
Vytas M. Rimas
TRADE SECRET PROTECTION OF
COMPUTER SOFTWARE†

I. INTRODUCTION

Intellectual property may be legally protected under patent, copyright, or trade secret law. Trade secret law originated from the tort of unfair competition.¹ Patents and copyrights are solely governed by federal statutes, whereas the law of trade secrets developed from the common law. “Maintenance of standards of commercial ethics and the encouragement of invention are the broadly stated policies behind trade secret law.”²

In 1939, the First Restatement of Torts (“Restatement”) was published. Three sections were devoted to trade secret principles³ from which subsequent case law has evolved. Virtually every state and all federal jurisdictions have adopted the Restatement's principles.⁴ Reporters of the Second Restatements of Torts omitted numerous sections of the original Restatement, because trade secrets had evolved into an independent body of law encompassed by unfair competition and trade regulation.

Recently, the Uniform Trade Secrets Act (“Uniform Act”) was adopted by the Commissioners on Uniform State Laws at their 1979 Annual Conference.⁵ The Uniform Act codified the basic principles of common law trade secret protection, preserving its essential distinctions from patent law.⁶ The new act was needed because state trade secret law had developed unevenly and the most widely accepted rules of trade secret law were omitted from the Second Restatement of Torts.⁷ The Uniform Act has been enacted in Connecticut, Delaware, Indiana, Kansas, Louisiana, Minnesota and Washington.

† Awarded National Second Place in the Computer/Law Journal's First Annual Computer Law Writing Contest.
3. RESTATEMENT (FIRST) OF TORTS §§ 757-59 (1939).
4. 12 MILGRAM, TRADE SECRETS § 2.01, at 2-3, n.2 (Supp. 1982).
5. UNIF. TRADE SECRETS ACT (1980).
6. Id. at 537-51.
7. Id.
II. NATURE OF TRADE SECRETS

A. TRADE SECRET DEFINED

All federal jurisdictions and twenty five states, including California, follow the Restatement's expansive definition of a 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 of use it. It may be a formula for a chemical compound, a process of manufacturing, treating or reserving materials, a pattern for a machine, or a list of customers.

The Uniform Trade Secrets Act updates the definition of a trade secret, providing that:

"Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(1) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and

(2) is the subject of efforts that are reasonable under the circumstances to maintain secrecy.

The Uniform Act departs from the definition in the Restatement that requires a trade secret to be "continuously used in one's business." The Act's broader definition extends protection to a plaintiff who has not yet had an opportunity or acquired the means to put another's trade secret to his own use.

B. SCOPE OF PROTECTION

With some variations among jurisdictions, trade secrets have been used to protect computer databases, software, hardware, and firmware. Databases are collections of discrete data, being analogous to customer lists. Since lists lack the element of novelty, some courts treat lists differently from technological trade secrets.

Unlike patent law, trade secret law protects computer software. Computer software is commonly differentiated into: (1) the underlying process or algorithm upon which the program is based; (2) the program itself coded in some programming language; and (3) the supporting documentation including items such as flow-charts, in-
construction manuals, and other materials that explain the operation of the program.\textsuperscript{14}

\textit{Bleth v. Insurance Department}\textsuperscript{15} illustrates the broad scope of protection available under trade secret law. In that case the insurance company's computer programs, math models, procedures, and statistical assumptions were held to be protected trade secrets.

Unlike copyrights, trade secrets cover computer hardware—the actual computer and associated peripheral equipment. Trade secrets are commonly used to protect an invention that has not yet been granted a patent or is not patentable, e.g., for insufficient novelty.\textsuperscript{16} Examples of hardware found to be trade secrets include semiconductors,\textsuperscript{17} high speed data acquisition modules,\textsuperscript{18} disc drives and disc packs,\textsuperscript{19} microprocessors,\textsuperscript{20} and minicomputers.\textsuperscript{21}

A trend in the computer industry has been the proliferation of firmware. Firmware has been defined as micro-instructions permanently embodied in hardware elements.\textsuperscript{22} Firmware was protected under both copyright and trade secret law in the California memorandum decision of \textit{GCA Corp. v. Chance}.\textsuperscript{23} The object code was in chip form as an E-PROM (Electrically Programmable Read Only Memory). The first and last twenty five pages of the long source code were registered with the copyright office. The registration did not disclose the workings of the diagnostics and operating system programs, and the program trade secrets were not destroyed.

\textbf{C. Restatement's Six Tests}

Factors relevant in finding a trade secret are set forth in the Restatement:

\begin{enumerate}
\item [(1)] [External Secrecy]—the extent to which the information is known outside the business;
\item [(2)] [Internal Secrecy]—the extent to which it is known by employees and others involved in the business;
\end{enumerate}

\textsuperscript{15} 95 Misc. 2d 18, 406 N.Y.S.2d 649 (Sup. Ct. 1977).
\textsuperscript{17} Sperry Rand Corp. v. Rothlein, 241 F. Supp. 549 (D. Conn. 1965).
\textsuperscript{19} Forro Precision, Inc. v. IBM Corp., 673 F.2d 1045 (9th Cir. 1982).
\textsuperscript{20} Packard Instrument Co. v. Reich, 89 Ill. App. 3d 908, 412 N.E.2d 617 (1980).
\textsuperscript{22} Bradley & Franklin, 202 U.S.P.Q. (BNA) 480, 484 (C.C.P.A. 1979).
\textsuperscript{23} GCA Corp. v. Chance, No. C-82-1063 (N.D. Cal. July 12, 1982); see also, 217 U.S.P.Q. (BNA) 718.
(3) [Security Measures]—the extent of the measures taken to guard the secrecy of the information;
(4) [External Value]—the value of the information to the business and to competitors;
(5) [Investment]—the amount of effort or money expended in developing the information;
(6) [Accessibility]—the ease or difficulty with which the information could be properly acquired or duplicated by others.24

