January 1983

Trade Secrets and the Skilled Employee in the Computer Industry

Laura Wheeler

Follow this and additional works at: http://openscholarship.wustl.edu/law_lawreview

Part of the Computer Law Commons, Intellectual Property Law Commons, and the Labor and Employment Law Commons

Recommended Citation
Available at: http://openscholarship.wustl.edu/law_lawreview/vol61/iss3/6

This Note is brought to you for free and open access by the Law School at Washington University Open Scholarship. It has been accepted for inclusion in Washington University Law Review by an authorized administrator of Washington University Open Scholarship. For more information, please contact digital@wumail.wustl.edu.
TRADE SECRETS AND THE SKILLED EMPLOYEE IN THE COMPUTER INDUSTRY

With the development of the Electronic Numerical Integrator and Computer (ENIAC), the Electronics Revolution began. As the Revolution gained momentum, the need for highly trained researchers, engineers and technicians increased dramatically. These key employees often obtain access to an employer’s confidential business information. When they change jobs within the same competitive industry, they inevitably reveal previously acquired knowledge, much of it confidential business information, to their new employers. Some of this knowledge may constitute a trade secret.

When determining whether trade secret protection is warranted, courts must strike a balance between the conflicting social policies of freedom of contract, business ethics and private economic freedom. This balancing process has left a checkered history of the law of trade secret protection in the context of the employment relationship.

This Note discusses the legal grounds for trade secret protection, with a particular focus on the employment relationship. Further, this Note considers the conflicting social policies which courts must balance.

3. See infra notes 74-77 and accompanying text.
4. See infra note 78 and accompanying text.
5. Commentators refer to skilled researchers, engineers and technicians as “key employees” because of their uniquely knowledgeable positions in the employer's firm. See, e.g., VonKalinowski, Key Employees and Trade Secrets, 47 VA. L. REV. 583, 583 (1961).
6. The term “confidential business information” refers to all information which the employer subjectively wishes to keep confidential. The term “trade secret,” on the other hand, refers to confidential business information which is legally protectable. See infra notes 45-59 and accompanying text.
7. See, e.g., Gillette Co. v. Williams, 360 F. Supp. 1171, 1176-78 (D. Conn. 1978). Key employees have access to items of confidential business information, many of which are often assimilated into their general knowledge. If a second employer asks a computer programmer to develop a program to solve a particular problem, this programmer will undoubtedly draw upon the knowledge and experience gained while with the first employer. If the employee uses confidential information of his first employer to solve the second employer's problem, it is conceivable that the second employer could acquire some of the first employer's trade secrets.
8. See infra notes 37-59 and accompanying text.
10. See infra notes 29-59 and accompanying text.
11. See infra notes 60-69 and accompanying text.
when faced with trade secret protection problems arising from computer industry employment relationships. Finally, this Note examines the viability of proposed means of dealing with employee appropriation of trade secrets, and suggests an alternative approach to alleviate that problem.

I. HISTORICAL BASIS OF TRADE SECRET LAW

Trade secret protection originated in the first century when the definition of "plagium" expanded to encompass the pirating of literary works. Throughout ancient history, the law strictly curtailed the dissemination of trade secrets. The Romans used slavery to control the descent of trade secrets. During the Middle Ages the guild system evolved, under which only guild members were entrusted with trade secrets. By the seventeenth century, statutory protection for some types of intellectual property had begun to develop.

In contrast to the stringent protection historically afforded trade secrets, current American law offers little protection. Although the framers of the Constitution explicitly provided for patents and copyrights, they failed to include protection for trade secrets. In the ab-

---

12. See infra notes 72-117 and accompanying text.
13. See infra notes 118-138 and accompanying text.
14. See infra notes 139-140 and accompanying text.
17. B. Bugbee, supra note 15.
18. Schiller, Trade Secrets and the Roman Law, 30 Colum. L. Rev. 837, 838-39 (1930). Roman law granted relief to a master if a slave betrayed a secret to a third party. Id.
19. Harris & Siegel, Trade Secrets in the Context of Positive Competition, 10 Idea 297, 312 (1966). Strict enforcement of this rule sometimes caused trade secrets to disappear with the death of the last member of the guild. Id.
20. These statutes consisted primarily of grants of individual monopolies under private benefit legislation. Historians trace the beginning of patent law to this time period, when statutes generally prohibited monopolies but reserved monopolies for inventors' licensed inventions. An Act Concerning Monopolies, 1623, 21 Jac., ch. 3 §§ I-XIV. These early statutory protections assisted individuals in competing against the guild monopolies. Arahamson, The Patent System: Its Economic and Social Basis, Subcommittee on Patents, Trademarks, and Copyrights, Study No. 26, Senate Committee on the Judiciary, 86th Cong., 2d Sess. (1960). Almost a century later, Parliament enacted the first statutory copyright protection. An Act Vesting the Copies of Printed Books in the Authors of Such Copies, 1709, 8 Anne ch. 19 §§ I-XI.
sence of constitutional or statutory regulation, trade secret protection in the United States arose from the common law. 22

