Spring 1977


Joseph Scafetta Jr.
COMPUTER SOFTWARE
AND
UNFAIR METHODS OF COMPETITION

by JOSEPH SCAFETTA, JR.*

UNFAIR COMPETITION IN THE TRADITIONAL SENSE

When the common law term “unfair competition” is bandied around in legal circles in discussions of wrongful actions by others in the computer industry, the term itself is not appropriate because it traditionally refers only to the practice of attempting to pass off one's own goods, by imitation of general appearance, as the goods of a competitor who enjoys immediate favorable public recognition. The phrase that should be used is the more general term “unfair methods of competition” which is, unfortunately, quite nebulous itself and, not unexpectedly, appears undefined in Federal Trade Commission Act section 5. Although not defined therein, this term has generally become known to embrace any unfair trade practice which dishonestly negates a competitor's opportunity for fair play in the marketplace, such as false advertising, palming off, misappropriation of trade secrets, etc.

Common law unfair competition and false advertising are exemplary of unfair methods of competition that either do not occur or are not special problems in the computer industry. However, because of the nature of software and the meager extent of legal protection available to the industry, there is one unfair

---


method of competition that stands out as a matter of deep and anxious concern—misappropriation of trade secrets. This article will attempt to explore why both present laws and software itself have led to this problem, what are the major aspects of the problem, and, finally, what those in the industry can do to protect themselves against its occurrence.

**THE PREFERRED CHOICE OF LEGAL PROTECTION FOR COMPUTER SOFTWARE**

There are three routes by which one may protect intellectual property. Usually, the most favored protection for property of a utilitarian nature is patenting. However, this route has been generally shunned by the computer industry because of the present uncertainty over the extent, if any, of protection available for software. In *Gottschalk v. Benson* the Supreme Court denied a patent on a process for use in programming a digital computer but specifically refused to preclude a patent for all programs servicing a computer. Later, in *Dann v. Johnston* the Supreme Court denied a patent on a computer-programmed system for automatic record keeping on the grounds that the invention was obvious to one of reasonable skill in the data processing art. However, in so ruling the Court again deliberately sidestepped the threshold issue of the general patentability of computer programs. Thus, the continuing refusal of the Supreme Court to decide the basic issue has resulted in a concomitant reluctance on the part of the computer industry to seek patent protection.

The most favored route for protection of property of a written nature is usually copyrighting but this likewise has been

---

6. Software is a generic name for various inputs to computers. "Systems" software is an input via machine-readable cards or magnetic tape by which switches are set to wire the electronic circuits so they function as may be required by any subsequent "applications" software. Applications software is a synonym in the trade for the more commonly used term "program." A program is a series of machine-readable representations on a deck of cards or magnetic tape which directs the operation of a general purpose digital computer through a desired procedure or algorithm.

Software is also called "instant hardware" because, upon its input into the general purpose digital computer, it causes the computer automatically to make circuit connections so that it may process electrical signals in a way determined by the connections in the same manner as if the circuits were hand-soldered. Because the general purpose digital computer is simply an organized storeroom of electrical components waiting to be interconnected in any manner by the introduction of software (see Guidelines, 829 Off. Gaz. Pat. Office 1 (1966)), the valuable part of a digital computer lies in the instructions or "soldering directions" of the software.

8. Id. at 71.
10. Id. at 220.
generally shunned by the computer industry. The reason is two-fold. First, a copyright provides protection only against a taking by substantial copying of the expressed form in the written program. To find infringement, there must be some actual appropriation of language.\textsuperscript{11} A skilled programmer can easily avoid infringement by restating any routine in analogous machine-readable language that would produce the identical end result of the program sought to be appropriated. Second, a copyright does not provide protection to the owner against another's use of the concept, idea, or algorithm\textsuperscript{12} embodied in the software.\textsuperscript{13} Also, there is a prerequisite of "publication" before a written program can be registered for a federal statutory copyright.\textsuperscript{14} At the point of publication, the contribution made by the concept, idea, or algorithm to the data processing art, copyright protection of only a particular written expression of a program is too narrow and totally inadequate in the eyes of the computer industry.

