3-1-1980

# Computer Law: An Overview

David C. Tunick

# COMPUTER LAW: AN OVERVIEW

*by David C. Tunick**

Since World War II, computer use has increased dramatically.[1] Computers[2] are now used in such diverse activities as accounting, hotel and airline reservations,[3] subway and ship movement, traffic light timing,[4] bank check processing,[5] credit bureau information storage,[6] space mission control, manufacturing processes, patient monitoring in hospitals, newspaper printing, and even in the design of other computers.[7]

* B.A., 1963 (University of California at Los Angeles); J.D., 1971 (University of California at Los Angeles). Professor of Law, Loyola Law School, Los Angeles.

[1] This increased use is discussed in Bigelow, *The Lawyer's Role in the Computer Age*, [1972-1979 Transfer Binder] 1 COMPUTER L. SERV. § 1-1, at 1-4 (R. Bigelow ed.) [hereinafter cited as Bigelow].

[2] It is appropriate to define "computer" to assure that the scope of this article is clear. Unfortunately, there is no unanimous agreement as to the meaning of "computer." See, *e.g.*, C. MEEK, GLOSSARY OF COMPUTING TERMINOLOGY 52 (1972) [hereinafter cited as MEEK], which provides four definitions of "c.omputer."

In the materials prepared by the author for his law school course, Computers and the Law, the author defines "computer" by the functions it is capable of performing. Six functions have been found to be shared by devices commonly accepted as "computers." First of all, a computer is capable of containing a stored program, *i.e.*, the computer program can be input into the computer so that the computer becomes capable of analyzing data without human intervention. Second, a computer has branching capability such that the computer program has a choice of following more than one path of instructions, depending upon the nature of the data input to the computer. Third, a computer does arithmetic operations, *i.e.*, addition, subtraction, multiplication, and division. Fourth, a computer does comparison operations, *i.e.*, the computer must be able to tell if two numbers are equal, or one is greater, and if so, which is greater. Fifth, a computer has input capability. And finally, a computer has output capability. Without the last two functions, a computer would be virtually useless.

[3] Bigelow, *supra* note 1, at 1.

[4] *Id.*

[5] Freed, *A Lawyer's Guide Through the Computer Maze*, 6 PRAC. LAW. 15, 18 (Nov. 1960) [hereinafter cited as Freed]. It is beyond the scope of this article to discuss the problems that arise from the use of computers in banking. Cases that address this area include Independent Bankers Ass'n of America v. Smith, 534 F.2d 921 (D.C. Cir.), *cert. denied*, 429 U.S. 862 (1976) (customer-bank communication terminals may constitute a bank branch under some circumstances); First Nat'l Bank & Trust Co. v. Georgia R.R. Bank & Trust Co., 229 S.E.2d 482 (Ga. Ct. App. 1976), *aff'd per curiam*, 235 S.E.2d 1 (Ga. Sup. Ct. 1977) (check in amount of $25,000 improperly encoded magnetically as being for $2500); Gabalac v. Firestone Bank, 346 N.E.2d 326 (Ohio Ct. App. 1975) (check in amount of $45 improperly encoded magnetically as being for $10,045).

[6] *The Battle to See Your File—Part Three*, PRIVACY J., June 1978, at 6.

[7] These uses and others are noted in Telex Corp. v. IBM, 367 F. Supp. 258, 271-72 (N.D. Okla. 1973), *rev'd on other grounds*, 510 F.2d 894 (10th Cir.), *cert. dismissed*, 423 U.S. 802 (1975).

As an indication of the extent of computer use in this country, it has been estimated that in 1978 about 350,000 small business computer systems were installed.[8]

Because computers are becoming an integral part of our lives, attorneys should understand how they work and be able to address the legal problems created by computer use. As advisors, negotiators, and defenders, attorneys may become involved in the following: negotiation and drafting of contracts for the purchase or lease of computer systems; taxation problems involving computers; prosecution or defense of those charged with crimes involving computers; invasions of privacy through computer use; procurement of patent, copyright, and trade secret protection for computers, computer programs, and computer goods and services; and problems of introducing computerized business records into evidence in judicial proceedings.[9] This article is written for the attorney with little background in the area of computers who may be called upon for advice on a computer-related matter. Without some familiarity with computers and the law relating to them, an attorney may be unable to prevent, resolve, understand, or even recognize a computer-related legal problem.

## I. COMPUTER CONTRACTING

When a client is contemplating the purchase or lease of a computer system, his attorney may either draft the contract or review a contract drafted by another. At present, however, contracting expertise in the data processing field is inadequate.[10] The major problem in ne-

[8] McCartney, *Small Business Systems: They're Everywhere*, 24 DATAMATION 91 (Oct. 1978). Pharmacies and insurance brokerage offices are suggested as likely candidates for small business computers. *Id.*

[9] It is acknowledged that computer-related problems occur in other areas, such as international computer law, banking, and data communications, and that the discussion of selected topics could be expanded. Such expansion, however, would prevent this article from achieving its purpose, which is to provide a non-technically oriented attorney with a *brief* background in computer law sufficient to enable the attorney to recognize problems that otherwise may go unnoticed. Readers seeking a more in-depth discussion are referred to sources cited in this article.

[10] The consensus at a recent Computer Law Association convention was that "[c]omputer contract litigation should be a booming [business] for years to come, considering the sorry state of existing [data processing] contracting procedures." Computerworld, Nov. 6, 1978, at 9, col. 1. The Computer Law Association is a national organization, the membership of which is composed of lawyers, data processors, and others interested in computer law.

Sources that discuss the negotiation and drafting of data processing contracts include R. BERNACCHI & G. LARSEN, DATA PROCESSING CONTRACTS AND THE LAW (1974) [hereinafter cited as BERNACCHI]; D. BRANDON & S. SEGELSTEIN, DATA PROCESSING CONTRACTS (1976) [hereinafter cited as BRANDON & SEGELSTEIN]; Bigelow, *Computer Contract Check-*

gotiating for computer services is the failure of the user to specify his needs,[11] particularly the computer output he desires. Perhaps this is caused by the belief that the computer company is familiar with other businesses and knows what a user's needs are. This assumption, however, may not be justified. The user should specify his needs exactly to ensure that an unwanted product is not delivered. These specifications should become a part of the contract.

The contract for the purchase or lease of the computer hardware[12] should set out not only the general description of the hardware, but also the detailed specifications.[13] The greater the detail of these specifications, the less likely it is that a dispute will arise as to what is to be delivered. For example, there is little margin for misunderstanding if the specifications for a line printer include the number of characters per line and the number of lines to be printed per page.

The purchaser or lessee must get information from the computer company about site requirements,[14] including electrical power, cabling, fire protection equipment, air conditioning, and floor load limits. The contract must specify who has the responsibility for site preparation and when that preparation must be done.

Both the hardware and the software[15] must be delivered. There

*list*, in R. BIGELOW & S. NYCUM, YOUR COMPUTER AND THE LAW 213-31 app. H (1975) [hereinafter cited as *Checklist*]; COMPUTER L. SERV. (R. Bigelow ed. 1972) (a multi-volume set containing many items of interest, including sample contracts, cases, and articles in the computer law area).

[11] Computerworld, Nov. 6, 1978, at 9, col. 1.

[12] "Hardware" is defined as "the physical equipment such as the mechanical, magnetic, electrical and electronic devices from which a computer is fabricated, the material forming a computer, as distinct from the [programs]." MEEK, *supra* note 2, at 103. Usually the hardware is thought of as including the computer and various peripheral equipment hooked up to the computer and used for input, output, and storage of data. The peripheral equipment includes tape drives, disc drives, memory extensions, printers, card readers, and remote terminals such as typewriters or cathode ray tubes. *See* BERNACCHI, *supra* note 10, at 217.

[13] *See Checklist*, § 3.1.a, *supra* note 10, at 215.

[14] BRANDON & SEGELSTEIN, *supra* note 10, at 102; *Checklist*, § 4, *supra* note 10, at 217-18.

[15] Here, the reader should become familiar with two definitions: "program" and "software." A program is a "complete set of instructions directing a computer to perform a data processing task. The term implies an extended sequence incorporating all of the detailed steps and procedures required to complete a job." MEEK, *supra* note 2, at 176. Software has been briefly defined as "[t]he collection of all programs for a computer." *Id.* at 210. However, the word has no generally accepted meaning within the data processing industry. Software may include a listing of computer program instructions that can be read by a human; it may include those same computer instructions translated into machine readable form and now residing on some storage media such as magnetic tape; it may include those same computer instructions after they have been "read into" the computer; and it may include human readable documentation which describes the capabilities of the computer pro-

will be several types of hardware, such as the computer, the printer, and the remote terminals. The system may be functionally useless, however, until the software is also delivered. Because failure of timely delivery has been a major problem in the data processing industry,[16] contract remedies for late delivery must be given careful attention.

Once the hardware and software are delivered, there must be acceptance of the system. The contract should be written so that the user need not accept it unless the hardware works as specified in the hardware components manual,[17] the computer programs work in accordance with their specifications, and the system operates in accordance with an agreed standard of reliability.[18] Even after acceptance, however, if the system does not perform properly, the purchaser or lessee may have a cause of action for breach of specific contract terms or misrepresentation during negotiations.[19]

After the computer system is installed, emergency and periodic maintenance of the hardware must be performed either by the manu-

gram. Software also may be used to describe data to be processed by the computer. Such data may be customer lists, student grades, or some other set of information. As with computer programs, this data may be represented in human or machine readable form, and either form may be considered software. *See* D. BENDER, COMPUTER LAW: EVIDENCE AND PROCEDURE § 2.06 (1978) [hereinafter cited as BENDER].

[16] BERNACCHI, *supra* note 10, at 124.

[17] BRANDON & SEGELSTEIN, *supra* note 10, at 94.

[18] *Checklist*, § 6.3.c, *supra* note 10, at 220. For example, new equipment should run for 30 consecutive days with no more than five percent "downtime." Downtime generally is defined as equipment failure that prevents use of the computer. BERNACCHI, *supra* note 10, at 658. To have a basis for deciding whether to accept the entire delivered system, the user should prepare test data with known results. *Checklist* § 6.3.c., *supra* note 10, at 220. The test data could then be input to the computer, and the output could be compared with the known results. If the computer generated incorrect results, the computer company should be allowed a period of time within which to make corrections. After the correction period, the test data would be run again. A breach could be declared if the output were again incorrect. BRANDON & SEGELSTEIN, *supra* note 10, at 94.