The decision in Peabody v. Norfolk 23 marks the beginning of American trade secret law. 24 In Peabody, the plaintiff’s decedent successfully developed a unique manufacturing process. He hired a machinist, the


22. The common law of trade secrets and the statutory regulation of patents and copyrights co-existed peacefully in American law for over a century. Courts did not consider the possibility that federal patent and copyright statutes preempt state trade secret law until the Supreme Court decisions in Sears, Roebuck & Co. v. Stiffel Co., 376 U.S. 225 (1964), and Compco Corp. v. Day-Brite Lighting, Inc., 376 U.S. 234 (1964). In Sears-Compco the Supreme Court held that federal patent law preempted the state common law of unfair competition. 376 U.S. at 229. The Court found preemption justified even though “the state law [was] enacted in the exercise of otherwise undoubted state power.” Id.


After a decade of confusion the Supreme Court settled the federal preemption issue in Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974). In Kewanee, the Court held that federal patent law does not preempt state trade secret law, even if a plaintiff could acquire patent protection for some of the material in question. Id. at 474. Since Kewanee, courts have consistently ruled against claims that state trade secret law is preempted by the federal copyright laws. See, e.g., Truck Equip. Serv. Co. v. Fruehauf Corp., 536 F.2d 1210 (8th Cir.), cert. denied, 429 U.S. 861 (1976) (design of truck trailer protectable under state law, even though protectable under federal copyright law), cert. denied, 429 U.S. 861 (1976); Time Mechanism, Inc. v. Qonaar Corp., 422 F. Supp. 905 (D.N.J. 1976) (design of parking meter protectable under state law even though not protectable under federal copyright law).

Similarly, in Goldstein v. California, 412 U.S. 546, 569 (1973), the Court ruled that federal copyright law did not prohibit California from banning the copying of records and tapes made before February 15, 1972, the date Congress amended the federal copyright statute to include these items. See Pub. L. No. 92-140, 85 Stat. 391 (codified as amended at 17 U.S.C. § 102(a)(7) (1976)). See also Aronson v. Quick Point Pencil Co., 440 U.S. 257 (1979) (state has the right to enforce royalty payments under a trade secret agreement even though the licensee’s production and sale of the item has placed it in the public domain).

23. 98 Mass. 452 (1868).

defendant, to help him implement the process. The defendant became intimately acquainted with the process and promised by contract not to disclose the secret process or any information pertaining to it. Subsequently, the machinist began working for another entrepreneur and used the secret process in his factory. The developer's heir sued both the former employee and the entrepreneur, seeking an injunction against their use of the process.

The *Peabody* court discussed several possible bases for trade secret protection, including protection as a property interest; protection as the subject of an employment contract restricting future disclosure; and, absent a contract, protection as the subject of a confidential relationship. The court ultimately relied on the plaintiff's proprietary interest in the secret process to enjoin its use by both defendants. Today, courts use all the rationales first enunciated in *Peabody* to protect trade secrets.

II. THE THEORETICAL BASIS FOR PROTECTING TRADE SECRETS

Many of the difficulties that arise with respect to trade secret protection stem from the problem of how to conceptualize a trade secret. A majority of courts classify trade secrets as property.

In *E.I. DuPont de Nemours Powder Co. v. Masland*, however, Justice Holmes suggested that courts consider the confidential relationship of the parties as an alternative ground for trade secret protection. One
commentator finds the cases which base trade secret protection upon breach of a confidential relationship consistent with the property characterization because the courts could not grant relief to the holder in these latter cases unless he possessed property which courts could protect.\(^{32}\) Other commentators, however, urge that *Masland* dismissed the proprietary view.\(^{33}\) These commentators argue that confidential business information only acquires protection as a trade secret when it arises from a confidential relationship.\(^{34}\) The fundamental precept of "fairness" underlies the rationale of both the proprietary and the confidential relationship theories. While courts disagree on the proper rationale,\(^{35}\) they unanimously agree that the law will not allow parties to

---

The word property as applied to trademarks and trade secrets is an unanalyzed expression of certain secondary consequences of the primary fact that the law makes some rudimentary requirements of good faith. Whether the plaintiffs have any valuable secret or not the defendant knows the facts, whatever they are, through a special confidence he accepted. The property may be demanded but the confidence cannot be. Therefore the starting point for the present matter is not the property or due process of the law, but that the defendant stood in confidential relations with the plaintiffs, or one of them.