Because of the uncertainty of the extent of protection available via the usually favored routes of patenting and copyrighting, the preferred choice of legal protection for computer software has been to maintain them as trade secrets.\textsuperscript{15} Now that state

\textsuperscript{12} An algorithm is a prescribed set of well-defined rules or processes for the solution of a problem in a finite number of steps, e.g., a full statement of an arithmetic procedure for an evaluation to a stated degree of precision. See Joint Technical Committee on Terminology of the International Federation for Information Processing and International Computation Centre, IFIP-ICC Vocabulary of Information Processing 13 (1966).
\textsuperscript{14} 17 U.S.C. § 13 (1970), as amended by Act of October 19, 1976, Pub. L. No. 94-553, 90 Stat. 2541 (to be codified in 17 U.S.C. § 13) constituted a general revision of the copyright laws, to be effective on January 1, 1978. Publication is no longer a prerequisite of registration since unpublished works may be registered. Section 104(a) of the amended Act states that "works specified . . . , while unpublished, are entitled to protection under this title . . . ." However, registration is a prerequisite to institution of an infringement suit and certain remedies available. Section 411(a) of the amended Act states that "no action for infringement of copyright in any work shall be instituted until registration of the copyright claim has been made . . . ." Also, Section 412 of the amended Act states that "no award of statutory damages or of attorney's fees . . . shall be made for—(1) any infringement of copyright in an unpublished work commenced before the effective date of its registration . . . ." Although the objection of the computer industry to copyright protection has been partially overcome by the removal of the publication prerequisite, objection to copyrights remains because of the narrow scope of protection to only particular written expressions of a work. Finally, Section 102(b) of the amended Act states that "[i]n no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work."

\textsuperscript{15} For an in depth and sophisticated treatment of this subject, see
laws for the protection of trade secrets have been recognized as generally constitutional by the Supreme Court, the trade secret route has become the rule for the industry. Concomitantly, the industry considers computer software programs to be clearly trade secret subject matter.

Another reason the trade secret route is preferred over patenting and copyrighting is that, unlike the statutorily limited terms for patents and copyrights, state protection for trade secrets lasts as long as the software program is kept secret, which conceivably may be forever. Secrecy, an essential element, must be proven in order to establish a trade secret. Indeed, the value of a trade secret resides in its secrecy, not in its disclosure. However, a problem for owners lies in obtaining restitution and possibly even retribution against those who would unfairly compete in the industry by misappropriating trade secrets.

A New Look at Unfair Methods of Competition in View of a New Technology

Unfair methods of competition involving misappropriation of trade secrets have traditionally required a taking or copying of


17. Restatement of Torts § 757, Comment b (1939) states: Definition of trade secret. A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. A trade secret is a process or device for continuous use in the operation of the business. Generally it relates to the production of goods, as, for example, a machine or formula for the production of an article. It may, however, relate to the sale of goods or to other operations in the business.

18. 35 U.S.C. § 154 (1970) states: "Every patent shall contain... a grant to the patentee, his heirs or assigns, for the term of seventeen years..."

19. 17 U.S.C. § 24 (1970) states: "The copyright secured by this title shall endure for twenty-eight years from the date of first publication... [and]... for the further term of twenty-eight years when application for such renewal and extension shall have been made to the copyright office." Act of October 19, 1976, Pub. L. No. 94-553, § 302(a), 90 Stat. 2541 (1976) states: "Copyright in a work... subsists from its creation and... endures for a term consisting of the life of the author and fifty years after the author's death." 90 Stat. 2541 (1976) states: "Copyright in a work... subsists from its creation and... endures for a term consisting of the life of the author and fifty years after the author's death."

20. Restatement of Torts § 757, Comment b (1939) states: Secrecy. The subject matter of a trade secret must be secret. [A] substantial element of secrecy must exist, so that, except by the use of improper means, there would be difficulty in acquiring the information. An exact definition of a trade secret is not possible. Some factors to be considered in determining whether given information is one's trade secret are: (1) the extent to which the information is known outside of his business; (2) the extent to which it is known by employees and others involved in his business; (3) the extent of measures taken by him to guard the secrecy of the information; (4) the value of the information to him and to his competitors; (5) the amount of effort or money expended by
tangible property. Analog computers—which by their very nature do not utilize software—and the hardware parts of digital computers constitute tangible property. Consequently, their misappropriation would easily meet the traditional common law requirement of a "taking."

However, the digital computer requires the use of software. This technological innovation led to the creation of basic legal problems for those who wanted to protect their software against the unscrupulous by traditional tort and criminal law concepts.

Software as Property

The first and most basic problem facing owners was whether or not software was indeed property. Because of its nature as input in the form of holes in paper cards and magnetized areas on magnetic tape, software was questioned initially in the courts as to whether it was property capable of being taken in the traditional, legal sense. A reexamination of the basic concept of property as a tangible was required. The question was answered affirmatively when the criminal law was viewed through the magnifying glass of computer programs in Hancock v. State.