D. Novelty

One of the elements of a trade secret is the degree to which the subject matter is known or readily ascertainable by others. Generally matters of public knowledge in the industry cannot be appropriated by one as his secret.25 In Jostens, Inc. v. National Computer Systems,26 plaintiff argued that its computer-aided graphics subsystem was novel since it was the first such system in the jewelry ring business. This claim was rejected because similar graphics systems were used in other industries. The scanner and the engraving subsystems and the hardware and operating systems software all utilized technology that was both generally known and ascertainable. These were all standard vendor products that did not warrant trade secret status.27

The degree of novelty needed to reach trade secret status varies among jurisdictions. Courts agree that trade secrets lie somewhere on a continuum between that which is generally known in the field and that which has some degree of originality.28 Jurisdictions are generally in accord that a trade secret requires less novelty or originality than does a patent29 or copyright.30

Novel combinations of generally known concepts will be considered trade secrets.31 In Com-Share, Inc. v. Computer Complex,
plaintiff developed a time-sharing operating system together with a high level programming language and text editor. Defendant argued that the software was not novel. The court disagreed and reasoned:

[T]he existing software systems which are unique in the computer time sharing industry all contain certain elements which perform similar functions and many utilize certain similar fundamental concepts, of a general nature. This is no more than saying that all have a common concept, and, in the most general sense, a common base. Such is common in all engineering. Thus, the concept of vehicular locomotion, involving in one aspect, the basic principles of the internal combustion engine, is common to snowmobiles, ships, airplanes, and automobiles, but there the similarity stops.33

Plaintiff's software was held to be a trade secret since it was based upon "new principles and concepts with unique engineering, logic and coherence."34

In some jurisdictions novelty or uniqueness is not a requirement for trade secret protection.35 In Structural Dynamics Research Corp. v. Engineering Mechanical Research Corp.,36 even though the information making up the structural analysis program was found in the literature, the program was upheld as a trade secret.

E. Secrecy

The prime prerequisite for a trade secret is secrecy.37 Secrecy need not be total; depending on the circumstances, partial or relative secrecy will suffice.38

Efforts to maintain secrecy may encompass both keeping the information in-house and keeping the information from those outside in the general trade or industry. The Com-Share court found the existence of a trade secret based on the evidence of plaintiff's security measures.39 Each page of the listings embodying plaintiff's software system was stamped with Com-Share's proprietary legend. Passwords were built into the system to prevent unauthorized access. Magnetic tapes were kept locked when not in use. In Telex v.
IBM's elaborate in-house trade secret protection program consisted of magnetic door locks, confidential legends, exit interviews with employees, nondisclosure agreements, guards, television cameras and sensors. In *Jostens, Inc. v. National Computer Systems*, the court found no trade secret, because there was evidence that plaintiff did not consider or establish a trade secret policy to keep its development secret. The court held that employees must understand that information is not to be made readily available to the trade. In *J. & K. Computer Systems, Inc. v. Parrish*, the accounts receivable program was sufficiently protected because the program bore proprietary legends and the employment agreement contained a nondisclosure covenant.

Secrecy must also be maintained if the developer chooses to license its software or enter into a joint venture with another company. For instance, in *Telex*, IBM maintained the secrecy of its diagnostic program by distributing only the source code version, while keeping the object code in its safe. In *Digital Development Corp. v. International Memory Systems*, plaintiff protected its controller design secret by following the industry practice of putting proprietary legends on instruction manuals before they were sent to customers. In *Com-Share*, the court enforced the nondisclosure clause in the technical exchange agreement entered into by the two companies. In *University Computing Co. v. Lykes-Youngstown Corp.*, the restrictive use agreement preserved the trade secret status of plaintiff's inventory control software system when abused by its joint venturer.

### F. Value

The value of the development is another characteristic of a trade secret useful in determining the measure of damages. In *Analogic Corp. v. Data Translation, Inc.*, plaintiff spent more than $100,000 over eighteen months to develop its high speed data acquisition module, compared to defendant's expenditure of $2,500 over a few months to create its facsimile. In *Computer Print Systems, Inc.*

---

41. *Id.* at 330.
42. 318 N.W.2d 691, 700 (Minn. 1982).
43. 642 P.2d 732 (Utah 1982).
44. 367 F. Supp. at 258.
46. 338 F. Supp. at 1229.
47. 504 F.2d 518 (5th Cir. 1974).
SOFTWARE TRADE SECRET PROTECTION

v. Lewis,\textsuperscript{49} plaintiff's considerable investment in and competitive advantage from its direct mail advertising program overcame the fact that the computer programs were not novel. The Uniform Act\textsuperscript{50} goes further in protecting information that has commercial value from a negative viewpoint, such as the results of lengthy and expensive research that proves that a certain process that will not work may be of great value to a competitor.