---


34. *See supra* note 33.

“reap where they have not sown.”

III. TRADE SECRETS DEFINED

Although the theoretical basis of trade secret protection varies among the courts, the vast majority agree that the *Restatement of Torts* contains the most accurate definition of a trade secret: Any process or information which gives the possessor an “opportunity to obtain an advantage” over his competitor, and which does not constitute public knowledge.

Drawing on the definition provided by the *Restatement*, courts have developed factors which help determine the existence of trade secrets. These factors include: the degree of secrecy involved inside and outside the firm; the methods used to protect the secret; the value of the secret to the firm’s business and to its competitors; the extent of money, time and effort invested in developing the information that constitutes the secret; and the degree of difficulty by which another could attain


Justice Holmes first expressed the fundamental fairness concept in Board of Trade v. Christie Grain Co., 198 U.S. 236 (1905): “The plaintiff has the right to keep the work which it has done, or paid for doing, to itself. The fact that others might do similar work, if they wished, does not authorize them to steal plaintiff’s.” *Id.* at 250. *See also* Pachmayr Gun Works, Inc. v. Olin Mathieson Chem. Corp., 502 F.2d 802, 807 (9th Cir. 1974), in which the court stated, “it appears settled that the law of trade secrets is essentially concerned with protecting ‘against breach of faith and reprehensible means of learning another’s secret.’” (quoting 4 *RESTATEMENT OF TORTS* § 757 comment b, at 7 (1939)).

See generally R. Ellis, supra note 33, § 12, at 19.

37. *RESTATEMENT OF TORTS* § 757 comment b (1939). Twenty eight states and all federal circuits accept this definition. 12 R. Milgrim, *supra* note 29, § 2.01 n.2. The *Restatement (Second)* of *Torts* excludes this section and, in fact, all of the chapter which formerly covered unfair competition and trade regulation. The reporters explained:

[U]nfair competition and trade regulation were rapidly developing into independent bodies of law with diminishing reliance upon the traditional principles of Tort Law. . . . If it should be later decided that the law on these subjects ought to be restated it will be done by separate restatements on the subjects involved.

4 *RESTATEMENT (SECOND) OF TORTS* commentary at 1 (1979). *See* Amoco Prod. Co. v. Lindley, 609 P.2d 733, 743 n.4 (Okla. 1980) (recognizing Reporter’s rationale for exclusion but stating that “tort premises are nonetheless an integral part of the developed case law of trade secrets”). But see Sims v. Mack Trucks, Inc., 463 F. Supp. 1068, 1070 (E.D. Pa. 1979) (although acknowledgement trade secret and unfair competition claims have basis in different legal theories, dismissing trade secret action as it had dismissed unfair competition action).

In Imperial Chem. Indus. Ltd. v. National Distillers & Chem. Corp., 342 F.2d 737 (2d Cir. 1965), the court similarly defined trade secrets: “[A] trade secret can exist in a combination of characteristics and components, each of which, by itself, is in the public domain, but the unified process, design or operation of which, in unique combination, affords a competitive advantage and is a protectable secret.” *Id.* at 742.
the information by proper means.\textsuperscript{38}

A trade secret need not be unique and may be clearly anticipated in "prior art."\textsuperscript{39} Nevertheless, it must afford the holder an opportunity to obtain a competitive advantage.\textsuperscript{40} Additionally, the information or process for which trade secret protection is sought must not be common knowledge within the industry or among the general public.\textsuperscript{41} While novelty may help the possessor in proving the existence of a trade secret, it does not in itself constitute the basis of protection. Instead, courts base trade secret protection upon breach of confidentiality or unfair means of acquisition.\textsuperscript{42}

Although the law of trade secrets does not require a discovery, some courts confuse the "advantage in the industry" requirement with uniqueness in the sense of discovery. Courts which mistakenly import such a requirement test the discovery by a standard which barely falls short of the uniqueness requirement necessary to establish patentabil-

38. See \textit{4 Restatement of Torts \S 757 comment v} (1939) [hereinafter cited as \textit{Restatement}].

An exact definition of a trade secret is not possible. Some facts 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 him in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.