The defendant, a computer programmer employed by Texas Instruments (TI) in Dallas, worked with approximately 100 secret programs that related to seismic and other geophysical applications. He printed out and photocopied fifty-nine of these programs, valued by his employer at two and one-half million dollars, and attempted to sell them to Texaco Oil for five million dollars. Texaco representatives alerted TI to the offer and they

---


22. An analog computer system provides a continuous representation of a changing physical system. The output of an analog appears as the operation of a printing press, flow control in an oil refinery, synchronization of machinery in an industrial plant assembly line, or the tracking of a guided missile.

23. A digital computer system makes use of "discrete" quantities which are manipulated to generate the desired result or answer. The output of a digital appears in the form of a mathematical or scientific calculation or a stack of payroll checks. "Hardware" is a term used in the trade for the assembly of disconnected and inoperative circuits and apparatuses within the digital.

24. A "taking," as an element of the crime of larceny, has been defined broadly to mean that one "will acquire dominion over the property, enabling him to take actual custody or control thereof, and amounting to a trespass or its equivalent." 50 Am. Jur. 2d Larceny § 10 (1970) (footnotes omitted).

25. The first commercial use of software-programmed digital computers began about 1953.

jointly hired an investigator who, upon being shown the programs by the defendant's accomplice, confiscated the photocopies and turned them over to the state prosecutor in Dallas. Criminal charges for theft of property worth more than fifty dollars were brought. Defendant contended that the programs were not "corporeal personal property" within the meaning of the state penal code, that if the programs were property they were valueless in Dallas because there was no market for them, and that, if the programs were valuable property, he had stolen at most thirty-five dollars worth of tangible paper.

These defenses were unavailing and defendant was convicted. On appeal, the Court of Criminal Appeals of Texas found that the computer programs were property subject to theft because the state statute enumerated "all writings of every description, provided such property possess any ascertainable value." The court also found that, although the programs were used in Dallas only by TI employees, they had a market value in excess of fifty dollars because they were used for a price by others, albeit outside Dallas.

The defendant's petition for a writ of habeas corpus in the federal district court was denied, and on appeal to the fifth circuit, the appellate court felt bound by the statutory interpretation of the state court that the papers containing the photocopied computer programs were corporeal property. Consequently, the appellate court affirmed the denial of the request for a writ of habeas corpus on the grounds that the state law, as so construed, did not violate due process.

Although the case was decided on the basis of a liberal interpretation of a state statute, the Hancock opinions show a clear willingness to extend the definition of property to include a valuable intangible, such as a computer program.

**Intangible Property Capable of Being Taken**

A second basic problem confronting those who wished to protect their software by traditional tort and criminal law concepts was whether or not software, as intangible property, was capable of being "taken." It appears that, after the Hancock cases cleared the hurdle of finding that software was property, the decision-makers concluded sub silentio that software—like any

27. Id. at 908.
28. Id.
29. Id. at 910-11.
30. Hancock v. Decker, 379 F.2d 552 (5th Cir. 1967).
31. Id. at 553.
32. See notes 26 & 30 supra.
other property—was indeed capable of being taken. Because the Hancock cases did not analyze the issue of whether or not there was a taking in the traditional legal sense by trespass and asportation, the issue is still wide open for a detailed analysis that may result in a contrary conclusion. Clearly, if any court is to decide that software can be the subject of trespass and asportation, it must do so by making a constructive finding to include situations where a disloyal person enters upon the employer's premises and carries off valuable software information in his mind. In any event, unsatisfied with this singular legal victory in the Hancock cases, representatives of the computer industry have actively petitioned state legislatures for enactment of broadly worded criminal laws specifically punishing those who would take intangible property such as computer programs.

Although a "taking" is often broadly defined in criminal statutes, the concomitant strict construction of penal codes by the courts may not provide a sufficient deterrent effect in some future cases, and consequently it may be necessary to pursue money damages in a tort action against any apprehended, solvent culprit—individual, corporate, or otherwise—with resort to the broader concept in the Restatement of a taking as any "improper means of discovery."