III. CHOICE OF PROTECTION

Congress created the National Commission on New Technological Uses of Copyrighted Works (CONTU) to revise comprehensively the Copyright Act of 1976.\textsuperscript{51} In 1979, the Final Report of CONTU was published. The Final Report discusses the deficiencies of trade secret law.\textsuperscript{52} First, since trade secrets are known to only a few people, and are to be kept "secret," they impede the free exchange of ideas. Second, trade secrets of general programs are not suited for mass distribution. Third, protection is readily lost if disclosure occurs. Fourth, substantial expenditures, that increase the cost of a product, are necessary to maintain a trade secret program. Last, the lack of uniformity of trade secret law leads to uncertainty. In contrast, copyright law serves those interests with which trade secrets fail to deal.\textsuperscript{53}

The primary advantages of trade secret protection are threefold. First, while patent law does not protect the patent applicant in the interim between the submission of the application and the grant of the patent, trade secret law protects the secret at the moment its underlying subject matter is created.\textsuperscript{54} Second, trade secret protection for software protects a greater range of subject matter than does copyright protection. Trade secret law may protect ideas, procedures, processes, systems concepts, principles and discoveries irrespective of the form of expression, whereas copyright protects only the form of expression.\textsuperscript{55} Finally, criminal sanctions exist to punish those who willfully infringe a copyright or misappropriate a trade secret.\textsuperscript{56}

The burgeoning software industry is the area of the computer

\textsuperscript{50} UNIF. TRADE SECRETS ACT § 1 commissioner's comment (1980).
\textsuperscript{52} NATIONAL COMMISSION ON NEW TECHNOLOGICAL SOURCES OF COPYRIGHTED WORKS, FINAL REPORT 17 (1978) [hereinafter CONTU, FINAL REPORT].
\textsuperscript{53} Id. at 19.
\textsuperscript{54} Id.
\textsuperscript{55} Id. at 17.
\textsuperscript{56} ROSE, PROTECTING TRADE SECRETS 352-78 (1981).
sector that is most in need of legal protection. The total software investment in the United States is on the order of $100 billion and the industry is still in its infancy. Trade secrets are the predominant form of protection for computer software. An estimated one million programs are developed annually. Between 1964 and 1976 only 1205 programs had been registered for copyright, and of these IBM and Burroughs accounted for 911. From 1976 to 1980, 2000 programs were registered. The fact that many more programs are created then are registered for copyright supports the view that trade secrets are the primary form of software protection.

IV. PREEMPTION

Since a trade secret claim is based on state law, it might be challenged on the grounds that it is preempted by federal law and the Patent-Copyright Clause in the Constitution, under the Supremacy Clause. Under the doctrine of federal preemption, where Congress enacts copyright and patent protection for industrial property, the states cannot enact laws that are in conflict with or defeat the purposes of the federal legislation.

A. BY PATENT LEGISLATION

Until 1974, the issue of whether federal patent law preempted state trade secrets law remained unresolved. In 1974, however, the Supreme Court held in *Kewanee Oil Co. v. Bicron Corp.* that patent law does not preempt the law of trade secrets. Thus, until Congress takes action to the contrary, states are free to grant protection to trade secrets. Kewanee Oil Co. sought to enjoin its former employees from using or disclosing the trade secrets associated with a synthetic crystal used in detecting ionizing radiation. The Court reviewed the objectives of trade secret and patent law and found no conflict between them; the Constitutional objective behind the Patent-Copyright Clause is to "promote the Progress of Science and the Useful Arts." Patent laws promote this progress by offering a right of exclusion for a limited period as an incentive to invent. This benefits the society through introduction of new products and

57. *Id.*
59. ROSE, *supra* note 56.
60. U.S. CONST. art. I, § 8, cl. 8.
61. U.S. CONST. art. VI, cl. 2.
63. *Id.*
64. *Id.* at 480-84.
processes, in exchange for the right of exclusion. The trade secret policies include the maintenance of standards of commercial ethics and the encouragement of inventions.\textsuperscript{65}

The Supreme Court delineated three categories of trade secrets.\textsuperscript{66} The first and second categories encompass nonpatentable subject matter and subject matter of dubious patentability, and are appropriate for trade secret protection.\textsuperscript{67} The third category includes subject matter that is clearly patentable. Here the federal interest prevails. If a state's system of protection causes a substantial risk that holders of patentable inventions may seek only trade secret rather than patent protection, that system may be found unconstitutional. The court held there was no such risk under the present trade secret law; therefore, trade secret protection is extended to clearly patentable inventions.\textsuperscript{68}

\section*{B. By Copyright Legislation}

While the majority view holds that copyright law does not preempt trade secret law, a minority view holds that trade secrets are preempted by copyright law. In \textit{Synercom Technology, Inc. v. University Computing Co.},\textsuperscript{69} the district court held that where input formats embodied only an idea, they were unprotected by trade secret law. Texas' law of misappropriation is preempted by federal law and its policy of disclosure of and free access to ideas.\textsuperscript{70} The court distinguished \textit{Kewanee} from \textit{Synercom} in that in the former case the state interest in enforcing trade secret law is more compelling where theft of secrets or industrial espionage is involved. On the other hand, in \textit{Synercom}, the interest involved was the competitor's design of a structural analysis package that was to be compatible with plaintiffs input methodology.\textsuperscript{71}