[19] *See, e.g.*, Clements Auto Co. v. Service Bureau Corp., 444 F.2d 169 (8th Cir. 1971), in which a user of data processing services recovered damages from a supplier for misrepresentations made by the supplier during negotiations as to the efficiency and effectiveness of the services provided. Recovery was permitted under Minnesota law even though the contract disclaimed the supplier's responsibility for statements not occurring in the contract. Unlike many states, Minnesota permits recovery for innocent misrepresentation. *Id.* at 176-79. Readers are cautioned that many states have a scienter requirement. *Id.* at 179. *See also* Applied Data Processing, Inc. v. Burroughs Corp., 394 F. Supp. 504 (D. Conn. 1975), in which the lessee of data processing equipment recovered general damages against the lessor of the equipment on grounds of breach of warranty. Because there was a lease clause providing that the lessor would not be liable for consequential damages, and because the consequential damages flowed from misrepresentations made by the lessor during negotiations which were not included in the contract, the court held that the lessee could not recover consequential damages on a breach of warranty cause of action. The court, however, permitted these damages under the cause of action for tortious misrepresentation. *Id.* at 508-11.

facturer or by an independent maintenance company. If the maintenance is to be done by the manufacturer, it may be part of a comprehensive contract. If the maintenance is to be performed by another company, a separate maintenance contract is required. Maintenance provisions for prompt and effective maintenance as well as remedies for failure to provide such maintenance and for continuing failures of the hardware are necessary.[20] The contract may provide for "fixed price" maintenance, which is in essence an insurance policy for maintenance and probably for replacement parts as well. This is a secure method, but expensive. The alternative type of maintenance contract may require payment for time and materials, and is expensive if the equipment malfunctions frequently.

Hardware maintenance contract considerations other than cost may be important. For example, because the computer system may become totally inoperative, it is important that the emergency maintenance be done promptly. Thus, response time is a key contract factor. It is useful to negotiate a maximum time for response and to provide for some type of compensation[21] if the response time is not met. Another important maintenance consideration is access to the computer system. In negotiating this item, the user should attempt to contract for the preventive maintenance to be performed during the firm's nonwork hours in order to prevent disruption of use of the computer.

Considerations for maintenance of the software are similar to those for the hardware. The vendor should guarantee that the computer programs will work according to specification for a set period of time. Any corrections necessary during this period should be guaranteed to be made at no charge. After the guarantee period, of course, there can be service charges[22] pursuant to a separate maintenance agreement or clause. The user should secure a contractual commitment that software errors will be corrected within a specified time. A liquidated damages provision may be drafted as a remedy if the errors are not corrected promptly.[23]

Remedies are a key aspect of any contract. In the data processing area it is important that the contract remedy fit the breach. For example, if the computer system is delivered late, liquidated damages may

[20] BRANDON & SEGELSTEIN, *supra* note 10, at 95.

[21] One example is reduced maintenance costs. *Id.* at 96.

[22] Note that this may occur even though the program error existed prior to the expiration of the guarantee period, if the error is unfortunately not discovered until after the period expires. Most computer programming firms, as a gesture of goodwill, do not charge to correct latent errors discovered after the expiration of the warranty period.

[23] *See* R. FREED, COMPUTERS AND LAW 223, cl. 9.a (1976).

be more appropriate than termination because it may take many months to obtain delivery of another system. Once the computer system is installed, the user may be more interested in having the vendor supply a back-up computer facility than receiving money damages.[24]

The purchaser or lessee of data processing services may wish to hire a consultant to assist in acquiring the services.[25] While a contract between the hirer and the consultant should be considered, circumstances may not justify a formal contract. For example, the hirer may be dealing with an extremely reliable consultant who will provide only a few hours of service for a fee. The time and expense of a detailed contract are not required in this instance. If, however, a formal contract is desired, there are some factors that should be considered. For example, the contract should specify the consultant's tasks in order to avoid unnecessary charges and to provide for the needed services. The contract should specify the number of days, weeks, or months the consultant's services are to be provided. The hirer should have an option for early termination of unsatisfactory consultant services. In addition, there should be an option to extend the services if necessary. It should be determined whether the consultant's fees increase for work done on weekends or holidays. The hirer may wish to specify the maximum charge in order to avoid the possibility of the consultant's taking advantage of an open-ended consulting agreement.

In helping to implement the system, the consultant may learn confidential information about the hirer's clients or about other aspects of the hirer's business. The contract should mention the confidential nature of the information and require that the consultant use such information *only* in fulfillment of the consulting project.

A final point regarding consultants is the evaluation of their services. Unfortunately, there are few guidelines to determine malpractice by a data processing consultant. The hirer must monitor the work of the consultant and determine whether the work is proceeding in a professional manner. Scheduled meetings with the consultant at which the consultant gives progress reports may be useful.

## II. State and Local Taxation of Computer Goods and Services

The following discussion deals with state and local taxation

[24] *See* Brandon & Segelstein, *supra* note 10, at 93, 260 (examples of contract clauses on the availability of backup facilities).

[25] *See generally* Bernacchi, *supra* note 10, at 455-62.

problems[26] and concentrates on three areas: the classification of computer software as "tangible" or "intangible," the classification of computer programs according to the exact function they perform, and the taxation of goods and services provided by computer service bureaus.

### *A. Taxing Computer Software: Is It To Be Taxed as Tangible or Intangible?*

In the area of taxation, one question that courts have recently addressed is whether software should be treated as tangible or intangible property. This classification is often a crucial factor when determining whether a transaction that involves software is taxable. In the cases discussed below, the courts found the software to be intangible property.

In *District of Columbia v. Universal Computer Associates, Inc.*,[27] Universal purchased a computer (the hardware) and punched cards (the computer programs) from IBM. Local laws subjected tangible personal property, but not intangible property, to a personal property tax.[28] The court held that the punched cards (programs) were intangible and should not be subject to the tax on tangible personal property. It noted that the punched cards themselves were of little value and that the consideration had been paid for the intangible information contained on the cards.[29]

[26] Federal income tax questions involve both hardware and software and raise problems in the area of investment credits, capitalization versus expense, and depreciation. For a list of articles on federal taxation of computers, see 1 COMPUTER L.J. 611, 658-59 (1979). *See also* Bigelow, *Federal Software Taxation*, [1972-1979 Transfer Binder] 1 COMPUTER L. SERV. § 2-3.2 (R. Bigelow ed.); Computer Taxation at the Federal Level—Update: 1979, Presentation by Michael W. Berwind to the 1979 Computer Law Association Conference in Washington, D.C. (March 5, 1979).

[27] 465 F.2d 615 (D.C. Cir. 1972).

[28] *Id.* at 617.

[29] *Id.* The court compared computer software to the cartoon mats involved in Washington Times-Herald v. District of Columbia, 213 F.2d 23 (D.C. Cir. 1954), in which the cartoon mats sold by publishing syndicates to individual newspapers were held not to be tangible personal property for sales tax purposes. This was because the mats from which the cartoons could be reproduced had inconsequential value, and the newspapers had really bought the right to reproduce the creations of the artists who made the drawings. *Id.* at 24. The court in *Universal Computer* found that the knowledge stored on the computer cards was more demonstrably intangible property, in the sense of being the result of individual intellectual efforts, than the right to reproduce the cartoonists' drawings in *Washington Times-Herald.* 465 F.2d at 618.

In *Universal Computer*, the court faced another common computer tax problem, that of "unbundling." The hardware and software had been "bundled" together and sold for about $290,000; but only the hardware was subject to the personal property tax. The court unbundled the sale to determine the value of the hardware. After making some mathematical calculations, explaining the uncertainty involved, and describing the contradictory evidence

Although *Universal Computer* involved personal property taxes, the same problem of determining if software is tangible or intangible occurs with sales and use taxes. *Commerce Union Bank v. Tidwell*[30] involved the question of whether computer software is tangible personal property for sales tax purposes. The court defined tangible personal property as that " 'which may be seen, weighed, measured, felt, or touched, or is in any other manner perceptible to the senses,' "[31] and held that computer software is not tangible personal property and therefore is not subject to the sales tax.[32] The court found that magnetic tapes and punched cards are not a crucial element of software because the information could be transmitted by telephone lines without any tangible manifestation of transmission.[33] Therefore, the court reasoned, the transfer of any tangible personal property was incidental to the purchase of the intangibles stored on tape, and the sale of computer software did not constitute the sale of tangible personal property under the applicable state statute.[34] In *State v. Central Computer Services, Inc.*,[35] the Alabama Supreme Court had to decide whether computer software constitutes tangible personal property for purposes of the state use tax. The reasoning of the majority paralleled that of the courts in *Universal Computer* and *Commerce Union Bank*, and it concluded that computer software is intangible property.[36]

regarding the value of hardware and software, the court found that a fifty-fifty split was reasonable, saying that "[w]ith a different set of facts, King Solomon did no better in making a similar choice." *Id.* at 619-20 (citing I *Kings* 3:16-28).

[30] 538 S.W.2d 405 (Tenn. Sup. Ct. 1976).

[31] *Id.* at 406 (quoting TENN. CODE ANN. § 67-3002(1) (1976)).

[32] The court said:

> What is created and sold here is information, and the magnetic tapes which contain this information are only a method of transmitting these intellectual creations from the originator to the user. It is merely incidental that these intangibles are transmitted by way of a tangible reel of tape that is not even retained by the user.

538 S.W.2d at 407.

[33] *Id.* at 407-08.

[34] *Id.* at 408. In 1977, Tennessee enacted legislation to impose sales tax on certain types of computer programs. This was repealed in 1978, leaving *Commerce Union Bank* as the law in Tennessee in the area of sales tax on computer programs. COMPUTER L. & TAX REP., May 1978, at 7; COMPUTER L. & TAX REP., Mar. 1978, at 7; COMPUTER L. & TAX REP., Feb. 1978, at 5-6.

[35] 349 So. 2d 1160 (Ala. Sup. Ct. 1977).

[36] The court compared computer software to movies and discussed Boswell v. Paramount Telev. Sales, Inc., 282 So. 2d 892 (Ala. Sup. Ct. 1973), in which it was held that the leasing of movie films and tapes by Paramount to television stations in Alabama involved the leasing of tangible personal property rather than an intangible right to publish. 349 So. 2d at 1162. However, the court in *Central Computer* distinguished the use of computer software from the use of movies by noting that the physical presence of the movie film is essential to broadcasting the movie, while the physical presence of magnetic tape or punched

### B. *Taxing Computer Software: Is It To Be Taxed Based on Its Function?*

California has enacted legislation specifically dealing with personal property taxation of computer programs.[37] Thus, in California it is not necessary to determine whether the programs are tangible or intangible. Essentially, California's personal property tax is levied on the basic operational programs,[38] and there is no tax on the other programs.[39] Thus, California's approach for personal property tax determinations is to categorize, not according to what is "tangible" or "intangible," but rather according to the function of the programs.[40]

### C. *Sales Tax on Goods and Services Provided by Service Bureaus*

A final area of interest involves the taxation of goods and services provided by service bureaus.[41] *Accountants Computer Services, Inc. v. Kosydar*,[42] an Ohio case, provides a good discussion of the issues in-

cards is not essential to the transmittal of the computer programs. As an example, the court said that the programs can be transmitted to the computer by telephone. *Id.*

The dissent responded to this argument by stating that films can also be transmitted by telephone lines or radio waves, or the actors could make a personal appearance. The film still has value, however, because of what it contains and therefore is considered tangible. Similarly, the computer cards and tapes have value because of their contents. Also, in *Boswell*, hardware was used to get information from the film, just as hardware is used to get information from the computer cards or tapes. *Id.* at 1164-65 (Maddox, J., dissenting). The dissent's point seems to be that if the computer programs were transmitted by telephone lines, there would be no use tax because nothing tangible was transmitted. But because the medium chosen for transmittal was tangible, the use tax applies. In essence, the dissent's argument would exalt form over substance.