33. Although not specifically discussed, this issue was obviously resolved affirmatively.
34. 50 Am. Jur. 2d Larceny § 14 (1970) (footnotes omitted) states: A rule universally recognized, in the absence of any statute to the contrary, although characterized by some elasticity of interpretation in certain situations, is that there must be a trespass in the taking of another's goods in order to constitute larceny—a trespass to the possession of the owner, either actual or constructive. Without this trespass there can be no larceny.
35. 50 Am. Jur. 2d Larceny § 15 (1970) (emphasis added) (footnotes omitted) states: Both at common law and under statutes declaratory thereof, the felonious taking which is an essential element of larceny must be followed by such an asportation or carrying away as to supersede the possession of the owner for an appreciable time. Unless otherwise provided by statute, the crime is not complete until there has been an asportation, although the offender had the power to carry the property away. Furthermore, property that is not subject to asportation cannot be stolen.
36. See text accompanying notes 45-57 infra.
38. See note 24 supra.
39. Although solvency is not usually a characteristic of the criminal milieu, it may sometimes be an attribute of those sophisticated enough to engage in the piratical activity under discussion.
40. RESTATEMENT OF TORTS § 757, Comment f (1939) states: Improper Means of Discovery. The discovery of another's trade secret by improper means subjects the actor to liability independently of the harm to the interest in the secret. Examples of such means are fraudulent misrepresentations to induce disclosure,
THE PRIME METHOD OF UNFAIR COMPETITION IN THE COMPUTER INDUSTRY—MISAPPROPRIATION OF TRADE SECRETS

The most common method of unfair competition in the computer industry is the misappropriation of trade secrets. Liability for this type of interference with business relations is expounded in the Restatement of Torts section 757 which has been noted as "widely relied upon" by the Supreme Court. Damages will be levied by state courts in tort cases whenever trade secrets are discovered by improper means. Although incapable of precise definitions, improper means of discovery do include "means which fall below the generally accepted standards of commercial morality and reasonable conduct." However, known incidences of such improper means are not too numerous. Perhaps this is so because the intellectual sophistication of those involved in such activity and the nature of the offense as a nonviolent, inconspicuous commission have combined to prevent widespread detection. On the other hand, the sparsity of cases may be due to a level of honesty among those in the industry that is higher than that of the general population. In either event, the quarter century since the commercial advent of computer technology has not been long enough to produce abundant examples of improper means. Nevertheless, there are some cases that merit attention.

The Disloyal Employee

Although "equity has no power to compel a man who tapping of telephone wires, eavesdropping or other espionage. A complete catalogue of improper means is not possible. In general they are means which fall below the generally accepted standards of commercial morality and reasonable conduct.

41. Liability for Disclosure or Use of Another's Trade Secret—General Principle.

One who discloses or uses another's trade secret, without a privilege to do so, is liable to the other if
(a) he discovered the secret by improper means, or
(b) his disclosure or use constitutes a breach of confidence reposed in him by the other in disclosing the secret to him, or
(c) he learned the secret from a third person with notice of the facts that it was a secret and that the third person discovered it by improper means or that the third person's disclosure of it was otherwise a breach of his duty to the other, or
(d) he learned the secret with notice of the facts that it was a secret and that its disclosure was made to him by mistake.

RESTATEMENT OF TORTS § 757 (1939).

42. In ruling that state laws for the protection of trade secrets are not preempted by the federal patent law, the Supreme Court cited this Restatement section in Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 474-76 (1974).

43. RESTATEMENT OF TORTS § 759 (1939) states: "One who, for the purpose of advancing a rival business interest, procures by improper means information about another's business is liable to the other for the harm caused by his possession, disclosure or use of the information."

44. See RESTATEMENT OF TORTS § 757, Comment f (1939), supra note 39.
changes employers to wipe clean the slate of his memory,"\textsuperscript{45} this maxim applies only as long as there is no breach of confidence by the former employee. However, a breach may occur in several ways. An employee may be disloyal at heart and commit larceny of tangible computer hardware by his own hand.

In \textit{Sperry Rand Corp. v. Pentronix, Inc.},\textsuperscript{46} Sperry Rand began research and development in 1954 on a process for making magnetic memory cores for use in computers. By 1962, commercial production began at its UNIVAC plant in suburban Philadelphia. During the development, Sperry Rand had its project employees sign a confidential agreement not to disclose any trade secrets or other proprietary information learned during the course of the employment. In late 1966 and early 1967, officers of a small competitor, Pentronix, met with and offered three of Sperry Rand's top employees a higher salary and a profit-sharing plan that amounted to approximately four times their present salary. The trio accepted Pentronix's offer and tendered their resignations to Sperry Rand. Before leaving, however, they photocopied 668 pages of progress and technical reports and 420 pages of engineering bulletins. They also took a certain circuit diagram design and a set of model cores. Finally, other employees observed them toting out briefcases and cardboard boxes full of undetermined documents. Five months after the resignations were effective, Pentronix began commercial sales of sixteen different magnetic memory cores substantially identical to those cores that Sperry Rand had taken eight years to develop. Sperry Rand sued the three former employees for breach of contract and Pentronix for unfair competition. Citing the Restatement of Torts section 757,\textsuperscript{47} the court found that the former employees had misappropriated trade secrets, that the competitor was engaging in a conspiracy with the individual defendants, and that, as a result thereof, Sperry Rand had been irreparably harmed. A permanent injunction was issued against Pentronix's manufacture of the cores and damages for lost profits were awarded to Sperry Rand.