The prevailing view is that the copyright law does not preempt trade secrets. In \textit{Technicon Medical Information v. Green Bay Packaging},\textsuperscript{72} decided under the 1909 Copyright Act, the court held that trade secret law was not preempted by copyright law, because there was no inherent conflict between the Copyright Act and state trade secret law. The court in \textit{Warrington Associates v. Real-Time Engi-

\begin{itemize}
\item \textsuperscript{65} \textit{Id.} at 480-82.
\item \textsuperscript{66} \textit{Id.} at 484.
\item \textsuperscript{67} \textit{Id.} at 484-89.
\item \textsuperscript{68} \textit{Id.} at 489.
\item \textsuperscript{69} 474 F. Supp. 37 (N.D. Tex. 1979).
\item \textsuperscript{70} \textit{Id.} at 43.
\item \textsuperscript{71} \textit{Id.} at 42.
\item \textsuperscript{72} 687 F.2d 1032 (7th Cir. 1982), \textit{cert. denied}, 103 S. Ct. 732 (1982).
\end{itemize}
neering Systems,73 interpreted the 1976 Copyright Act74 as not pre-
empting trade secret law because the claims are not equivalent. Copy-
right protects only the author's particular expressions, whereas trade secret protection extends to the very ideas of the author.

In M. Bryce & Associates, Inc. v. Gladstone,75 the court reviewed
the 1976 Copyright Act and found that Congress had not intended to
preempt trade secret law with copyright law.76 The plaintiff claimed
that its management information systems methodology had been
misappropriated. The court found the demarcation between trade
secret and copyright protection clear: trade secret law protects con-
tents irrespective of the form of expression, whereas copyright law
protects the form of expression but not the underlying idea.77

Finally, Representative Robert Kastenmeier has introduced
H.R. 6983,78 a bill designed to improve the protection of computer
software. If the bill were adopted, subsection “(e)” would be added
to 17 U.S.C. § 301, clarifying the preemption issue as follows:
Nothing in [Title 17] shall alter or limit any right or remedy which
the owner of a copyright may have under State trade secret law
that is not equivalent to any of the exclusive rights within the gen-
eral scope of copyright as specified by section 106.

This proposed subsection would be the first express statement of
Congressional intent regarding trade secret preemption.

V. PROPRIETARY RIGHTS

The ownership of a trade secret does not give the owner a mo-
nopoly in its use, as with a patent, but merely a proprietary right
that equity protects against usurpation by unfair means.79 When
the employer-employee relationship ends, the issue arises as to
which employment-gained information or know-how a former em-
ployee is free to use and disclose to others. Nondisclosure obliga-
tions may be imposed on the employee by both state trade secret
law and agreement. The employer may go further and wish to cre-
ate a covenant not to compete, in order to protect itself from future
competition by an ex-employee.

---

76. Id. at 259, 319 N.W.2d at 916.
77. Id. at 258, 319 N.W.2d at 915.
    (1962).
A. Policies

The existence and extent of any duty is influenced by competing policies; the protection of an employer's interest in its development versus the protection of an employee's job mobility. These policies, as set forth in *Wexler v. Greenberg*, are often cited by courts in reaching their determination of whether to allocate the proprietary rights in a development to the employer or employee. The *Wexler* court reasoned that society benefits from technological improvements; without some means of post-employment trade secret protection, a company could not afford to subsidize research or improve its current operating methods. On the other hand, society and the employee have an interest in preserving the job mobility of skilled employees; an employee should not be restrained from advancing further in the industry in which he is most productive because of his increased expertise. Former employees will become less attractive to new employers as their acquired skills and knowledge become regarded as trade secrets. The result will be diminished competition and dissemination of ideas.

B. Employee-Developer

It is often necessary to determine who owns the software before the issue of liability is reached. Most software is developed in a multiparty, employer-employee environment. Where the employee originates or develops the software, the question arises as to whether the ownership rights vest exclusively in the employer or the employee.

In *Structural Dynamics Research Corp. v. Engineering Mechanical Research Corp.*, two employees developed a general purpose isoparametric computer program. The court found that the former employees had a proprietary interest in the program at least equal to that of their employer, because it was the employees' initiative and innovation that brought the trade secret into being. The court stated that, absent an express contractual obligation not to disclose, an employee is free to use or disclose the confidential information in subsequent employment. In this case, however, a confidentiality agreement was found to exist and the former employees were ordered to pay to the employer a fifteen percent royalty over three

---

In *Amoco Production Co. v. Lindley*, the employer wanted to enjoin the use of a well log analysis program developed by the former employee. The court reviewed prior cases and found that courts balance the equities between the employer and the employee. Among the factors delineated by the court was the degree to which the company's resources, such as time, facilities, and money, were used. The court implicitly recognized that both the employer and employee had proprietary rights in the program, and refused to enjoin the former employees from disclosing or using the software.

California's proprietary statute governing inventor-employees sets forth the standards required for protection. Any attempt by an employer to contract away an employee's interest in a qualified invention is void as against public policy, as stated in Labor Code section 2870:

Any provision in an employment agreement which provides that an employee shall assign or offer to assign any of his or her rights in an invention to his or her employer shall not apply to an invention for which no equipment, supplies, facility, or trade secret information of the employer was used and which was developed entirely on the employee's own time, and (a) which does not relate (1) to the business of the employer or (2) to the employer's actual or demonstrably anticipated research or development, or (b) which does not result from any work performed by the employee for the employer. Any provision which purports to apply to such an invention is to that extent against the public policy of this state and is to that extent void and unenforceable.

In *GCA Corp. v. Chance*, former employees of the plaintiff were enjoined from using plaintiff's diagnostic system program in their business of repairing plaintiff's silicon wafer processing machines. The district court's memorandum decision rejected defendant's section 2870 defense, holding that the persons that the section intended to protect are inventors, and defendants were not the inventors of the system.

