyrighted works. These limitations include the fair use of the work (section 107), cer-

---

117 Commentators point out that only 10 percent of all copyrighted works are affected by multimedia and networking, and that while some review of the law may be necessary, what is really needed is a confluence of business and licensing practices. (Oliver Smoot, Executive Vice-President, Computer and Business Equipment Manufacturers Association, personal communication, May 1994.)

118 American Association Of Law Libraries, "Copyright Consideration for the Use of Mixed Media in Libraries," discussion draft, appeared as an appendix to *A-V Micrographics S1S Newsletter, vol. 10, No. 2,* May 1990, and *Automation, vol. 9, No. 2,* winter 1990, pp. 12-23.

119 17 U. S. C., sec. 106.

tain kinds of reproduction by libraries and archives (section 108), certain educational performances and displays (section 110), and certain other uses (section 117).

The copyright law also provides a *first-sale doctrine* that upholds the copyright of the copyright owner during the first sale or commercial transaction of the work, but extinguishes the copyright owner's rights in subsequent sales or transactions of the purchased copy. The House Report accompanying the original (1976) legislation provided an example of the application of the first-sale doctrine:

> Thus, for example, the outright sale of an authorized copy of a book frees it from any copyright control over its resale price or other conditions of its future disposition. A library that has acquired ownership of a copy is entitled to lend it under any conditions it chooses to impose. [120]

Exceptions to this provision include computer programs embodied in a machine or product that cannot be copied during ordinary operation or use, or computer programs embodied in or used in conjunction with a limited-purpose computer, those designed particularly for playing video games.

The unifying issue surrounding all copyrighted works is the right to make copies for various purposes. Once a copy is sold, the loaning of physical objects, such as books or serials, is not at issue, nor is the ability of a library patron to view a book owned by a library. But when copyright law is applied beyond the realm of printed material (e.g., recordings, videotapes, and disks), it addresses not only the right to copy, but also the right to publicly display and perform works.

The issues related to traditional audiovisual materials have already been a source of problems for libraries. Early experiences with the lending of software also has raised numerous issues.[121] More important, however, may be determining to what extent the rights of public performance and display will be attributed to the viewing of electronic information of all types, ranging from the library user's browsing of bitmapped images of print pages through interaction with a digital movie driven by a program, 22

Widespread development of multimedia authoring tools will raise other issues as well. Multimedia integrates film clips, visual images, music, and sound along with other content, and most developers of multimedia are not simultaneous y artists, composers, and musical performers. There may well be a demand for copyright-free (public domain) materials that can be included in multimedia works. There are a large number of ambiguous copyright questions in this regard, with limited consensus and certainty. These questions include:

- Who owns the rights to digitize an image, including photographs, images of classic paintings, and other materials?
- If an image or other kind of data is digitized and subsequently enhanced, is the second-generation image protected under copyright?
- To what extent is the linkage of a series of media (e.g., images and a sound tract) copyrightable

---

120 See U.S. Congress, House of Representatives, Committee on the Judiciary, *Report to Accompany .$. 22,* H.Rpt. *94-1476* (Washington, DC: U.S. Government printing Office, September 1976), p. 79.

121 Library lending ~) f computer software was the subject Of a recent Copyright Office study and report to Congress, The *Computer Software Rental Amendments Act Of 1990: The Nonprofit Library Lending Exemption to the Rental Right,* A Report of the Acting Register of Copyrights, March 1994. Some commentators note that these issues are even more complicated with respect to multimedia works. They assert that it is unclear whether the Software Rental Act applies to multimedia. (Jeffrey Neuberger, Associate, Brown, Raysman & Millstein, personal communication, May 1994.)

122 U.S. Congress, *office* of Technology Assessment, *Accessibility and Integrity of Networked Information Collections—Background Paper,* background paper prepared for OTA by Clifford A. Lynch, BP-TCT-109 (Washington, DC: Office of Technology Assessment, July 1993).