An employee may also be disloyal at heart and commit larceny of intangible computer technology by carrying out trade secret information in his mind. In \textit{Sperry Rand Corp. v. Rothlein},\textsuperscript{48} Rothlein approached Sperry Rand in 1953 about going into the business of manufacturing semiconductors for use in computers. Sperry Rand agreed and hired Rothlein to head a re-

\textsuperscript{47} Id. at 913.
search and development division on Long Island, New York. In 1956, the division was moved to Norwalk, Connecticut, and commercial production began. In the meantime, Rothlein, as did each new employee, signed an agreement not to divulge any trade secret to any unauthorized person during or after his term of employment.

Early in 1959, Sperry Rand reorganized the semiconductor division and appointed Sittner as Rothlein's superior. Because this appointment was made without prior consultation with Rothlein, and because of other difficulties with Sperry Rand's management over equipment and production performance, Rothlein decided to form his own company, National Semiconductor Corporation. For another five months, Rothlein worked for Sperry Rand while he obtained financial backing and recruited other Sperry Rand employees for the new firm. After all arrangements were completed for the establishment of National Semiconductor, Rothlein and his recruits resigned en masse from Sperry Rand and the new company went into direct competition, severely cutting into Sperry Rand's share of the market.

One month after the resignations, Sperry Rand sued Rothlein and seven of the twenty-seven other former employees who went to work for National Semiconductor, charging breach of contract and misappropriation of trade secrets. The court found that the defendants had breached their fiduciary duty to their former employer by suppressing corporate opportunities for their own advantage, inducing fellow employees to quit in order to staff their own operation, and taking and using trade secrets learned while in Sperry Rand's employ for the purpose of furthering National Semiconductor's business; all in violation of their employment contracts. Citing the Restatement of Torts section 757, the court also found that the defendants had physically taken a copy of specifications for a silicon alloy junction transistor, various drawings, and other confidential documents. The defendants vigorously contested this point. The court's statement was most interesting on the issue of mental misappropriation:

The defendants claim that the drawings used by their company, National Semiconductor Corporation, most of which were the same as and interchangeable with Sperry's drawings, were constructed, not by copying from Sperry's, but from memory. It may be and if so, it was a remarkable display of memory, for numerous measurements were in thousandths of an inch. But it does not matter whether a copy of a Sperry drawing came out

in a defendant's hand or in his head. His duty of fidelity to his employer remains the same.\textsuperscript{51}

Also, regarding employees, an employer must guard against not only the disloyal at heart but also those vulnerable to bribery and coercion through threats of harm by third parties or through blackmail because of an employee's present or past matters of personal sensitivity. Finally, simply because an employer has information that it regards as a trade secret is no assurance that a court will hold a disloyal employee accountable for any unauthorized use of such information after terminating his or her employment. An employer must take reasonable safeguards to maintain the confidentiality of a trade secret. Information cannot be a trade secret one day for purposes of muting an employee and not be a trade secret another day for purposes of obtaining new business. Confidentiality must be maintained at all times. Although it is not absolutely necessary to have employment agreements prohibiting disclosure of confidential information as in the two \textit{Sperry Rand} cases,\textsuperscript{52} an employer should be advised to have such written agreements. A failure to safeguard purported trade secrets and to have nondisclosure employment agreements can have disastrous consequences on an employer's business.

In \textit{Republic Systems \\& Programming, Inc. v. Computer Assistance, Inc.},\textsuperscript{53} a computer software business had a branch office managed by Vignola who, like the rest of its employees, had no written employment contract. Disenchanted with financial conditions and supervision by the home office, Vignola consulted his top assistants and his lawyer about forming his own company and discussed subsequent merger plans with his employer's chief competitor. As soon as the incorporation papers of the new company were prepared, Vignola mailed a letter of resignation to the home office. The resignation, sent on a Friday, was to be effective immediately. During the weekend Vignola contacted his former co-workers and offered them jobs with his new company at slightly higher salaries than they were being paid at that time. When the employer's branch office opened Monday morning, only five of the twenty-five employees arrived. On that Monday, Vignola started soliciting business from his former employer's customers, and most switched their business to him.