**C. Employee-Nondeveloper**

The information that an employee who did not develop the software can disclose or utilize upon leaving his employer varies among jurisdictions. An employee may take with him general skills

---

84. *Id.* at 1111-20.
85. 609 P.2d 733 (Okla. 1980).
86. *Id.* at 745-47.
88. No. C-82-1063 (N.D. Cal. July 12, 1982); *see also* 217 U.S.P.Q. (BNA) 718.
In *Packard Instrument Co. v. Reich*, defendant, a former director of research, had access to his employer's research and marketing information concerning microprocessor controlled liquid scintillation equipment. The evidence showed that the microprocessor expertise came from an independent consultant and from defendant's attendance at a public seminar. Further, based on the evidence, the court found that plaintiff failed to establish any proprietary right to the instruments. The court also found that since an employer's non-disclosure agreement is ineffective if there is no trade secret to be disclosed, and the subject matter involved in the case was generally known to people in the trade, plaintiff could not prevail.

California's proprietary statute grants the employer all rights to its developments. An employee has no rights in what he has "acquired" from his employment, as stated in Labor Code section 2860:

> Everything which an employee acquires by virtue of his employment, except the compensation which is due to him from his employer, belongs to the employer, whether acquired lawfully or unlawfully, or during or after the expiration of the term of his employment.

In *King v. Pacific Vitamin Corp.*, the court interpreted section 2860 consonantly with the established rule that business information acquired by an employee that is not confidential in fact or by agreement is not protectable property of the employer. The right of the employer to protection is derived from the fact that the information is secret and not from the mere fact that it came to the employee in the course of his employment.

**D. COVENANT NOT TO COMPETE**

In some jurisdictions an employer may protect its proprietary interest in a trade secret by including a covenant not to compete within an employment or post-employment agreement. Courts do not favor noncompetition covenants, and require the covenants to be reasonable.

In Massachusetts, a covenant restricting trade or competition will be enforced if it is reasonably limited in time and space, and does not conflict with the public interest. In *Modern Controls, Inc.*

---

90. 89 Ill. App. 3d 908, 412 N.E.2d 617 (1980).
91. Id. at 916-17, 412 N.E.2d at 622-23.
93. 256 Cal. App. 2d 841, 64 Cal. Rptr. 486 (1967).
94. Id. at 849, 64 Cal. Rptr. at 490.
v. Andreadakis Translation, Inc., the Eighth Circuit enforced a covenant not to compete, because the covenant was supported by independent consideration. The noncompetition covenant was supported by the employer's obligation to pay the employee his base pay for two years if the employee could not find suitable work. In J. & K. Computer Systems, Inc. v. Parrish, liquidated damages for joining a competing company was part of the employment agreement. The employer was to receive one thousand dollars for each year that the employee was employed by plaintiff. This sum represented the value of the training and information received by the employee from his employer. On this basis the Utah Supreme Court enforced the noncompetition covenant.

In other jurisdictions, covenants not to compete are unenforceable. In Structural Dynamics Research Corp. v. Engineering Mechanical Research Corp., an "Employee Patent and Confidential Agreement" included noncompetition and nondisclosure provisions. Under Michigan law the noncompetition covenant was invalid; therefore, the court could only enforce the covenant not to disclose.

California has a strong public policy against unfair competition, described in Business and Professional Code section 16600: "Except as provided in this chapter, every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void." In the cases of Winston Research Corp. v. Minnesota Mining & Manufacturing Co. and Cyberteck Computer Products, Inc. v. Whitfield the courts held that the noncompetition provisions within the employment agreements were invalid under section 16600. The nondisclosure provisions prohibiting an employee from disclosing confidential information were enforceable, however, because these provisions did not come under section 16600.

Thus, an employer should draft its nondisclosure provisions narrowly to avoid invalidation. Even a covenant tailored to protect only an employer's trade secrets may run afoul of the policy against restraining competition. A programmer's specialized experience may

96. 578 F.2d 1264 (8th Cir. 1978).
97. Id. at 1268.
98. 642 P.2d 732, 736 (Utah 1982).
100. Id. at 1115.
102. 350 F.2d 134 (9th Cir. 1965).
104. Id. at 1022.
limit the ex-employee's job opportunities solely to competitors of the former employer. A court may void the nondisclosure covenant for restraining competition, interpreting it to be a covenant not to compete.

VI. LIABILITY

A. THEORIES OF LIABILITY

Once the trade secret is established, liability can be established by the manner in which the trade secret was obtained, the relationship between the parties, or the degree of notice to or knowledge by the recipient. The theories of liability are directed toward the trade secret policy of maintaining the standards of commercial ethics. The bases for liability are set forth in the First Restatement of Torts, section 757:

One who discloses or uses another's trade secret, without a privilege to do so, is liable to the other if:

(a) [Misappropriation]—he discovered the secret by improper means; or

(b) [Breach of Confidence]—his disclosure or use constitutes a breach of confidence reposed in him by the other in disclosing the secret to him; or

(c) [Knowing Receipt]—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) [Known Mistake]—he learned the secret with notice of the facts that it was a secret and that its disclosure was made to him by mistake.

Misappropriation theory has its basis in tort. One is liable for obtaining another's trade secret by "improper means." In Telex v. I.B.M., Telex's means of misappropriation involved luring away IBM employees possessing knowledge of the trade secret by offering them substantial salary increases and bonuses. Criminal liability may be incurred for egregious misappropriation such as theft, bribery, and espionage. The manner of misappropriation is not limited to a physical taking or copying of the trade secret; misappropriation may occur by memory alone. In Sperry Rand Corp. v. Rothlein, 108

106. Restatement (First) of Torts § 757 (1939).
a former employee who memorized his employer's drawings of semiconductors was found liable for misappropriation.