Some commentators believe that these rights would be best determined from a license agreement. (Oliver Smoot, Executive Vice-President, Computer and Business Equipment Manufacturers Association, personal communication, April 1994.)

separately from the images themselves and the soundtrack itself?
- To what extent are libraries (or other networked information providers) liable for contributing to copyright infringement in an electronic information environment? [123]
- Does the rightholder in a work hold all necessary rights to that work's components? What rights have been conveyed through already existing agreements? How are necessary rights acquired?
- Depending on what works are incorporated, and the method by which the product is to be exploited (including manufacture, sale, and distribution), what rights are necessary to each item included in the product? [124]

While these questions may be decided through the courts, most libraries do not wish to serve as test cases, and some are concerned that this attempt to limit the potential legal liability of the current uncertain copyright framework may contribute to the destruction of the interlibrary loan system by turning to a contract or licensing approach to acquiring material.[125]

With respect to these types of works:

- ***Congress could allow the courts to continue to define the law of copyright as it is applied in the world of electronic information; alternatively,***
- ***Congress could take specific legislative action to clarify and further define the law in the world of electronic information.*** [126]
- ***Congress could also allow information providers and purchasers to enter into agreements that would establish community guidelines without having the force of law.*** [127] ***In so doing, Congress*** *could decide at some point in the future to review the success of such an approach.*

Copyright Collectives

Collectives are a way to share the profits within an industry when tracking the user of individual elements of intellectual property is not feasible. The music industry, represented in organizations such as the American Society of Composers, Authors and Publishers (ASCAP) and Broadcast Music, Inc. (BMI), adopted such an approach to manage the copyright in musical works and share the revenue from those rights based on statistical estimates of the amount of use of the artist's work.

ASCAP assigns each performance a value depending on the type, for example, a feature or background performance. Each performance is then weighted according to the size and importance of the logged station, time of day of program, and so forth, to determine the total number of performance credits. Quarterly, the total performance credits for writers as a group and for publishers as a group are divided into the respective dollars of distributable revenue to yield the dollar value of a performance credit for each group. On payment, ASCAP issues a detailed statement showing the title of the work surveyed, the num-

---

123 Lynch (ibid.), pp. 26-27. Digitization Of information and creation of digital libraries raises questions central to the law Of copyright itself. For example, what constitutes a copy? How much must a work be changed when it is no longer a copy? When a work has been digitally manipulated, how does one prove that is or is not a copy? What constitutes fair use in a digital environment? These questions, however, are beyond the scope of this inquiry, but are discussed in depth in an earlier OTA report, *Finding a Balance*, op. cit., footnote 113. Recent work on the appropriateness of the copyright paradigm for the information highway includes: R. Nimmer and P. Krauthaus, 'copyright in the Information Superhighway: Requiem for a Middleweight," *Stanford Journal of Law and Policy* (in press).

124 Jeffrey Neuberger, Associate, Brown, Raysman & Millstein, personal communication, May 1994.

125 C.A. Lynch, op. cit., footnote 122, pp. 19-28.

126 Some commentators suggest that it is inappropriate to make potentially radical changes to the copyright law to address the concerns of libraries. (Oliver Smoot, Executive Vice-President, Compuater and Business Equipment Manufacturers Association, personal communication, April 1994.)

127 Some commentators express the concern that such an approach would potentially violate the antitrust laws. (Ibid.)

ber of performance credits earned, and the media on which the performance appeared.

ASCAP has two systems of payments for its writers: the *current performance* plan distributes the writer's share of the money on the basis of his or her performance over the past four quarters. New writer members are initially paid on the current performance plan, with the option of switching to the *four-find* basis after three full survey years. The four-fund system is a deferred payment plan based partly on current performance, but mostly on an average of performances over a period of five or 10 years.

Distribution of royalties to publishers is determined on a current performance basis only, in which the publisher is paid on account for the first three quarters, with adjustments made in the fourth quarter.

BMI affiliates are paid according to a published royalty payment schedule, which distinguishes between radio and television performances and between feature, theme, and background musical performances. A performance index is calculated for each performance, based on the number of times it is played on the radio and television stations and the total revenue earned paid to the affiliates. BMI's royalty payment schedule allows for bonus credits based on the number of times a work is played on the radio or television. Bonus credits are calculated on a song-by-song basis.

Management and protection of copyright in the context of digital libraries and the National Information Infrastructure face similar challenges to those confronted by the music industry. OTA suggests that private efforts to form clearing and royalty collection agencies for groups of copyright owners be encouraged or that Congress create such groups. Collectives similar to ASCAP and BMI are contemplated by some for administering copyright in digital information; private-sector information providers are particularly concerned that these collectives remain a private-sector initiative.