[37] CAL. REV. & TAX CODE §§ 995-995.2 (West Supp. 1979).

[38] The functions of basic operational programs are:

> operation of a computer by managing the allocation of all system resources, including the central processing unit, main storage, input/output devices and processing programs. A processing program is used to develop and implement the specific applications which the computer is to perform. Its operation is possible only through the facilities provided by the . . . [basic operational] program; however, it is not in itself fundamental and necessary to the functioning of a computer.

*Id.* § 995.2. The California code uses the phrase "processing program" similarly to the way others use the term "application program." Application programs are designed to carry out specific tasks for the user of the computer, such as bookkeeping, billing, and statistical analysis. *See* BERNACCHI, *supra* note 10, at 280-82.

[39] CAL. REV. & TAX CODE §§ 995, 995.2 (West Supp. 1979). Other programs include: (1) application programs (defined in note 38 *supra*), (2) programs allowing the user to write a computer program in one computer language and have it translated to another, and (3) several other programs not necessary to this discussion. *Id.* § 995.2.

[40] *Id.* §§ 995, 995.2.

[41] Service bureaus are businesses that provide data processing services for others. *See* BERNACCHI, *supra* note 10, at 380.

[42] 298 N.E.2d 519 (Ohio Sup. Ct. 1973).

volved by considering three separate fact situations. In all three, the issue was whether the transfer of personal property would be exempt from taxation because the real purpose of the transaction was the purchase of services, and the personal property was transferred only as an inconsequential element of the transaction. The problem exists because most transactions involve both personal services and the transfer of some tangible personal property.

The court said that the real objective of the buyer is the critical factor in determining whether the sales tax would apply. If what is sought is service, the sales tax does not apply. If the objective is obtaining tangible personal property, however, the tax applies to the entire gross receipts without deduction for work, labor, skill, thought, time, or other expense of producing the property.[43]

The court listed three possibilities regarding mixed sales of services and property:

> 1. The service is the main item sold and the property sold is incidental thereto and not separately charged (not a taxable sale as a sale of services).
>
> 2. The services and property sold can be readily separated (one tax exempt and the other taxable).
>
> 3. The service sold is incidental to the property and not separately charged (taxable in gross).[44]

The court then applied these three standards to the situations before it. In the first situation, the service bureau (taxpayer) received raw material from its customer and transcribed it onto key punched cards. The cards were then fed into a data processing machine to be sorted, classified, and rearranged. The printout was delivered to the customer who studied, altered, analyzed, and adjusted the data. Thus, the object of the transaction was to produce the rearranged raw material, the "writeup work." The limited personal service was an inconsequential element of the object that was sought and purchased. Therefore, the entire transaction was taxable, under the sales tax, with no allowance for the insignificant personal service rendered.[45]

In the second situation, the service bureau obtained information from its client for analysis of business problems. The service bureau's

[43] *Id.* at 526. The court did not specifically describe how to determine the true object sought by the purchaser. In its examination of the three situations before it, the court suggested that one can readily determine whether a purchaser seeks services or tangible property by examining the facts. *Id.* at 527-28.

[44] *Id.* at 526 (quoting Goodyear Aircraft Corp. v. Arizona State Tax Comm'n, 402 P.2d 423, 427 (Ariz. Ct. App. 1965)).

[45] *Id.* at 527-28.

employees analyzed the client's present system. The data processing machines and their printouts were used to assist the service bureau in sorting work to allow its personnel to solve the client's problems. The printed matter was valuable because it was the result of personal service efforts by the service bureau personnel. Thus, the tangible property (*i.e.*, the printed paper) was an inconsequential element for which no separate charge was made. The contents of the paper represented personal services, that is, analysis of the client's problems, and, therefore, no tax was imposed on this analysis.[46]

The third situation before the court did not involve a data processing service bureau, but the facts nevertheless seem applicable to the problem of applying a sales tax to output from a service bureau. In this instance, a market research firm was to compile and interpret statistical data in order to determine marketing information. It was also to analyze, interpret, and present to the customer the statistical information and assist the customer in management and marketing decisions based on the data. The court concluded that the intellectual and manual efforts of the employees of the marketing research firm were what was purchased, and not the inconsequential tangible personal property that was transferred. Thus, there was no taxation of any portion of the consideration paid.[47]

## III. CRIMINAL LAW

In the area of criminal law, it is important for attorneys to understand the workings of computers in order to assist a company with a computer to anticipate the types of crimes that might be committed and to take steps to prevent these crimes. It is also important for the prosecutor to understand exactly how the crime was committed so that he can determine whether state or federal law was violated and choose the correct forum for prosecution, decide exactly which section of the criminal code encompasses the behavior sought to be prosecuted,[48] and de-

[46] *Id.* at 528.

[47] *Id.* It should be noted that in 1978, Ohio revised its tax code so that the transfer of the results of electronic data processing of another's data is deemed to be a service and not taxable under the tax code. OHIO REV. CODE ANN. § 5739.01(B) (Page Supp. 1978). The analysis in the *Accountants Computer Services* case is useful in construing other tax codes that do not refer specifically to electronic data processing.

[48] Charging the correct crime can be a major problem. Because criminal codes rarely are written with computer crime in mind, the prosecutor often must attempt to fit a computer crime into a category when the fit might not be comfortable. For example, if software is misappropriated using a remote terminal, the prosecution, depending on state law, may take any of several forms, *e.g.*, misappropriation of trade secrets, larceny, telephone abuse, and forgery. *See* Nycum, *The Criminal Law Aspects of Computer Abuse*, RUTGERS J. OF

cide how to investigate the alleged crime.

Experts believe that computer crime is almost impossible to detect and that it costs the public at least $10 billion annually.[49] Computers are heavily used in banking, credit transactions, payroll, inventory, trading of securities, maintenance of tax and health records, and in various other kinds of information processing. None of these areas of computer processing appears to be safe from criminal infiltration.

Five categories of common computer crime are financial crimes, property crimes, information crimes, theft of services, and vandalism.[50] Financial crimes usually involve the taking of money or negotiable instruments and are executed in systems in which the computer is used for payroll, accounts payable and receivable, and various financial records.[51] In an ingenious crime, an individual in Washington, D.C., opened a bank account. He received checks and deposit slips, both bearing his name at the top and his magnetically coded computer-readable account number at the bottom. He took a stock of blank deposit slips which the bank had made available for depositors who had forgotten their deposit slips. He then had printed his account number in magnetic ink at the bottom of these blank deposit slips and placed them back into the bank's tray. Unwary depositors used the slips to make deposits. The deposit slips were fed into the bank's computer system for sorting. Slips with no magnetic coding were sorted out of the sys-

COMPUTERS AND THE L. 271, 276-91 (1976). Fortunately, some states have legislation specifically describing computer crime. *See, e.g.*, CAL. PENAL CODE § 502 (West 1980); FLA. STAT. ANN. § 815.01-.07 (West Supp. 1979).

[49] L.A. Times, Jan. 6, 1980, Part I, at 4, col. 1. *See also* Bequai, *Computer Crime: A Growing and Serious Problem*, 6 POLICE L.Q. 22, 23 (1976) [hereinafter cited as Bequai].

[50] Bequai, *supra* note 49, at 23.

[51] *Id.* In one well-publicized incident, a computer expert, Stanley M. Rifkin, followed through with a remarkable plan. L.A. Times, Oct. 5, 1979, Part I, at 16, col. 1. "Rifkin, a computer expert, illegally used Security Pacific's inter-bank funds wire to transfer $10.2 million to . . . [another] bank." Santa Monica Evening Outlook, Oct. 5, 1979, at A-5, col. 3. The following account of the crime was relayed by Kathy Stoltz, an Assistant United States Attorney, who was chief prosecutor in the Rifkin case. She recalled that prior to the time of the crime, Rifkin was an independent contractor doing computer work at Security Pacific Bank in Los Angeles. His job was completed, but because of the trust relationship he had built at the bank, he was able to get access to the wire transfer room. In the wire room he learned an identification number. Posing as a bank officer, he then telephoned Security Pacific Bank in Los Angeles and ordered a $10.2 million wire transfer, through a New York bank, to the Swiss bank account of a Russian diamond company. In this way he was able to purchase diamonds from the diamond company. Security Pacific Bank personnel made a computer entry to effect the transfer, but Rifkin did not have any interaction with the computer. Telephone Interview with Kathy Stoltz, Asst. U.S. Atty., in Los Angeles, Calif. (Oct. 15, 1979). Perhaps Rifkin's crime should be labeled a "telephone crime" rather than a "computer crime."

tem by machine and processed manually. Those having magnetic coding were routed for deposit into the account represented by the magnetic code. Thus, the deposits of bank customers using these altered deposit slips were directed to the criminal's account. By the time customers began to complain that their deposits were not being credited to their accounts, the criminal had withdrawn $100,000 from his account and disappeared.[52]

Property crimes involve the taking of merchandise or other property, either for personal use or for sale. In an instance of such conduct, a college engineering student who periodically rummaged through the telephone company's trash cans looking for computer information discovered a set of computer system instructions for the company's equipment ordering system. Using a touch-tone telephone and the system instructions, the student placed orders for various products with the company's computer. From the material he had found in the trash, he knew that the company allowed for a certain amount of loss in deliveries. Thus, he was able to keep his orders within the loss allowance and avoid detection. It is estimated that he stole more than one million dollars of equipment by the time he was caught.[53]

Information crimes encompass those in which a criminal gains access to a computer and gets valuable information from it, often for sale to others. For example, three computer operators for Encyclopaedia Britannica allegedly extracted from a computer a customer list valued at one million dollars and then sold it.[54] In another scheme involving theft of information, a computer operator for the Illinois Driver Registration Bureau was bribed to steal a computer tape reel containing drivers' names and addresses. These had a direct mail value of $70,000. The stolen list was put to commercial use by outsiders.[55] A variation of the information crime involves the addition of unauthorized information to a computer list. In one such instance, employees of the New York Department of Motor Vehicles were charged with accepting bribes to add names to the computer's list of approved applicants for

[52] Whiteside, *Annals of Crime: Dead Souls in the Computer*, NEW YORKER, Aug. 22, 1977, at 35 & 50 [hereinafter cited as Whiteside].

[53] Bequai, *supra* note 49, at 23; Whiteside, *supra* note 52, at 55-56. Perhaps this was a situation when crime did pay because after some plea bargaining, the student was sentenced to 60 days at a prison farm. With time off for good behavior, he served only 40 days. Furthermore, he settled a $250,000 civil suit brought against him by the telephone company for $8,500. He then went into business serving as a consultant to various businesses in computer crime prevention. Whiteside, *supra* note 52, at 56.