An alternative basis for liability is breach of confidence, which sounds in contract and implied contract law. It is the most common basis for finding liability with respect to software. The requisite secrecy restricts access to the trade secret to individuals in a position of trust with the developer. A confidential relationship can be created by either employment, contract, license, or agency. Non-disclosure and nonuse covenants are commonly employed to create contractual confidential relationships and to delineate the obligations flowing therefrom. In *University Computing Co. v. Lykes-Youngstown Corp.*, the defendant joint venturer was held to be liable for wrongfully appropriating plaintiff's computer system in a knowing violation of the joint venturer's restrictive use agreement. Outside the employer-employee context, absent an agreement, it is less likely that liability will be imposed and a confidential relationship implied.

Liability can attach where there has been no misappropriation or confidential relationship. In *Computer Print Systems, Inc. v. Lewis,* liability was found on the "knowing receipt" basis. An officer in plaintiff's company provided defendant, one of plaintiff's customers, backup copies of plaintiff's direct mailing programs with machine code instructions. Subsequently, the officer went to work for defendant. The court held that defendant was liable for the trade secret infringement at the time the officer was hired. It was irrelevant that defendant initially obtained the backup copies innocently.

The scope of liability under the Restatement and Uniform Trade Secrets Act implicitly requires that the trade secret knowledge be obtained in bad faith. North Carolina recently enacted its own Trade Secrets Protection Act of 1981 which expanded the scope of liability. This act departs from the "lack of good faith" standard in certain circumstances. Thus, a good faith appropriator may

---

110. See Bender, supra note 1, at 52.
112. 504 F.2d 518 (5th Cir. 1974).
115. RESTATEMENT (FIRST) OF TORTS § 757 (1939).
116. UNIF. TRADE SECRETS ACT § 1(2) (1980).
be enjoined from using the trade secret, or if he has changed his position in reliance on the trade secret, he may be required to pay a reasonable royalty.

B. UNFAIR COMPETITION

The law governing protection of trade secrets is essentially designed to regulate unfair competition. Not infrequently, the trade secret misappropriator may incur further liability and the trade secret owner may have an alternate cause of action under unfair competition law. In *Sperry Rand Corp. v. Electronic Concepts*, plaintiff's departing employees, by conspiring to misappropriate employer's trade secret materials and data, engaged in unfair competition. The finding of unfair competition and trade secret liability together contributed to an award of punitive damages and attorney's fees to the employer.

California's unfair competition chapter is found in Business and Professionals Code sections 17200-17208. Section 17200 provides: "As used in this chapter, unfair competition shall mean and include unlawful, unfair or fraudulent business practice and unfair, deceptive, untrue or misleading advertising . . . ." In *Chicago Lock Co. v. Fanberg*, the court found no "improper means" because the code was discovered by reverse engineering; no breach of confidence existed because there was no confidential relationship. Therefore, relief was denied under the unfair competition statute, the court holding that commission of the common law tort of trade secret misappropriation is enjoinable under the purview of "unfair competition."

VII. DEFENSES

Many of the defenses to a trade secret claim go to the inherent weakness of trade secrets, including the ease with which a trade secret can be inadvertently or otherwise lost through disclosure or by another's independent origination of the same subject matter. In contrast, patents and copyrights protect their owners against such circumstances.

One who independently develops subject matter that is coexten-

121. 676 F.2d 400 (9th Cir. 1982).
122. Id. at 405.
123. CONTU, FINAL REPORT at 17-19.
sive with another's trade secret has a complete defense against a claim by the latter. \(^{124}\) Discovery by reverse engineering is a proper means to acquire knowledge of the trade secret. \(^{125}\) "Reverse engineering" is the means by which a competitor starts his investigation with the known product, and, by working backwards, discerns the method by which it was developed. \(^{126}\)

By definition, a trade secret is information that has not been placed in the public domain. When the subject matter of a trade secret is a matter of public or trade knowledge, its trade secret status is lost. \(^{127}\) The trade secret information may enter the public domain by being published in a trade journal as well as from a demonstration or display of the product; \(^{128}\) limited publication, however, does not necessarily extinguish the trade secret. In *Management Science America, Inc. v. Cyborg Systems, Inc.*, \(^{129}\) the trade secret was protected even though the payroll system was licensed to six hundred customers. The court based its decision on the fact that each prospective customer needed to sign a nondisclosure agreement as a precondition to receiving the license.

Trade secret law is widely perceived as nonsuitable for mass distributed products. \(^{130}\) Courts, however, are gradually lowering the barrier to mass distributed trade secrets, as illustrated by *Data General Corp. v. Digital Computer Controls, Inc.* \(^{131}\) Here the defendant raised the defense that the plaintiff took inadequate precautions to protect the secrets in its Nova 1200 minicomputer. Defendant claimed that as a result of plaintiff's relatively unrestricted and uncontrolled distribution of copies of its Nova 1200's logic design among customers, third party users, vendors, and trainees, almost 6000 individuals had access to the drawings. \(^{132}\) The court rejected the defense, being satisfied that plaintiff took sufficient precautions, since each distributee had agreed to abide by the provisions of the proprietary legend appearing on each diagram.