Four days after receiving Vignola's letter of resignation in the mail, the former employer sued Vignola for breach of fiduciary duty and for misappropriation of trade secrets, i.e., customer

\textsuperscript{51} Id. at 563.
\textsuperscript{52} See notes 46 \\& 48 supra.
\textsuperscript{53} 322 F. Supp. 619 (D. Conn. 1970), aff'd per curiam, 440 F.2d 996 (2d Cir. 1971).
lists. The district court dismissed the employer's action. The court ruled that the fiduciary duty ended when the employment ended and that, since there was no written contract between the parties, each employee was "entitled to terminate the employment relationship at will at any time with or without cause."\textsuperscript{54} Citing the Restatement of Torts section 757, comment b,\textsuperscript{55} the court also ruled that customer lists did not qualify as trade secrets because many of the clients were openly listed in advertising brochures as "representative clients" and "efforts to keep the names of the remainder secret were meager at best."\textsuperscript{56} The court of appeals affirmed the district court's opinion with one judge dissenting.\textsuperscript{57}

**Customers**

Secrecy in the industry is ordinarily maintained by software owners through nondisclosure clauses in leases with customers for the computer programs.\textsuperscript{58} These written agreements allow owners to seek money damages in court through breach of contract actions for any unauthorized disclosures made by lessees of the trade secret.

For example, in *Data General Corp. v. Digital Computer Controls, Inc.*,\textsuperscript{59} a manufacturer sold small general-purpose digital computers. Ordinarily, the logic or design drawings of the machine were not included in the sale; however, if a customer wanted to make its own repairs rather than wait for the manufacturer's maintenance personnel to do so, the drawings would be made available at no extra cost upon signing an agreement not to disclose them to third parties. All drawings were marked with a legend that they were proprietary information and not to be used for manufacturing purposes. One customer sold everything, including the design drawings, to one of the competitors of the computer manufacturer. The competitor used the drawings as the basic design for a new model.

The manufacturer sought a preliminary injunction against the use of its drawings and the competitor filed a motion for

\textsuperscript{54} 322 F. Supp. at 625-26.
\textsuperscript{55} Id. at 628. See note 19 supra.
\textsuperscript{56} 322 F. Supp. at 628.
\textsuperscript{57} 440 F.2d 996 (2d Cir. 1971).
\textsuperscript{58} Software is usually not sold by its owners because control over its subsequent use is necessarily lost by a sale. To attempt to maintain control of use after sale would be a violation of Sherman Antitrust Act § 1, 15 U.S.C. § 1 (1970), as amended by Act of December 21, 1974, Pub. L. No. 93-528, § 3, 88 Stat. 1708, as an unreasonable restraint on commercial trade. Only by retaining title to the software may an owner condition its continuing use by a lessee on perpetual nondisclosure to third parties.
summary judgment. The state chancery court denied both motions. Apparently, because the manufacturer sold the computer, making it generally available to the public for reverse engineering purposes, the court denied the motion for a preliminary injunction. The court considered the manufacturer entitled to an injunction only for that period of time determined to be necessary for the competitor to reverse engineer the computer without the drawings. Since the term of the injunction during the court proceedings might extend beyond that period needed for successful reverse engineering, the court decided not to grant any injunction. However, because the manufacturer had taken some precautions to protect the design drawings as trade secrets, the court denied the competitor's motion for summary judgment. The conclusion was that the adequacy of the precautions was a factual dispute preventing summary judgment. Ten months later, the state supreme court affirmed the chancery court, citing the Restatement of Torts section 757.

Also, an owner must guard against not only those customers who obtain the trade secret legally and later sell it for their own monetary gain when the opportunity comes, but also customers who approach the owner and initially misrepresent their intentions for the sole purpose of obtaining the trade secret to sell or otherwise dispose of it for their own gain. Such activity suggests criminal acts of deceit and taking property under false pretenses.

**Competitors**

In protecting its trade secrets, a software owner should design safeguards mainly against discovery by direct competitors. However, as indicated above, those safeguards can be breached by a competitor via the instrumentality of employees and customers. In an industry where high intellect and low capital are the only requirements to enter the marketplace, it is no surprise that the competition is fierce and occasionally sinks to the most unscrupulous level. The unfair methods of competition practiced in the software industry by competitors today have taken an interesting twist from those of unfair competition in the traditional sense. In the latter type of practices, a competitor sold its own goods as those of another—commonly known as "palming off."

Today in the software industry, a competitor, as a result of a misappropriation of a trade secret, sells or leases another's goods or information as its own. However, since most software arrangements are leases and most of these are made in confidence, it is difficult for one to learn when a competitor has mis-

60. 297 A.2d at 436.
61. Id. at 439.
appropriated one's trade secrets. This is true even if both approach the same prospective customer. Unless the customer has the highest moral standards, the customer will usually stand mute when the same computer program at substantially different prices is offered confidentially by two competitors, because it is in the financial interest of the customer to remain silent and accept the lower offer.