[54] Bequai, *supra* note 49, at 23-24; Whiteside, *supra* note 52, at 60.

[55] Whiteside, *supra* note 52, at 60.

drivers' licenses. The names belonged mostly to non-English speaking immigrants who had never taken the required eye, written, and driving examinations.[56]

Theft of services involves unauthorized use of the computer. For example, one bookmaker gained access to a university computer to make his betting calculations.[57] In another instance, an employee was discovered to have used a company computer for his own business.[58] Inasmuch as the computer may be sitting unused, it may be thought that there is no monetary loss to the company from unauthorized access. However, the loss in the rental value of computer time must be considered. In one instance, a computer service organization rented out computer time. One of its former employees gained access by telephone to the service organization's computers in order to benefit his current employer. One hundred forty-three hours of computer time, with a rental value of $15,000, were used in this scheme.[59]

Vandalism is a serious crime involving intentional damage to the computer or equipment.[60] For example, a computer-tape librarian, fired because her love affairs with two data processors caused turmoil at the company, erased or mislabeled enough computer tapes before she left to cost the company $10 million to recreate the destroyed data.[61] Computers have also been the targets of physical attacks, apparently because people view them as an electronic destroyer of personal identity, or as otherwise representing an unwanted system.[62] For example, it is suspected that groups opposed to the Vietnam War were responsible for bombing computer centers at universities reported to be engaged in Defense Department research.[63]

In addition to the categorization of the types of computer crime, it is worthwhile to outline the five phases of computer operation during which a criminal can intervene in the process. The five common phases of operation are: (1) input, (2) programming, (3) processing in the central processing unit, (4) output, and (5) communication of data.[64] During the input phase, the criminal might place false data into the

[56] *Id.*

[57] *Id.*

[58] Bequai, *supra* note 49, at 24.

[59] Whiteside, *supra* note 52, at 60.

[60] Bequai, *supra* note 49, at 24.

[61] Whiteside, *supra* note 52, at 63.

[62] *Id.* at 36.

[63] In particular, one should note the events that occurred in 1970 at the University of Wisconsin and at Fresno State College in California. *Id.*

[64] Bequai, *supra* note 49, at 24-26.

computer. In one instance, an officer of a manufacturing firm inserted into the computer false data creating phony suppliers and truckers. About one million dollars in checks were issued to these accounts and pocketed by the officer and several cohorts.[65] Also, computer programmers have been known to alter payroll input data in order to give certain employees unauthorized pay raises.[66] As another example, a computer specialist employed by the Australian Taxation Commission was reported to have sold highly confidential information about how the Commission's computerized system checked on the legitimacy of taxpayers' claims for deductions. Using the information, taxpayers were able to exaggerate claims for tax deductions.[67]

In the programming stage, the criminal can program the computer to operate in a manner consistent with his scheme. For example, two programmers employed at a large New York company programmed the company's computer to increase by two cents the amount withheld from other employees' paychecks for federal taxes. They also programmed the computer to add two cents per employee to their own federal withholding accounts. At the end of the year, they received the money in the form of refund checks from the Internal Revenue Service.[68] In another programming scheme, a computer programmer for a mail-order sales company instructed the computer to subtract a few cents from commissions that were to be added to the company's sales-commission accounts and add the money to a dummy sales commission account he had established for himself under the name Zwana. He knew that the company's computer processed accounts in alphabetical order and he programmed the computer to transfer the excess pennies to the last account. By accident he was caught when the first and last sales-commission accounts were selected as a public relations promotion for ceremonial treatment.[69]

Serving as the computer's memory bank, the central processing unit is vulnerable to attack by criminals. An incident of infiltration of a central processing unit involved two competing computer-service companies. An employee of one of the companies decided to raid the memory of the competitor's computer in order to obtain a listing of a computer program that had been developed by the second company. The employee used a terminal connected to a telephone and some code

[65] *Id.* at 25.

[66] Whiteside, *supra* note 52, at 60-61.

[67] *Id.* at 60.

[68] *Id.* at 54.

[69] *Id.*

words, which he learned when he visited a firm that was a customer of the competing computer company. He was able to infiltrate the competitor's computer and have it print out, on his employer's computer, a listing of the instructions for the desired computer program.[70]

Another method of obtaining listings of computer programs is to take already printed programs. In *Hancock v. Texas*,[71] a defendant's felony conviction for the theft of fifty-nine computer programs from his employer was affirmed. In defense to the charges, he contended that the computer programs were not corporeal property and not the possible subject of theft. The court rejected this argument, quite possibly because of evidence that the programs had a market value of approximately two and a half million dollars.[72]

During the output phase, data are transmitted to the user. These data may be provided by the criminal to unauthorized sources. Mailing lists, customer lists, and confidential marketing data are generated at this output stage and may be illegally sold to competitors. For example, a computer service company in California had access to computer tapes containing lists of registered voters. In a civil suit brought by the state, the service bureau was accused of using the tapes for commercial purposes. The suit was settled out of court.[73] In another scheme, a computer operator instructed the computer to print out extra payroll checks. The checks were made payable to various employees but were taken by the computer operator. He forged the employees' signatures and cashed the checks by endorsing them. To avoid detection, the computer operator spread out the duplicate checks among many employees, hoping that this would minimize the risk that the employees might notice the increase in earnings in their year-end statements of earnings.[74]

Criminal intrusion during communication of data over telephone lines can make the outsider privy to the information transmitted. In one instance, a major oil company was bidding on drilling rights in Alaska. The oil company used a terminal in Alaska to send informa-

[70] *Id.* at 58-59. In another example, an electronics enthusiast, who found a computer password, used it to infiltrate a computer in order to play computer games. *Id.* at 60.

[71] 402 S.W.2d 906 (Tex. Ct. Crim. App. 1966).

[72] *Id.* at 909-11. In the subsequent petition for federal habeas corpus relief, the defendant contended that he had been unlawfully convicted of felony theft because the corporeal personal property that he was accused of stealing did not have a value in excess of $50, but was instead only $35 worth of paper. The federal court of appeals held that the law as authoritatively construed by the Texas court was not so unreasonable or arbitrary as to be violative of federal due process. Hancock v. Decker, 379 F.2d 552, 553 (5th Cir. 1967).

[73] Whiteside, *supra* note 52, at 61.

[74] Bequai, *supra* note 49, at 26.

tion by telephone lines to a computer thousands of miles away. Financial analysis based on the information was transmitted back to the terminal in Alaska. It was discovered that a competitor had tapped into the oil company's communication lines and used the information to underbid the oil company for the drilling rights.[75]

Very few computer crime cases are reported in court opinions.[76] One reported case, *United States v. Jones*,[77] addressed the issue of whether alteration of accounts payable documents fed into a computer, resulting in the issuance of checks payable to an improper payee, constituted forgery. If it had been forgery, the indictment should have been dismissed because forgery was specifically excluded from coverage in the code sections on which the indictment was based.[78] The case involved the issuance of five checks to "A.L.E. Jones" that should have been issued to Whirlpool Corporation. The defendant had altered the accounts payable material, which was input to the computer, so that the checks were made payable to "A.L.E. Jones." The defendant was charged with transporting in interstate or foreign commerce securities valued at more than $5,000, knowing the securities to have been stolen, converted, or taken by fraud, and selling or receiving these same securities knowing them to have been stolen, converted, or taken by fraud. The defendant moved to dismiss the indictment, contending that the securities involved were forgeries, and that forgery had specifically been excluded from coverage in the sections upon which the indictment was based. The court agreed that the sole issue was whether the defendant's alleged activity constituted forgery. The court said that under the common law a forgery is a writing "which falsely purports to be the writing of a person other than the actual maker."[79] In other words, forgery relates to genuineness of execution and not falsity of content.[80]

The district court was of the opinion that the defendant made a false writing because, in a practical sense, the defendant drafted the instruments, even though he employed the computer as an instrumentality to write the checks.[81] The appellate court disagreed, saying that the defendant's acts did not constitute the making of a false writing, but

[75] Whiteside, *supra* note 52, at 57-58.

[76] *See* [1972-1979 Transfer Binder] 6 COMPUTER L. SERV. §§ 5-6 (R. Bigelow ed.). Most of the computer crime cases, such as those discussed in Bequai, *supra* note 49, and Whiteside, *supra* note 52, are reported only in the newspaper.

[77] 553 F.2d 351 (4th Cir.), *cert. denied*, 431 U.S. 968 (1977).

[78] *Id.* at 352, 356.

[79] *Id.* at 354 (citing Greathouse v. United States, 170 F.2d 512, 514 (4th Cir. 1948)).

[80] *Id.* at 355.

[81] *Id.* A false writing is an essential element of the crime of forgery. *Id.* at 354-55.

rather amounted to the creation of a writing that was genuine in execution but false as to the statements in it.[82] The court explained that the accounting department was defrauded into issuing a check to Jones. Thus the check was a genuine instrument that contained a false statement as to the true creditor. Because the purported maker of the check did in fact issue the check, there was no forgery,[83] and because the checks did not fall within the statutory exclusion as forgeries, the order of the district court dismissing the indictment was reversed. Thus, *Jones* demonstrates that a prosecutor must understand the exact method by which the computer was used to perpetrate a crime so that he charges the correct crime.

## IV. Privacy

Computers are used in a variety of ways to collect and disseminate information regarding the personal, economic, and social status of individuals within our society.[84] The flow of information from computers poses a serious threat to the ability of individuals to maintain a significant degree of privacy in their lives.[85] There exist, however, three possible sources of protection for the right of privacy that may serve to limit the nature and extent of computer assisted invasions of privacy. While these protections overlap to a certain degree, they possess varied effectiveness in preventing the abuse of computer capabilities.

### *A. The Constitutional Right of Privacy*

The United States Supreme Court has recognized that a right of privacy is embodied in the Constitution.[86] In *Roe v. Wade*, the Court noted that though the Constitution does not explicitly mention any pri-

[82] *Id.* at 355.

[83] *Id.* at 355-56.

[84] Records are kept, for example, on medical services, health insurance, credit, family assistance, and education. *See* Bouvard & Bouvard, *Computerized Information and Effective Protection of Individual Rights*, 12 SOCIETY 62, 64 (Sept.-Oct. 1975) [hereinafter cited as Bouvard & Bouvard].

[85] Information in one computer can be cross-indexed with information contained in another computer, thus aggregating information about an individual. Because the information contained in the computers may be incomplete, the profile produced may be inaccurate. *Id.* at 63. The threat of this aggregation is made imminent through the use of "universal identifiers," such as social security numbers. *See generally* Bigelow, *Computer Privacy—A 1975 Status Report*, [1972-1979 Transfer Binder] 4 COMPUTER L. SERV. § 5-2, at 8-11 (R. Bigelow ed.). Computers can be used to invade privacy in a variety of ways; for example, computers can be used to make unwanted telephone solicitation. *See* PRIVACY J., Mar. 1978, at 2; PRIVACY J., Feb. 1978, at 7.