Often a trade secret claim is defended upon the basis that the trade secret has been disclosed upon the receipt of a patent grant or by the publication required by a copyright. In *Data General*, how-

---

125. UNIF. TRADE SECRETS ACT § 7 commissioner's comment (1980).
126. *Kewanee Oil Co.*, 416 U.S. at 476.
127. *Id.* at 484.
128. UNIF. TRADE SECRETS ACT § 1, commissioner's comment (1980).
130. CONTU, FINAL REPORT at 17.
131. 37 A.2d 105 (Del. Ch. 1975).
132. *Id.* at 107.
ever, the court also held that the granting of a patent for one iso-
lated part of the minicomputer did not amount to full public
disclosure, and therefore did not destroy the trade secret protec-
tion.\textsuperscript{133} In \textit{Technician Medical Information v. Greenbay Packag-
ing},\textsuperscript{134} plaintiff affixed both a proprietary legend and a copyright
notice on its systems reference manual. This dual use of copyright
and trade secret did not estop plaintiff from asserting the trade se-
cret.\textsuperscript{135} The court found this to be a "limited publication," that is,
communicated to a select group for a limited purpose, and without
the right of reproduction, distribution, or sale.\textsuperscript{136} The California
case of \textit{GCA Corp. v. Chance}\textsuperscript{137} is in accord—registering the copy-
right via the source code did not destroy the trade secrets within the
firmware.

The defense that the statute of limitations has run can also be
raised. The Uniform Trade Secrets Act has simplified matters by es-
tablishing a uniform three-year limitation on actions.\textsuperscript{138} This pre-
vents possible maneuvering under tort, property, or contract
theories that have different limitation periods.

\section*{VIII. REMEDIES}

Equitable, legal, and criminal forms of relief are available to the
trade secret holder. The jurisdictional differences in the remedies
awarded usually involve the duration of an injunction and the mea-
sure of damages. Courts and the Uniform Trade Secrets Act provide
for punitive damages and attorney's fees in relevant cases.\textsuperscript{139}

\subsection*{A. EQUITABLE RELIEF}

An injunction is the most commonly sought form of relief in
trade secret litigation.\textsuperscript{140} An action to enjoin is appropriate to pre-
vent future harm by disclosure or adverse use of the trade secret.\textsuperscript{141}

Irreparable harm is an injunctive ground for relief. In \textit{Modern
Controls, Inc. v. Andreadakis},\textsuperscript{142} defendant went to work for Bor-
roughs Corporation, a competitor of plaintiff. The Eighth Circuit
found that the lower court had erred in denying plaintiff's motion for

\begin{footnotes}
\item[133.] \textit{Id.} at 113.
\item[134.] 687 F.2d 1032 (7th Cir. 1982).
\item[135.] \textit{Id.} at 1036-37.
\item[136.] \textit{Id.} at 1036.
\item[137.] No. C-82-1063 (N.D. Cal. July 12, 1982).
\item[138.] \textsc{Unif. Trade Secrets Act} § 6 (1980).
\item[139.] \textsc{Unif. Trade Secrets Act} § 4 (1980).
\item[140.] \textit{See Milgram, supra} note 4, at § 7.08(1).
\item[141.] \textsc{Restatement (First) of Torts} § 757 (1939).
\item[142.] 578 F.2d 1264, 1270 (6th Cir. 1978).
\end{footnotes}
preliminary injunction to enforce a covenant not to compete. The court further found that it was likely that defendant would disclose trade secrets and other confidential information to Burroughs, thus giving it a competitive advantage over plaintiff who was a significantly smaller entity.\textsuperscript{143} In \textit{Com-Share, Inc. v. Computer Complex, Inc.},\textsuperscript{144} plaintiff and defendant had entered into a pooling agreement to share technological information. When defendant entered into another agreement with a third party corporation to sell its assets and goodwill, injunctive relief was granted to plaintiff. This prevented defendant from divulging any information regarding systems and technology that plaintiffs had previously supplied to defendant under the technological exchange agreement. The court found that irreparable injury and loss would result to plaintiff if the defendant were allowed to sell, transfer, or disclose the trade secret portion of the software.\textsuperscript{145} A preliminary injunction was refused to the defendant in \textit{Digital Development Corp. v. International Memory Systems}.\textsuperscript{146} Digital and IMS had embarked on a joint effort to market rotating disc memory units. The court found that there was an insufficient showing that Digital's use of IMS's controller design would do irreparable harm to IMS. Hence, IMS could only recover damages of $150,000 for Digital's wrongful appropriation of IMS' product.\textsuperscript{147}

The duration of an injunction is usually conditioned on the length of time it took to develop the trade secret or the period of time needed by a plaintiff to maintain its competitive advantage. In \textit{Analogic Corp. v. Data Translation, Inc.},\textsuperscript{148} the amount of time needed to reverse engineer the plaintiff's high speed data acquisition module was relevant in determining the reasonable duration of a final injunction. The court reasoned that defendant should not be permitted a competitive advantage from its avoidance of the normal costs of invention and duplication.\textsuperscript{149} The Uniform Trade Secrets Act sets forth the duration of injunctive relief as follows: "\textquoteright\textquoteright\textit{A}n injunction shall be terminated when the trade secret has ceased to exist, but the injunction may be continued for an additional reasonable period of time in order to eliminate commercial advantage that otherwise would be derived from the misappropriation."\textsuperscript{150}