Although there is a constant fear in the software industry about espionage, conspiracies, burglaries, malicious destruction of property, and other types of sabotage by competitors, the number of cases exposed is far less than one would expect for an industry that fluctuates so widely at times in its number of market participants. However, there is one leading case that is significant because of the amount of money involved. The owner survived simply because it was big enough to absorb the losses.

In *Telex Corp. v. IBM Corp.*, Telex sued IBM for violating the Sherman Antitrust Act by monopolizing the market in plug compatible peripheral products attachable to central processing units for IBM computers. IBM counterclaimed for misappropriation of trade secrets relating to the pertinent technology. In the manufacture of plug compatible peripheral products, IBM had about thirty-five percent of the market and earned about 1.14 billion dollars in 1970. All its combined competitors earned slightly less that 100 million dollars. About this time, one competitor in this computer products sub-market, Telex, embarked upon a systemic plan to lure away key employees of IBM. In 1970, only one of its fifty engineers had worked for IBM but, by 1973, 152 of its 1,929 employees were ex-IBM personnel. The recruits were offered substantially higher salaries, stock options, and bonuses, in one case up to one-half million dollars and were encouraged to take out all the confidential information and trade secrets they could before they left IBM's employment. As a result of this piratical activity, Telex was able to reduce significantly its development time on many projects, in one case from five to one and one-half years. Also, it was able to save signi-

---

62. Recall that in Hancock v. State, 402 S.W.2d 906 (Tex. Crim. App. 1966), supra notes 26-33 and accompanying text, the customer, Texaco Oil, reported to TI an offer by Hancock to sell the same program for five million dollars that TI said was worth only two and one-half million dollars. Query: Would the case have come to light if the offer by Hancock to sell was for one and one-quarter million dollars or less?
63. 510 F.2d 894 (10th Cir. 1975), cert. dismissed, 423 U.S. 802 (1975).
64. * This issue in the case will not be discussed because it is irrelevant to the subject matter of this article.
65. 510 F.2d at 899.
66. Id. at 900.
67. Id.
68. Id. at 910.
69. Id. at 911.
70. Id.
significantly on costs, as much as ten million dollars on the same pro-
ject and seven and one-half million dollars on another project.\textsuperscript{71}
On the counterclaim, the trial court awarded 20.9 million dollars
actual damages and assessed one million dollars punitive dam-
ages.\textsuperscript{72} The court of appeals affirmed the decision but reduced
the amount of actual damages to seventeen and one-half million dollars.\textsuperscript{73}

\textit{Joint Venturers}

A common practice, an outgrowth of the highly competitive
nature of the computer software industry, is the joint venture
in which several small competitors pool resources and assist each
other in carrying out their separate services. However, when one
company gets desperate, financially or otherwise, as sometimes
happens, there is a falling out between the parties. Such disagree-
ments often lead persons to commit acts which they would not
have considered in better times and, as has been the case from
the time of Caesar, a stab in the back has been known to be
delivered by a former friendly hand. Consider the following two
cases.

In \textit{Com-Share, Inc. v. Computer Complex, Inc.},\textsuperscript{74} two finan-
cially struggling software development companies entered into
a technical exchange agreement in 1967. After differences arose
between the parties, the agreement was prematurely terminated
in 1970. The agreement had provided that neither party could
disclose the exchanged trade secrets to third parties without prior
written consent of the other for a period of twenty-four months
after its expiration. However, nine months after the termination,
Computer Complex announced that it was selling out substan-
tially all of its assets to a larger competitor of Com-Share. The
former joint venturer sued for an injunction against the sale of
its exchanged trade secrets. The defendant contended that the
duty not to disclose ended when the agreement was terminated
by mutual consent and that the injunction would be an idle ges-
ture because the transfer of the software trade secrets had begun
and "the omelet cannot be unscrambled."\textsuperscript{75} The court was "not

\textsuperscript{71} Id.

\textsuperscript{72} Id. at 928.

\textsuperscript{73} Id. at 933. It was learned from the lead counsel for IBM that
his client never collected a penny on the judgment. After Telex filed
documents with the Securities & Exchange Commission stating that it
would be unable to pay, the parties entered into an overall settlement
whereby IBM gave up the right to pursue collection. Letter from
Thomas D. Barr, Esquire to the author (September 28, 1976). Certiorari
to the United States Supreme Court was dismissed after the settlement
agreement was finalized. Telex Corp. v. IBM Corp., 423 U.S. 802 (1975).