[86] Whalen v. Roe, 429 U.S. 589, 598-99 (1977); Roe v. Wade, 410 U.S. 113, 152 (1973); Katz v. United States, 389 U.S. 347, 350 (1967).

vacy right, "the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution."[87] This right of privacy is encompassed within the fourteenth amendment's guarantee of personal liberty.[88] By holding that the right of privacy is a fundamental right, the Court mandated that regulations interfering with these rights can be justified only if there is a compelling state interest.[89]

The Court further described the nature of the right of privacy in *Whalen v. Roe*.[90] The Court reasoned that there were two attributes to the right of privacy: (1) the right against disclosure of personal matters and (2) the right of an individual to make fundamental personal decisions free from governmental interference.[91] Invasions of privacy resulting from computer use relate primarily to the right against disclosure of personal matters.[92]

In *Whalen v. Roe*, the United States Supreme Court decided that the constitutional right to privacy did not prevent a state from using a computer to compile information on individuals obtaining medical prescriptions for certain drugs.[93] The State of New York justified the challenged statute on the basis that the state would otherwise be unable to prevent stolen prescriptions from being used, pharamacists from repeatedly refilling prescriptions, users from obtaining prescriptions from more than one doctor, and doctors from over-prescribing.[94] In part, the Act required the recording of patient information in a centralized computer file to assist in investigation of abuses.[95] Patients argued that the possibility that the information might become public, and thus adversely affect their reputations, made them reluctant to use the drugs.[96]

The Court found that the implementation procedures for the statute showed a proper concern for the individual's privacy.[97] In fact, the statute expressly prohibited public disclosure of the recorded informa-

[87] 410 U.S. 113, 152 (1973).

[88] *Id.* at 153. *See* Whalen v. Roe, 429 U.S. 589, 603-04 (1977). The fourteenth amendment provides that no state shall "deprive any person of life, liberty, or property, without due process of law." U.S. CONST. amend. XIV.

[89] Roe v. Wade, 410 U.S. 113, 155 (1973).

[90] 429 U.S. 589 (1977).

[91] *Id.* at 598-600.

[92] *See generally* Bouvard & Bouvard, *supra* note 84.

[93] 429 U.S. at 591.

[94] *Id.* at 592.

[95] *Id.* at 591-92, 597-98.

[96] *Id.* at 600.

[97] *Id.* at 593-94, 597-98, 600. The information was kept in a vault in a room which was surrounded by a locked wire fence and protected by an alarm system. *Id.* at 593-94.

tion.[98] The Court recognized the threat of privacy invasion created as a result of the computer's ability to store, retrieve, and disseminate vast amounts of information.[99] The Court found, however, that the operation of the statute did not violate the plaintiffs' right to privacy,[100] although the Court did indicate that there may exist situations in which the government's activities could violate the constitutionally protected right of privacy.[101]

The Court in *Whalen* was not presented with legislation that invaded privacy. Therefore, it is difficult to determine those factors essential to a finding of a computer aided invasion of privacy. From the Court's description of the nature of the right of privacy, it is clear that some sort of public disclosure, or a realistic threat of such disclosure, is necessary.[102] This disclosure requirement may significantly narrow the class of constitutionally actionable privacy invasions. Furthermore, such constitutional protection only exists against the government.[103] Legal protection against non-governmental computer privacy invasions must have its source outside the United States Constitution.[104]

### *B. Common Law Protection of Privacy*

Common law protections for the right of privacy have not been very effective at limiting computer assisted invasions of privacy. The ineffectiveness of common law protections is due largely to the historical developments of such protections in a pre-technological era. While a specific "right of privacy" did not exist at common law, various civil actions protected particular personal and property rights which roughly

[98] *Id.* at 605.

[99] *Id.* at 606.

[100] The Court held that the record supported a conclusion that some use of the medication had been discouraged by individuals' concerns for their privacy, but that thousands of prescriptions for the drugs had been filled each month, thus showing that the statute did not deprive patients of access to the drugs. *Id.* at 602-03.

[101] *Id.* at 605-06. The Court noted certain areas in which the government collects and uses personal information for public purposes, and that generally in those areas there is a statutory or regulatory duty to avoid unwarranted disclosures. The areas mentioned by the Court were tax collection, welfare and social security, public health, armed forces, and criminal law matters. *Id.* at 605.

[102] *See id.* at 600. It may be argued, however, that the mere collection of personal information by a governmental agency having no legitimate need for the information violates constitutionally protected privacy. *See id.* at 597-98.

[103] *See* U.S. CONST. amends. V & XIV.

[104] For example, California has, by its constitution, elevated privacy to an inalienable right. CAL. CONST. art. 1, § 1. This constitutional protection exists against acts by individuals, as well as by the government, and is aimed at curbing improper use of information that was properly obtained for a specific purpose. Porten v. University of San Francisco, 64 Cal. App. 3d 825, 829-30, 832, 134 Cal. Rptr. 839, 842-43 (1976).

correspond to modern privacy rights.[105] In an historic article, Samuel Warren and Louis Brandeis cogently argued for the consolidation of these discrete common law rights into a judicially cognizable right of privacy.[106] While Warren and Brandeis were clearly concerned about the effect that technological advances would have on the right of privacy,[107] their concept of privacy was defined in terms of the traditionally protected interests.[108]

The interests invaded by the relatively unsophisticated means of the pre-technological era were usually associated with a person's likeness or reputation. Information per se was not protected except as a copyright interest. The criteria that were developed to protect the common law notion of privacy, therefore, were not appropriate for preventing the more subtle invasions of privacy made possible by the development of computer technology.[109] The growing recognition of the common law right of privacy, however, preserves the possibility that the common law may one day serve as an effective source of protection from computer assisted invasions of privacy.[110]

One modern computer capability that threatens individual privacy is the use of customer and client lists by businesses. These lists are kept by magazines, credit card companies, and department stores. Specialized lists arranged by geographic area, age, income, or other variable can be generated quickly by computer and distributed to advertisers for use in direct mail advertising.[111] Such practices do not fall neatly within the ambit of common law protections of the right of privacy.

[105] Actions such as libel and slander protected an individual's "personality" to a limited extent, while actions for trespass, copyright, and assault protected person and property from direct invasion. However, there were some instances of protection afforded by the common law that were not limited by the traditional actions. *See* Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[106] *Id.* at 213. This article is generally regarded as the genesis of the right of privacy in America.

[107]
> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the "right to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the rooftops."

*Id.* at 195 (quoting T. COOLEY, LAW OF TORTS 29 (2d ed. 1888)).

[108] *Id.* at 200-04.

[109] *See* Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960). Dean Prosser indicates that no cause of action for public disclosure of private facts arises when a company supplies an individual's credit history to a potential employer or other small group. *Id.* at 393.

[110] *See* Annot., 14 A.L.R.2d 750 (1950).

[111] *See, e.g.*, PRIVACY J., Feb. 1978, at 1; PRIVACY J., Nov. 1978, at 2; PRIVACY J., Oct. 1979, at 4.

In *Shibley v. Time, Inc.*,[112] the plaintiffs brought an action against the publishers of Time, Esquire, Playboy, Ladies Home Journal, and the issuer of American Express credit cards. The plaintiffs argued that the sale of subscription lists constituted an invasion of privacy because the buyers of these lists may draw conclusions about the financial position, social habits, and general personality of the subscribers by virtue of their subscribing to certain publications. This information may then be used to determine the most effective types of advertising to be sent. The plaintiffs argued that this privacy invasion was not consented to at the time of the original subscription contract and that the defendants were unjustly enriched at the subscribers' expense.[113] The court, however, did not agree that any recognized right of privacy had been invaded:

> An actionable invasion of the right of privacy is the unwarranted appropriation or exploitation of one's personality, by the publicizing of one's private affairs with which the public has no legitimate concern, or the wrongful intrusion into one's private activities in such a manner as to outrage or cause mental suffering, shame or humiliation to a person of ordinary sensibilities.[114]

The court said that the plaintiffs recognized that their situation did not fall within the above situation but tried to bring defendants' behavior into the ambit of "appropriation of one's personality."[115] This argument was rejected because appropriation of one's personality refers to situations in which the plaintiff's name or likeness is displayed to the public to indicate that the plaintiff endorses the defendant's business or product.[116] The relative ineffectiveness of both the constitutional and common law protections against computer invasions of privacy has therefore created a need for legislative action to ensure that the individual right of privacy does not become an anachronism in the age of computer technology.

### *C. Right of Privacy by Statute*

Common law mechanisms safeguarding an individual's right of privacy have failed to serve as an effective means for limiting computer

[112] 341 N.E.2d 337 (Ohio Sup. Ct. 1975).

[113] *Id.* at 338.

[114] *Id.*

[115] *Id.* at 339.

[116] *Id.* (construing Housh v. Peth, 133 N.E.2d 340 (Ohio Sup. Ct. 1956)).

intrusions into private affairs. Legislatures have provided statutory protection, however, against computer aided privacy invasions.

Computers perform a critical function for the credit industry, providing potential creditors with financial and other pertinent information for the purpose of assessing credit risk. Given the role of computers in the credit industry and the concommitant potential for privacy invasions,[117] computer use must be regulated. There are three areas of regulation: (1) the subject matter permissible for regulation, (2) the means permissible for the accumulation of data, and (3) the appropriate dissemination of the accumulated data.

The California legislature has enacted the California Consumer Credit Reporting Agencies Act.[118] The legislative findings set forth in this statute[119] evince a substantial concern for the privacy of individuals. The legislature found that elaborate mechanisms had been developed to investigate and evaluate credit worthiness and reputations of consumers. They also discerned that credit reporting agencies play a vital role in compiling and evaluating credit and other information about consumers. Accordingly, the legislature determined that there was a need to insure that the credit reporting agencies are fair and impartial and respect consumers' privacy rights.[120] The legislature adopted this statute in order to guarantee the confidentiality, accuracy, relevancy, and proper use of the information collected.[121]

In order to achieve these goals, the legislature provided for the following: (1) mandatory disclosure to the consumer of the names of the recipients of the information;[122] (2) limitations on the subject matter of a credit report;[123] (3) prerequisites as to when a credit report may be furnished;[124] and (4) resolution of disputes concerning the content of the report.[125] To enforce compliance with the procedural requirements

[117] Privacy invasions by computers have a real potential for causing trouble. For example, credit investigation companies may employ inexperienced investigators who may compile misinformation that will end up in a computer data bank. *See, e.g.*, Santa Monica Evening Outlook, Oct. 31, 1977, Business Section, at 20, col. 2.

[118] CAL. CIV. CODE §§ 1785.1-1786.56 (West 1980). *See also* The Fair Credit Reporting Act, 15 U.S.C. §§ 1681a-1681s (1976 & 1978 Supp.).