\textsuperscript{143} \textit{Id.}
\textsuperscript{145} \textit{Id.} at 1239.
\textsuperscript{147} \textit{Id.} at 142.
\textsuperscript{149} \textit{Id.} at 649, 358 N.E.2d at 807-08.
\textsuperscript{150} \textbf{UNIF. TRADE SECRETS ACT} § 2(a) (1980).
This provision conforms the length of the injunction to the misappropriator's lead time over its competitors.\textsuperscript{151}

\section*{B. Legal Damages}

In determining the measure of damages, the court should consider the commercial setting of the injury, the likely future consequences of the misappropriation, and the nature and extent of defendant's use of the trade secret after misappropriation.\textsuperscript{152}

Plaintiff's damages may be measured by plaintiff's losses and/or defendant's profits. In \textit{Telex v. I.B.M.},\textsuperscript{153} IBM was awarded $17.5 million in compensatory damages. As to its peripherals, IBM received $4.5 million for lost monthly rentals. Telex, as a manufacturer of plug compatible peripherals, was able to market its units much sooner by reason of its misappropriation of IBM's trade secrets and thus Telex was able to displace IBM's products.\textsuperscript{154} IBM received $3.5 million out of Telex's profits on the theory of unjust enrichment. IBM received another $10 million from defendant's profits on IBM's Merlin disc. If Telex had not misappropriated and used IBM's trade secrets, Telex would have spent $10 million more than it did in connection with the work on its equivalent of the Merlin disc.

When the defendant has not destroyed plaintiff's trade secret through disclosure, damages are measured by the value of the secret to the defendant, a measure known as the "reasonable royalty" standard. In \textit{University Computing Co. v. Lykes-Youngstown Corp.},\textsuperscript{155} the reasonable royalty standard for measuring damages was used. The court found that plaintiff's trade secrets in its computerized inventory control system were not lost because of the other joint venturer's misappropriation. Also, defendant did not profit from the misappropriation, as it failed in its attempts to market the system. Hence, the proper measure of damages was what a willing buyer would have paid a willing seller at the time of the misappropriation, in this case $220,000.\textsuperscript{156}

The tort remedy of punitive damages is also available for trade secret misappropriation.\textsuperscript{157} In \textit{Telex}, IBM was awarded $1 million in
punitive damages for Telex's flagrant practice of luring away IBM's employees and utilizing the trade secrets known to them in manufacturing and marketing its own products. The Uniform Act allows exemplary damages not exceeding twice the damage award if willful and malicious misappropriation occurred.

Attorney's fees were recovered by plaintiffs in both *Sperry Rand Corp. v. Electronic Concepts, Inc.*, and *University Computing v. Lykes-Youngstown Corp.* In *Lykes-Youngstown*, secret meetings and the like constituted bad faith on the part of the defendants, which justified an award of attorney's fees. The Uniform Act also allows attorney's fees where the misappropriation is willful and malicious.

C. CRIMINAL PENALTIES

Many states impose criminal liability for trade secret misappropriation. Eighteen states have enacted criminal statutes specifically covering trade secrets. The availability of criminal sanctions provides an advantage to trade secret holders over that obtained by a patent holder, since patent law does not provide for criminal penalties. One of the objectives behind criminal penalties is deterrence. This is especially significant to a trade secret holder because the prevention of abuse is more important than the cure. Often, after misappropriation, the trade secret is disclosed and the trade secret is lost, thereby making it valueless to the holder.

California's criminal trade secret statute, Penal Code section 449c, states in pertinent part:

> Every person . . . who . . . offers . . . and every person who . . . receives or takes a benefit as an inducement . . . for . . . making available an article representing a trade secret owned by his present or former principal, employer or master, to any [unauthorized] person . . . is punishable by imprisonment . . . [for up to] one year, or by fine . . . [of up to] $5000, or both . . .

In *People v. Serrata*, an ex-IBM employee was convicted on two counts of theft under section 499c for having taken drawings dealing with IBM's computer devices.

Trade secret misappropriation may also violate various federal

---

158. *Telex*, 510 F.2d at 933.
159. *Unif. Trade Secrets Act* § 3(b) (1980).
161. 504 F.2d 518 (5th Cir. 1974).
criminal statutes. An illustrative case is *United States v. Hitachi, Ltd.* In February of 1983, Hitachi and two of its employees entered guilty pleas to charges of conspiring to steal IBM's trade secrets relating to IBM's latest computer technology. The stolen merchandise related to documents containing design information on three IBM computers, including the IBM 3081, the most powerful computer processing unit sold by IBM. Defendants were indicted under 18 U.S.C. § 371 for conspiring to transport stolen property in interstate commerce.

IX. CONCLUSION

*Kewanee Oil Co. v. Bicron Corp.* and subsequent decisions have elevated trade secrets to the third corner of legal protection, alongside copyright and patent laws. It is clear that trade secret protection is being expanded and strengthened by the courts and the state legislatures.

Recent decisions controvert the perceived shortcoming that trade secret status is readily lost upon disclosure through licensing or copyright publication. In *Data General Corp.*, the court made an inroad into the view that trade secrets are not suitable for mass distribution by granting protection even when there were more than 6000 distributors. The most promising development has been the judicially approved use of both trade secret and copyright, to maximize the protection of both software and firmware.

Thus, trade secrets have been the predominant form of computer software protection. The outlook is that trade secrets will be relied on by the computer industry as the primary choice of protection in the first instance and/or be used synergistically in conjunction with copyright.

*Vytas M. Rimas*

---

* Student, Golden Gate University School of Law.