\textsuperscript{74} 338 F. Supp. 1229 (E.D. Mich. 1971), aff'd per curiam, 458 F.2d
1341 (6th Cir. 1972).

\textsuperscript{75} 338 F. Supp. at 1239.
persuaded that modern technology has withered the strong right arm of equity" and ruled that the disposition of the assets would unjustly enrich the defendant at the expense of Com-Share. A preliminary injunction was issued and affirmed by the court of appeals.

A more complicated fact situation involving joint venturers and a disloyal employee arose in *University Computing Co. v. Lykes-Youngstown Corp.* In 1969, a small computer service company, University Computing Co. (hereinafter UCC), and a large holding company, Lykes-Youngstown Corp. (hereinafter LYC), entered into a joint venture agreement whereby a new company, Lykes/UCC, was formed to open new markets for computer systems. UCC was to provide management and LYC was to post capital. A UCC officer, Shinn, became president of Lykes/UCC, but advised LYC that, if it formed its own wholly-owned subsidiary, chances for commercial success would be substantially the same but at a better rate of return on its capital. Consequently, LYC terminated the joint venture agreement after only two months existence and established a subsidiary, Lykes-Youngstown Computer Services Corp. (hereinafter LYCSC), with Shinn as its president. Shortly thereafter, LYCSC bribed an employee of a UCC customer in order to steal the computer tapes and materials incident to a computerized retail inventory control system leased by UCC subject to a restrictive use agreement. LYCSC then began marketing the system in direct competition with UCC. UCC sued LYC, LYCSC, and Shinn for misappropriation of the computerized system. Citing the Re-statement of Torts section 757, the court of appeals affirmed the jury verdict for UCC that the computerized system was a trade secret wrongfully appropriated by the three co-defendants.

**Suggestions for Protecting Computer Software Against Methods of Unfair Competition**

Although there is no assured way to protect one's computer software against a determined enemy, a number of routine security precautions should substantially decrease the chance of inadvertent damage or losses and increase the likelihood of detection and apprehension of any ill-meaning culprits.

First, access to the computer and its material storage areas should be well controlled. Casually parading business visitors

---

76. *Id.*
77. 504 F.2d 518 (5th Cir. 1974).
78. *Id.* at 534.
79. *Id.* at 535.
and members of the general public on good will tours may result in the loss of a seemingly inconspicuous piece of hardware or software as a surreptitiously taken souvenir. Duplicate or even triplicate files of all card decks, tapes, and other tangible material should be maintained in separate storage areas, preferably remotely located from each other in individual fireproof safes or vaults. These are inadvertent losses that may be easily avoided by simple safety measures.

It is more difficult to protect one's computer software against deliberate abuse. However, a number of safeguards may be invoked particularly directed toward monitoring the activities of employees who, as was pointed out above, are the major perpetrators of trade secret misappropriations. The safeguarding process should begin before the potential employee is hired by conducting an extensive screening of the person's background. Nothing less than a check with the FBI for past criminal activity may be satisfactory. At the moment of hiring, an employment contract with a clause forbidding the disclosure of trade secrets should be presented for the prospective employee's signature. The clause should be carefully and forcefully explained in order to impress upon the person the seriousness of any violation and the resulting civil and criminal penalties. After the employee is hired, one way to keep him or her honest is to pay a high salary with generous bonuses and merit raises for good work. Since most employees that have become disloyal did so for more money, this practice, although applicable to any industry, takes on added significance in the computer field where the detection of misappropriation of trade secrets is quite difficult.

It is advisable that a password be developed for allowing direct access to the computer by only those employees who need to have such access. This password should be changed periodically so that former employees who no longer need access cannot obtain it at their pleasure or relay an effective password to the unscrupulous. A rewards policy for any employee who reports suspicious activity or unusual operating procedures by a co-employee that turns out to be justified creates an effective internal system of checks and balances. Finally, a periodic and unannounced random accounting and/or run of computer software by selected employees would also serve as an internal security procedure.

Some employees may object to such strict security measures on grounds that they create a work atmosphere of fear and sus-

80. Allen, Danger ahead! Safeguard your computer, 46 HARV. BUS. REV. 97, 100 (1968).
81. Id. at 100-01.
picion. The natural answer to the objection is that only employees who have anything to fear are those who have something to hide. After all, the employer is in a high risk business and must be vigilant with such an intangible as computer software. Likewise, the employer's attorney must not be ignorant of the pitfalls facing the client before and during its venture into the dark and treacherous business world of computer software technology.