[119] CAL. CIV. CODE § 1785.1 (West 1980).

[120] *Id.*

[121] *Id.*

[122] *Id.* § 1785.10(b).

[123] *Id.* § 1785.13(a). For example, information about bankruptcies more than fourteen years old, unpaid judgments more than ten years old, and arrests more than seven years old cannot be disseminated.

[124] *Id.* § 1785.11.

[125] *Id.* § 1785.16. Any disputed information must be investigated, and any misinformation corrected.

of the statute, the legislature announced sanctions for violations, including the payment of actual damages, court costs, attorneys fees, damages for pain and suffering, punitive damages for willful violations, and injunctive relief when appropriate.[126]

Congress enacted the Federal Privacy Act of 1974[127] to protect the privacy of individuals identified in information systems maintained by federal agencies. In addition, federal agencies are bound by the privacy protections of the Constitution. Requiring safeguards to prevent invasions of privacy,[128] the Privacy Act mandates that federal agencies obtain the consent of an individual prior to the disclosure of the record to another, unless the disclosure falls within an authorized purpose.[129] Furthermore, the Privacy Act provides that an agency may only record information that is relevant and necessary.[130] It also provides that individuals may see records relating to themselves and request that any errors be corrected.[131] The seriousness of the congressional intent to protect the privacy of individuals is indicated by the civil and criminal[132] penalties provided for violations of the Privacy Act.

## V. Protection of Computer Software

### *A. Patents*

One potential method of safeguarding computer programs is through application of patent law. United States Supreme Court decisions,[133] however, indicate that it will be extremely difficult to obtain patent protection for computer programs.[134] Patents are designed to give proprietors a "short-term, powerful monopoly in devices, processes, compositions of matter and designs which embody their ideas."[135] Patent holders have the right to "license and control the use of their patented devices or processes, [and] also to prevent the use of

[126] *Id.* § 1785.31.

[127] 5 U.S.C. § 552a (1976 & 1978 Supp.).

[128] *Id.* § 552a(b).

[129] *Id.* (*e.g.*, for census purposes or for civil or criminal enforcement activity).

[130] *Id.* § 552a(e).

[131] *Id.* § 552a(d).

[132] *Id.* § 552a(g), (i).

[133] Parker v. Flook, 437 U.S. 584 (1978); Dann v. Johnston, 425 U.S. 219 (1976); Gottschalk v. Benson, 409 U.S. 63 (1972).

[134] For a more complete discussion of patent protection for computer programs, see Note, Parker v. Flook *and Computer Program Patents*, 30 Hastings L.J. 1627 (1979); Note, *Patent Law—Patentable Subject Matter—Computer Software*—Parker v. Flook, 24 N.Y.L. Sch. L. Rev. 975 (1979).

[135] National Commission on New Technological Uses of Copyrighted Works, Final Report 41 (1979) [hereinafter cited as CONTU].

such devices or processes when they are independently developed by third parties."[136] The rights last for seventeen years.[137] To qualify, a "work must be useful, novel and non-obvious to those familiar with the state of the art in which the patent is sought."[138]

The United States Supreme Court has considered three cases[139] involving patents and computer programs. In all three decisions, the Court refused to afford patent protection. None of the cases, however, involved an attempt to patent solely the computer program. Rather, the applicants sought to patent various procedures employing computer programs. In these opinions, the Court has been careful to note that it has not addressed the question of whether computer programs constitute patentable subject matter, although the cases make it appear that patent protection for computer programs is difficult to obtain.

*Gottschalk v. Benson*[140] addressed the question of whether a patent could be granted on a method of converting numbers from one number system to another. The applicant for the patent had a method for converting from binary-coded decimal numbers to binary. The Court denied the patent, reasoning that the practical effect of granting it for the conversion method would be to patent an idea, and neither a scientific truth nor an idea may be patented.[141] The Court, however, noted that it was not denying the possibility that a patent might be granted for a computer program.[142]

In *Dann v. Johnston*,[143] the United States Supreme Court decided whether it was proper to patent a computer system permitting "a bank to furnish a customer with subtotals of various categories of transactions completed in connection with the customer's single account, thus

[136] *Id.*

[137] 35 U.S.C. § 154 (1976).

[138] CONTU, *supra* note 135, at 41 (citing 35 U.S.C. §§ 101, 102 & 103 (1976)).

[139] *See* cases cited in note 133 *supra*. The Supreme Court has recently granted certiorari in two other patent cases involving computer programs. *In re* Bradley, 600 F.2d 807 (C.C.P.A. 1979), *cert. granted sub nom.* Diamond v. Bradley, 48 U.S.L.W. 3595 (Mar. 18, 1980); *In re* Diehr, 602 F.2d 982 (C.C.P.A. 1979), *cert. granted sub nom.* Diamond v. Diehr, 48 U.S.L.W. 3595 (Mar. 18, 1980).

[140] 409 U.S. 63 (1972).

[141] *Id.* at 67. The Court found that the patent would have been one for a formula that was one of the "basic tools of scientific and technological work." *Id.*

A further problem with the patent application was that the conversion method for which protection was sought was not itself limited to its use in computers. *Id.* at 64. Thus, had the patent been granted, use of the conversion process anywhere, presumably even on a chalk board, would have infringed the patent. *Id.* at 71-72.

[142] The Court stated, "It is said that the decision precludes a patent for any program servicing a computer. We do not so hold." *Id.* at 71.

[143] 425 U.S. 219 (1976).

saving the customer the time and/or expense of conducting this bookkeeping himself."[144] The system was being sold as a computer service to banks and other data processing companies so that they could perform various services for customers. The parties and several amici asked the Court to address the general patentability of computer programs. The Court, however, elected not to reach that issue, dismissing the patenability argument on grounds of obviousness.[145] In rejecting the application, the Court relied on two factors. First, the system in question was similar to services already being performed by banks in their use of data processing equipment and computer programs, such as giving customers multiple accounts with separate periodic statements for each, as well as segregating service charge debits from other transactions within any given account.[146] Second, the Court said that the system was analogous to the previously patented Dirks system, which encompasses a data processing system used to keep track of various types of expenses for each department in a large business.[147]

In *Parker v. Flook*,[148] the applicant sought a patent on a method of updating alarm limits during catalytic conversion processes. The only distinction between prior methods and the Flook method was the inclusion in the latter of a mathematical formula used primarily for "computerized calculations producing automatic adjustments in alarm settings."[149] The Court stated that a scientific principle, such as that

[144] *Id.* at 220. For example, expenditures for food, fuel, and rent might be separately listed. The bank customer labels each check with a category code. When processing the checks, the bank enters the code on each check in magnetic ink characters. This allows the computer to list separately each type of expenditure on the periodic statement. *Id.* at 221-22.

[145] *Id.* The Court cited 35 U.S.C. § 103 (1976), which provides:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.

[146] 425 U.S. at 227. Although the Court did acknowledge that the system involved something more than providing a summary sheet for customers with many accounts, it nevertheless found that the "obviousness" test, requiring that the difference between the prior art and the subject matter in question be "sufficient to render the claimed subject matter unobvious to one skilled in the applicable art," was not met. *Id.* at 228 (citing the lower court's dissenting opinion, 502 F.2d 765, 772 (C.C.P.A. 1974) (Markey, C.J., dissenting)).

[147] *Id.* Again, despite the fact that the Johnston system was not identical to the Dirks system, it was similar enough that it was "obvious" to one who was reasonably skilled in the "art" of data processing systems' uses in the banking industry and hence presumably aware of the Dirks system. *Id.* at 229.

[148] 437 U.S. 584 (1978).

[149] *Id.* at 586. During catalytic conversion processes, conditions such as temperature and pressure are monitored. When any of these variables exceeds a predetermined alarm limit, an alarm signals an abnormality, indicating inefficiency or danger. It is often neces-

expressed in the mathematical formula in question, must be treated as though it were well known, and therefore, the overall process itself, not merely the formula, must be new and useful.[150] Here, inasmuch as this already known formula was the only novel feature of the Flook method, the process simply contained no patentable invention.[151]

All three of the aforementioned Supreme Court decisions in which patents were sought on computer related subject matter resulted in denial of patent protection. Similarly, in all three decisions, the Court did not foreclose the availability of patent protection for appropriate computer systems or computer programs. To be worthy of such protection the computer program must be novel, non-obvious, and do more than merely solve a mathematical equation. The Court in *Flook* asked Congress for guidelines specifying patent eligibility and duration for computer programs.[152] When considering the scope of patent protection for computer programs, there are some inherent difficulties that must be overcome. If a person were to patent instructions comprising a computer program, the protection would be illusory if another individual could employ the fundamentals of the program and, merely by changing some instructions, not infringe the patent.[153] Alternatively, attempting to obtain a patent on the function to be performed by the computer program, *e.g.*, a computer program to compute baseball batting averages, could be difficult because the function to be performed was obvious to one skilled in computers,[154] or because the program merely solved a mathematical equation,[155] or because it was a non-

sary to update alarm limits. The patent application described a method of updating alarm limits, consisting of three steps: (1) measuring the present value of the variable (*e.g.*, temperature); (2) using a mathematical formula to calculate an updated alarm limit; and (3) actually adjusting the alarm limit to the new value. The only difference between conventional methods and that described in the patent application was the second step—the mathematical formula. *Id.* at 585-86.

[150] *Id.* at 591-92.

[151] *Id.* at 594. By way of clarification, the Court analogized the claimed method in *Flook* to a claim that the formula for calculating a circle's circumference can be usefully applied to determine the circumference of a wheel. *Id.* at 595.

[152] It stated that the determination of what types of computer programs should be eligible for patent protection, as well as the form and duration of such protection, can best be answered by Congress based on empirical data not available to the Court. *Id.* at 595.

[153]

> Omission of one element or ingredient of a combination covered by any claim of a patent averts any charge of infringement based on that claim. This is true whether or not the omitted ingredient was essential to the combination of the patent and whether or not it was necessary to the operativeness of the device.

7 DELLER'S WALKER ON PATENTS § 543, at 324-25 (2d ed. 1972).

[154] *See* Dann v. Johnston, 425 U.S. 219, 220 (1976).

[155] *See* Parker v. Flook, 437 U.S. 584, 589, 591 (1978); Gottschalk v. Benson, 409 U.S. 63, 71-72 (1972).

patentable idea.[156] Thus, safeguarding computer programs through application of patent law is inadequate because its protection is often illusory or insurmountably difficult to obtain. These obstacles encourage a discussion of other, possibly more appropriate, forms of protection.