The Copyright Clearance Center, Inc. (CCC) has attempted to resolve some of these issues with respect to electronic conversion, storage, and distribution of full-text copyrighted material. The CCC is an organization of publishers, authors, and users formed at the suggestion of Congress to facilitate compliance with reprographic rights as defined in the 1976 Copyright Act. Since 1988, CCC has instituted pilot electronic licensing studies in, among others, the areas of telecommunications. CCC recognizes the need to address the possibilities for altering the integrity of the information or disseminating it widely without authority, and is investigating the role of encryption, validation, access and manipulation restrictions, and usage monitoring.

Several services already provided by CCC might serve as models or guides for treatment of copyright in electronic texts. The Transactional Reporting Service provides users-document suppliers, academic institutions, government agencies, law firms, medical centers, small corporations, and individual—with the immediate authorization to make photocopies from 1.5 million publications from more than 8,500 publishers worldwide A record of photocopying activity is reported to CCC, which provides a printed or CD-ROM catalog of all CCC-registered titles and their individual royalty fees. Copies are reported monthly, and CCC collects royalties and distributes fees to the rightholders.

CCC also provides the Annual Authorization Service, a mechanism for facilitating copyright compliance. By paying a single annual fee, licensees are authorized to photocopy excerpts (for internal distribution) from 1.5 million journals, books, magazines, and newsletters from 8,500 domestic and foreign publishers. Licensees eliminate the need to seek individual permissions from publishers, as well as the need for tracking, reporting, and paying fees for individual copying acts. The annual fee is determined by a statistical process that combines fees set by the rightholder with data derived from surveys of actual copying behavior by categorized employee populations.

In contrast to these licensing approaches to administering copyright, others believe that the tracking and monitoring capabilities of the computers and networks comprising the digital library

allow creation of an environment that operates strictly on a *fee-for-use* basis.[128] The Corporation for National Research Initiatives (CNRI) has proposed a test bed for an electronic copyright management system. The proposed system would include four major elements: automated copyright recording and registration, automated online clearance of rights, private electronic mail, and digital signatures to provide security. It would include three subsystems: a registration and recording system (RRS), a digital library system, and a rights management system (RMS). The RRS would provide the functions enumerated above and would be operated by the Library of Congress. It would provide "change of title" information. The RMS would be an interactive distributed system capable of granting rights online and permitting the use of copyrighted material in the digital library system. The test-bed architecture would involve computers connected to the Internet performing the RRS and RMS functions. Digital signatures would link an electronic bibliographic record (EBR) with the contents of the work, ensuring against alteration after deposit. Multiple RMS servers would be attached to the Internet. A user wishing to obtain rights to an electronically published work would interact electronically with the appropriate RMS. When copyright ownership is transferred, a message could be sent from the RMS to the RRS, creating an electronic marketplace for copyrighted material. The EBR submitted with a new work would identify the rightholder and any terms and conditions on the use of the document or a pointer to a designated contact for rights and permission. The CNRI test-bed proposal envisions the use of public key encryption to ensure the integrity of digital signatures and to ensure the authenticity of information.[129] The Copyright Clearance Center is attempting to develop a scheme for determining rights and permission for use online. Other private-sector groups have also been involved in this effort.[130]

With respect to rights and royalties:

- ***Congress may wish to encourage private efforts to form clearing and royalty collection agencies for groups of copyright owners; alternatively,***
- ***Congress might allow private-sector development of network tracking and monitoring capabilities to support a fee-for-use basis of copyrighted works in electronic form.*** *Congress could also choose to review whether such an approach is a workable one, both from the standpoint of technological capabilities and copyright protection (e.g., Does such an approach serve the fair-use exception? Can network technologies effectively address this question?). This might be accomplished by conducting oversight hearings, undertaking a staff analysis, and/or requesting a study from the Copyright Office.*

---

128 One set of requirements for protective services for dissemination of copyrighted materials that has been proposed includes a mechanism for authentication, implementation of means to limit redistribution, protection against plagiarism and change, storage and exchange of information in standardized but device-independent forms, and means for appropriate remuneration. R.J. Linn, "Copyright and Information Services in the Context of the National Research and Education Network," *IMA Intellectual Property Protection Proceedings, vol. 1,* Issue 1, p. 9.

129 H. Perritt, "Permissions Headers and Contract Law," *IMA intellectual Property Protect Proceedings, vol. 1, Issue* 1, p. 29-32.

130 Among these initiatives are efforts on the part of the Corporation for National Research Initiatives and the Interactive Multimedia Association, Project Xanadu, Coalition for Networked Information, and TULIP (The University Licensing Program).