### *B. Trade Secrets*

The doctrine of trade secrets[157] is recognized in all fifty states. Existing as a creature of state statute or common law, the trade secret doctrine differs in definition and application from state to state. The main premise is that, if a business maintains confidentiality regarding its information or the way it accomplishes some task, the business should be legally protected against misappropriation of the secret.[158] Many computer businesses rely upon trade secret protection for computer software,[159] although there are several problems in its application. First, lack of uniform laws reduces the utility of trade secret protection. Second, because the maintenance of secrecy is critical to receiving trade secret protection it may be an inappropriate method for safeguarding information intended to be distributed widely, such as the many computer programs that are sold in multiple copies over the counter. A seller of software must enter into non-disclosure agreements with buyers of the software, as well as with the seller's own employees and access to the secret must be limited to a small number of people. This reduction in the flow of information wastes human effort and causes people to write programs when similar programs have already been written, but are being kept secret. Despite the disadvantages attendant upon the use of trade secret protection, it is a frequently employed method because it affords an alternative to the narrow scope of protection provided by patent law. Furthermore, as will be discussed later, the availability of federal copyright protection is unclear.[160]

[156] *See* Gottschalk v. Benson, 409 U.S. 63, 71 (1972).

[157] A trade secret is "[a]ny formula, pattern, device or compilation of information which is used in one's business and which gives him an opportunity to obtain an advantage over competitors who do not know or use it." University Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518, 534 (5th Cir. 1974) (citing RESTATEMENT OF TORTS § 757, Comment b (1939)). For a more complete discussion of trade secret protection, *see* Bender, *Trade Secret Protection of Software*, 38 GEO. WASH. L. REV. 909 (1970).

[158] CONTU, *supra* note 135, at 42-43.

[159] Bigelow, *The Legal Protection of Proprietary Software—A Special Report*, 3 COMPUTER L. & TAX REP. 4, 5 (Nov. 1976). *See, e.g.*, University Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518 (5th Cir. 1974) (plaintiff awarded damages for misappropriation of its computerized retail inventory system).

[160] The National Commission on New Technological Uses of Copyrighted Works rec-

### C. Copyright

Because the availability of patent protection for computer programs is doubtful and maintaining trade secret protection requires great vigilance in protecting and limiting access to the programs, copyright may be the most useful and efficient legal protection available for computer programs. The National Commission on New Technological Uses of Copyrighted Works (CONTU) was created by Congress as part of its effort to revise the United States copyright law.[161] CONTU's function was to recommend changes in the copyright law to the President and Congress. These alternatives were to assure public access to copyrighted works used with computers while respecting the rights of the copyright owners in such works.[162] The Commission noted that two trends have created a need to extend legal safeguards to computer programs: first, computers have become smaller and less expensive in recent years, enabling many people to have computers in their homes and offices, and second, many computer programs can be used on more than one computer,[163] permitting widespread copying and use of programs. Without some type of legal protection against another's duplication and distribution of the programs, people are reluctant to produce computer programs. The Commission concluded that copyright protection should be available for computer programs[164] and data bases.[165]

ommended copyright protection for computer programs, CONTU, *supra* note 135, at 29, and a summary of the Commission proposals has been introduced by Rep. Robert Kastenmeier (D. Wis.) as the Computer Software Copyright Act of 1980, H.R. 6934, 96th Cong., 2d Sess., 126 CONG. REC. H2263 (daily ed. Mar. 26, 1980).

[161] CONTU, *supra* note 135, at 1.

[162] *Id.*

[163] *Id.* at 24.

[164] *Id.* at 29. In reaching these conclusions, the Commission compared copyright to patent and trade secret protection, *id.* at 40-47, discussed the difficulties in obtaining patent protection, *id.* at 41-42, as well as the inherent limitations of trade secret protection, *id.* at 43-44, and thus recommended copyright protection as the most appropriate alternative.

[165] *Id.* at 94. A data base is "the physical representation of information in some type of organized, organizable, or unorganized computer-readable form. For example, it may be a list of a corporation's customers, organized perhaps alphabetically by name or by geographic area, or volume of business, etc. The data base is input to the computer," and may be altered, as occurs when customers not ordering goods within the last year are dropped from the list; or unaltered, as occurs when the data base is used to print mailing labels. BENDER, § 2.06[1], *supra* note 15, at 2-112 to 2-113 (1979). For a discussion of the Commission's analysis and conclusions regarding data bases, see CONTU, *supra* note 135, at 94-104.

The Commission indicated that data bases are protected under 17 U.S.C. § 102(a) (1976), which provides in part that "[c]opyright protection subsists, in accordance with this title, in original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communi-

The Commission explained that the Constitution gives Congress the power to grant authors exclusive rights in their writings,[166] and that the word "Writing" in the Constitution has been given a "broad and dynamic meaning"[167] in case law. A computer program is created the same way that a novel, poem, play, musical score, blueprint, advertisement, or telephone directory is created—by placing symbols in a medium. All of these works are eligible for copyright protection under the Constitution; computer programs should be eligible for the same protection.[168]

The CONTU Report mentioned that Congress had included in the Copyright Act[169] a section specifying that the same copyright protection for computer works exists in the new law as had existed in the old.[170] However, the nature of the prior protection is unclear. While the Register of Copyrights has accepted computer programs for copyright protection since 1964, this determination has never been challenged.[171] To clarify the availability and scope of copyright protection, the Commission recommended several statutory changes to the copyright law. It recommended that section 101 be amended to add this definition: "A computer program is a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result."[172] It also recommended that section 117[173] be repealed and replaced with a new section that would allow the rightful possessor of a computer program to protect the program by making archival copies and to adapt the program so that it can be used on the possessor's computer.[174]

The Commission suggested that computer programs should be

cated, either directly or with the aid of a machine or device." CONTU, *supra* note 135, at 94. The Commission found that 17 U.S.C. § 106 (1976) prohibits the unauthorized copying or input of a data base embodied in a computer-readable medium. *Id.* at 95.

[166] U.S. CONST. art. I, § 8, cl. 8 provides: "The Congress Shall have Power . . . [t]o promote the Progress of Science and Useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."

[167] CONTU, *supra* note 135, at 35. *See, e.g.*, Goldstein v. California, 412 U.S. 546 (1973) (sound recordings); Mazer v. Stein, 347 U.S. 201 (1954) (lamp base statuettes); Kalem Co. v. Harper Bros., 222 U.S. 55 (1911) (motion pictures); Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53 (1884) (photographs).

[168] CONTU, *supra* note 135, at 36.

[169] 17 U.S.C. §§ 101-810 (1976 & 1978 Supp.).

[170] CONTU, *supra* note 135, at 21 (citing 17 U.S.C. § 117 (1976)).

[171] *Id.* at 38-39. The Register required that human readable copies of the program be submitted for registration. *Id.* at 38.

[172] *Id.* at 30.

[173] 17 U.S.C. § 117 (1976).

[174] CONTU, *supra* note 135, at 30. The suggested section provides:

> Notwithstanding the provisions of § 106, it is not an infringement for the rightful

safeguarded in all of their possible forms, including, but not limited to, a human-readable listing of the computer instructions, a magnetic tape or disk recording of the program, or a copy in the computer's memory.[175] Copyright protection was also recommended for the different forms in which a program may be represented, such as flowcharts,[176] source codes,[177] and object codes.[178] Such protection would prohibit users from taking the writings of others to operate their machines without obtaining the copyright owner's permission. One would remain free to make the computer perform the same function as it would with the copyrighted work, but only through creative effort, not piracy.

## VI. EVIDENCE

Problems of admissibility of computer printouts in judicial proceedings may arise because of rules against admitting hearsay evidence.[179] Computer evidence, however, may qualify for admission under a business record exception[180] to the hearsay rule. Under this

> possessor of a copy of a computer program to make or authorize the making of another copy or adaptation of that computer program *provided*:
> (1) that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner, or
> (2) that such new copy or adaptation is for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful.
>
> Any exact copies prepared in accordance with the provisions of this section may be leased, sold, or otherwise transferred, along with the copy from which such copies were prepared, only as part of the lease, sale, or other transfer of all rights in the program. Adaptations so prepared may be transferred only with the authorization of the copyright owner.

[175] *Id.* at 55-56. In a recent case, the plaintiff had marketed a computerized chess game, in which the computer program was part of the computer's circuitry. The defendant copied the circuitry and marketed a competing game. The court held that the copied circuitry did not violate the Copyright Act because one could not see and read the copy. Data Cash Sys., Inc. v. JS&A Group, Inc., 480 F. Supp. 1063, 1065-69 (N.D. Ill. 1979), *aff'd on other grounds*, No. 80-1085 (7th Cir. Sept. 2, 1980).

[176] CONTU, *supra* note 135, at 53. A flowchart is defined as "a graphic representation for the definition, analysis or solution of a problem in which symbols are used to represent operations, data flow, or equipment." *Id.* at 53 n.126.

[177] *Id.* at 53. A source code is defined as "a computer program written in any of several programming languages employed by computer programmers." *Id.* at 53 n.127.

[178] *Id.* at 53-54. An object code is defined as "the version of a program in which the source code language is converted or translated into the machine language of the computer with which it is to be used." *Id.* at 54 n.128.

[179] BENDER § 6.02[5], *supra* note 15. *See generally* Jacobson, *The Use of Computer Printouts as Evidence in Commercial Litigation*, 82 COM. L.J. 14 (1977). California provides that hearsay evidence is "evidence of a statement that was made other than by a witness testifying at the hearing and that is offered to prove the truth of the matter asserted." CAL. EVID. CODE § 1200 (West 1979).

[180] The California business record exception states:

exception, computer maintained business records are admissible if it can be shown that "the criteria for the admission of non-computer maintained business records have been met [and] the court finds that reliable computer equipment and techniques have been used."[181] It is necessary to understand the foundation required to admit computer printouts into evidence. An analysis of the cases discussing this question reveals that many foundational requirements relate both to computer produced records and non-computer produced records, while some prerequisites apply specifically to computer produced records.[182]

### *A. General Foundation Requirements*

#### 1. Personal knowledge of the foundation witness

The majority of courts, which addressed whether the foundation witness must have personal knowledge[183] of the act or event recorded,

> Evidence of a writing made as a record of an act, condition, or event is not made inadmissible by the hearsay rule when offered to prove the act, condition, or event if:
> (a) the writing was made in the regular course of a business;
> (b) the writing was made at or near the time of the act, condition, or event;
> (c) the custodian or other qualified witness testifies to its identity and the mode of its preparation; and
> (d) the sources of information and method and time of preparation were such as to indicate its trustworthiness.

CAL. EVID. CODE § 1271 (West 1979). The Federal Rules of Evidence similarly provide that the following shall not be excluded by the hearsay rule:

> A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

FED. R. EVID. 803(6).

[181] JUDICIAL CONFERENCE OF THE UNITED STATES COORDINATING COMMITTEE FOR MULTIPLE LITIGATION, MANUAL FOR COMPLEX LITIGATION § 2.716 (1977). It must be noted, however, that the admissibility of computer printouts, as well as all other evidence, is contingent upon a finding of relevance and materiality. *See* FED. R. EVID. 401 & 402.

[182] *See* Monarch Fed. Sav. & Loan Ass'n v. Genser, 383 A.2d 475 (N.J. Super. Ct. Ch. Div. 1977), and cases cited therein.

[183] According to general principles governing testimonial evidence regarding recorded entries, the person whose statement is received as testimony should speak from personal observation or knowledge. 5 J. WIGMORE, EVIDENCE § 1530, at 449 (Chadbourn rev. 1974). Is the personal knowledge requirement satisfied if the facts are personally known to another, but not to the entrant? It is concluded that

> where an entry is made by one person in the regular course of business, recording an oral or written report, made to him by other persons in the regular course of business, of a transaction lying in the personal knowledge of the latter persons,

have rejected this common law requirement.[184] The remaining foundational requirements concern the accuracy of the computer records themselves.[185]

### 2. Qualifications of the foundation witness

All of the cases that have discussed the qualifications of a foundation witness have involved statutes or case law describing the type of witness required.[186] Some courts have required that the supervisor of computer operations testify,[187] while other courts have been less stringent, permitting an employee of the company who maintains the records and is familiar with the records to testify.[188] One court noted that the jurisdiction did nót require the custodian of the records, or other equivalent witness, to testify as long as whoever testifies is able to provide the foundational information required.[189] The witness should be familiar with the way the computer printout was generated to be able to satisfy the court that the sources of information and time of preparation show that the evidence is trustworthy.[190]

> there is no objection to receiving that entry under the present exception, verified by the testimony of the former person only, or of a superior who testifies to the regular course of business, provided the practical inconvenience of producing on the stand the numerous other persons thus concerned would in the particular case outweigh the probable utility of doing so.

*Id.* at 451 (emphasis omitted).

[184] One reason for rejecting the personal knowledge requirement is that because of employee transiency and the time span covered in the business records, it may be impossible to locate the person(s) having personal knolwedge of the events described in the computer record. Monarch Fed. Sav. & Loan Ass'n v. Genser, 383 A.2d 475, 485 (N.J. Super. Ct. Ch. Div. 1977).

[185] The major justification for the hearsay exclusion is that the truth of the out-of-court statement cannot be verified through cross-examination. BENDER § 6.01[2], *supra* note 15.

[186] Monarch Fed. Sav. & Loan Ass'n v. Genser, 383 A.2d 475, 485 (N.J. Super. Ct. Ch. Div. 1977), and cases cited therein.

[187] Railroad Comm'n v. Southern Pac. R.R., 468 S.W.2d 125, 128 (Tex. Ct. Civ. App. 1971).

[188] Bobbie Brooks, Inc. v. Hyatt, 239 N.W.2d 782, 784-85 (Neb. Sup. Ct. 1976) (present custodian, rather than custodian at the time the records originally were made, allowed to testify).

[189] Monarch Fed. Sav. & Loan Ass'n v. Genser, 383 A.2d 475, 485 (N.J. Super. Ct. Ch. Div. 1977). The relevant New Jersey statute provides:

> A writing offered as a memorandum or record of acts, conditions or events is admissible to prove the facts stated therein if the writing or the record upon which it is based was made in the regular course of business, at or about the time of the act, condition or event recorded, and if the sources of information from which it was made and the method and circumstances of its preparation were such as to justify its admission.

N.J. STAT. ANN. § 2A:84A, Rule 63(13) (West 1976).

[190] *See* Monarch Fed. Sav. & Loan Ass'n v. Genser, 383 A.2d 475, 485-86 (N.J. Super. Ct. Ch. Div. 1977).

### 3. Computer records made in the ordinary course of business

The requirement that computer records be made in the ordinary course of business necessitates a showing that the computer records were routinely prepared,[191] rather than prepared just for trial.[192] The proponent of the evidence must further show that the printouts are relied on by the company as sufficiently accurate for business purposes.[193]

In one case in which it was argued that the computer printout was inadmissible because it was prepared for use in litigation, the Nebraska Supreme Court said that the argument exalted form over substance. While it was true that the printout was made for trial, the taped record from which the printout came was made in the usual course of business.[194]

### 4. Time of entry

Under the business records exception to the hearsay rule, the entry must be made at or about the time of the act.[195] This requirement is satisfied if the input is made reasonably contemporaneously with the occurrence of the events to which the printout relates.[196] In a Nebraska Supreme Court case it was held that this requirement was satisfied when the foundation witness testified that "the events contained in the record were recorded within 1 week of their occurrence in the regular course of business."[197]

It is immaterial when the computer printout itself was made. In one case, the printout was made several months after the information was fed into the computer. The Sixth Circuit rejected the claim "that the computer printout should not have been received in evidence because it was not prepared at the time the acts which it purports to describe were performed or within a reasonable time thereafter."[198] The court stated that the computer printout is just a presentation in compre-

[191] *See, e.g.*, United States v. Scholle, 553 F.2d 1109, 1125 (8th Cir. 1977) (disputed printouts found to be drug analyses computerized routinely in the regular course of business); King v. State *ex rel.* Murdock Acceptance Corp., 222 So. 2d 393, 398 (Miss. 1969); Transport Indemnity Co. v. Seib, 132 N.W.2d 871, 874 (Neb. 1965).

[192] D&H Auto Parts, Inc. v. Ford Mktg. Corp., 57 F.R.D. 548, 552 (E.D.N.Y. 1973).

[193] *See id.*; BENDER § 6.01[4], *supra* note 15.

[194] Transport Indemnity Co. v. Seib, 132 N.W.2d 871, 875 (Neb. 1965).

[195] *See* note 180 *supra.*

[196] BENDER § 6.01[4], *supra* note 15; Department of Mental Health v. Beil, 357 N.E.2d 875, 880 (Ill. Ct. App. 1976).

[197] Bobbie Brooks, Inc. v. Hyatt, 239 N.W.2d 782, 785 (Neb. 1976).

[198] United States v. Russo, 480 F.2d 1228, 1240 (6th Cir. 1973).

hensible form of what is maintained on the magnetic tape, and that it would be unjustly severe to require that the printout, as well as the input on which it was based, must be produced at or within a reasonable time after each act or transaction to which it relates.[199] The reasonable time requirement, then, applies only to the input of the data and not to the printout.

#### 5. Meaning of computer printout

The foundation witness must offer a thorough explanation of the meaning and identity of the computer printout.[200] In *Transport Indemnity Co. v. Seib*,[201] which involved an action for insurance premiums, the proffered printouts showed accidents by date, name of driver, type of accident, amount and type of loss, and various expenses and information from which the premium could be computed. The foundation witness directed the insurance company's accounting department, and the records in question were under his custody and control. He provided a detailed explanation of each item of information in the printout, thus satisfying the ,requirement that the meaning and identity of the printout be established.[202]

### *B. Foundation Requirements Specific to Computers*

Admissibility is dependent on a showing that the computer programs were performing properly. The procedures used for testing their accuracy and reliability must be presented to the court.[203] In *Transport Indemnity*, the computer program used a mathematical formula to compute insurance premiums based on a percentage of gross monthly receipts. The foundation witness performed hand calculations that established that the machine-generated results were accurate.[204]

The foundation witness additionally must describe the flow of information into and out of the computer. In *King v. State* ex rel. *Murdock Acceptance Corp.*,[205] a question arose whether certain computerized accounting records were admissible. The records were admitted after extensive testimony by the foundation witness under

[199] *Id.*

[200] Transport Indemnity Co. v. Seib, 132 N.W.2d 871, 874 (Neb. 1965); People v. Gauer, 288 N.E.2d 24, 25 (Ill. Ct. App. 1972).

[201] 132 N.W.2d 871 (Neb. 1965).

[202] *Id.* at 873-74.

[203] Monarch Fed. Sav. & Loan Ass'n v. Genser, 383 A.2d 475, 487 (N.J. Super. Ct. Ch. Div. 1977); United States v. Scholle, 553 F.2d 1109, 1125 (8th Cir. 1977).

[204] 132 N.W.2d at 874.

[205] 222 So. 2d 393 (Miss. 1969).

whose supervision the computerized records were maintained. The witness testified that the accounting was done using a Burroughs B-280 computer, which is standard equipment recognized as an efficient and reliable machine. The information was keypunched by experienced operators and verified by another operator. If a card had been punched incorrectly, it would not have gone through the verifying machine. The cards were fed into the computer and the information was stored on tape.[206] It must also be established that the computer operator[207] understood the operation of the computer and ran it properly before the evidence can be admitted.[208] Furthermore, it must be shown that the input data was in a format anticipated by the programs.[209]

Courts have been willing to assume that the computer functioned properly unless evidence to the contrary is presented by the opponent of the computer evidence.[210] Computer hardware malfunctions, however, do occur and may be the source of incorrect output.[211] The computer system may consist of the computer and various peripheral units for input, storage, and output. There may be card readers, magnetic tape drives, keyboard input devices, optical scanning devices, printers, graph plotters, disc storage, drum storage, and various other devices.[212] Any of these can fail.[213] Equipment maintenance records may be an effective way of determining whether the equipment was in good working order at the time the information in question was processed.[214] Human error in programming, preparing the data for processing, or operating the machine are likely sources of inaccuracy.[215] While the

[206] *Id.* at 396-97.

[207] The computer operator is the person who operates the computer, who inputs the information to be processed, and who removes the output. MEEK, *supra* note 2, at 159. It should not be assumed that the computer operator performed correctly. The operator may have used the wrong magnetic tape, punched wrong buttons on the computer, or otherwise run the computer improperly.

[208] United States v. DeGeorgia, 420 F.2d 889, 895 (9th Cir. 1969) (Ely, J., concurring); United States v. Russo, 480 F.2d 1228, 1241 (6th Cir. 1973). *See* Railroad Comm'n v. Southern Pac. R.R., 468 S.W.2d 125, 129 (Tex. Ct. Civ. App. 1971).

[209] For example, if a program expected that the first piece of information on the keypunched card was a numerical representation of the month of purchase, and the second piece of information was the price, problems could arise if these were reversed. BENDER § 2.04[3], *supra* note 15. *See also id.* § 2.05[1]; Freed, *supra* note 5, at 25.

[210] United States v. Scholle, 553 F.2d 1109, 1125 (8th Cir. 1977); United States v. Russo, 480 F.2d 1228, 1239-40 (6th Cir. 1973).

[211] *See* BENDER § 2.05[6], *supra* note 15.

[212] *See generally id.* § 2.05 for descriptions of these items.

[213] *See* Freed, *supra* note 5, at 25.

[214] *See* R. FREED, COMPUTERS AND THE LAW 216 (4th ed. 1973) (the maintenance contract of the General Services Administration requires written maintenance reports).

[215] BENDER § 2.05[6], *supra* note 15, at 2-100 n.261.

percentage of hardware errors in computer operations is very low, the number of hardware errors can be significant because of the great number of discrete operations performed by a computer.[216]

## VII. Conclusion

This article has been an attempt to familiarize attorneys with computers and some of the law relating to them. No attempt has been made to create experts in computer law. If after reading this article attorneys are able to identify problems and provide assistance to their clients on the basis of the research presented here, then the article has achieved a valuable result.

[216] *Id.* § 2.05[6], at 2-100.