\textit{Id.}

39. Prior art means existing technology. A change which is "clearly anticipated in prior art" means a change or development which only minimally improves or alters the existing technology. \textit{4 Restatement, supra} note 38, comment b, at 6-7.


As technical information approaches pure science it comes closer to purely abstract ideas which should be part of the public domain. Similarly, it leaves the realm of employer's property and becomes a part of the intellect of the employee.

42. \textit{See}, e.g., Booth v. Stutz Motor Car Co. of Am., 56 F.2d 962, 968 (7th Cir. 1932); Cornibert v. Cohn, 169 Misc. 285, 287, 7 N.Y.S.2d 351, 354 (Sup. Ct. 1938). \textit{See generally Restatement, supra} note 38, comment b, at 7 (Reporter's note that lack of novelty may limit defendant's liability to damages only, precluding injunctive relief).
The prevailing view, however, is that patentability is not a prerequisite to trade secret protection. For a protectable trade secret to exist, the owner must not only fulfill a secrecy requirement with regard to persons outside of his control, but must also fulfill a secrecy requirement as to persons within the firm. This internal secrecy requirement imposes an obligation on the employer to exercise reasonable precautionary measures to protect confidential information. The employer must develop and implement procedures which demonstrate to the employee the importance of not disclosing the information. Adequate precautionary measures may consist of confidentiality agreements, reminders of confidentiality.


44. See RESTATEMENT, supra note 38.

45. See 9A Z. CAVITCH, supra note 33, § 232.01[1][b] (this element of the secrecy requirement labelled "external" secrecy).

46. See id. § 232.01[1][a] (this element labelled "internal" secrecy).


and numerous security measures.  

If the owner publicly discloses confidential information, he may not impose conditions of secrecy on his employees.  Nevertheless, limited disclosure to employees and others in a confidential relationship with the owner does not destroy trade secret protection.

Similarly, public disclosure by the sale of a product embodying the trade secret in a non-obvious manner does not relieve an existing obligation of confidentiality. Some courts have extended the employee's obligation of confidentiality to situations in which the owner disclosed the trade secret by means other than sale. Other courts have refused to grant trade secret protection in this circumstance, however, on the


52. "Others" refers to those who have a contractual right or permission of the owner to use the trade secret, but who do not work for the owner. See infra note 53.


54. See Head Ski Co. v. Kam Ski Co., 158 F. Supp. 919, 923 (D. Md. 1958) (although ski publicly available, defendants learned its composition from working for plaintiff, not by reverse engineering); Maas & Waldstein Co. v. Walker, 100 N.J. Eq. 224, 229, 135 A. 275, 277 (1926) (chemical formulas for lacquers were generally known, but plaintiff's variations were secret and warranted protection), aff'd per curiam, 102 N.J. Eq. 328, 140 A. 921 (N.J. 1928); Stone v. Goss, 65 N.J. Eq. 756, 760, 55 A. 736, 738 (N.J. 1903) (where general ingredients of chemical formula generally known, but particular combination not generally known, plaintiff entitled to trade secret protection); Tabor v. Hoffman, 118 N.Y. 30, 37, 23 N.E. 12, 13 (1889) (public sale of pump did not make secret pattern for pump mold public); Extrin Foods, Inc. v. Leighton, 202 Misc. 592, 597, 115 N.Y.S.2d 429, 433 (Sup. Ct. 1952) (inclusion of ingredients on plaintiff's product label does not preclude trade secret protection); cf. Colgate-Palmolive Co. v. Carter Prods., Inc., 230 F.2d 855, 865 (4th Cir. 1956) (because technical process well-known in industry, defendant not liable for misappropriation of process even though he learned of it from former employer and communicated it to new employer).

theory of abandonment. If an employee cannot prove that the owner intended to abandon the trade secret, the court must determine the amount of confidential information which still warrants protection.

Courts also consider the effort incurred in initially developing an item of confidential business information when attempting to determine if trade secret protection is warranted. A finding that substantial effort was required to develop confidential information militates in favor of extending trade secret protection. If such a finding is made, a majority of courts granting trade secret protection even if appropriated information could be acquired easily by experimentation or reverse engineering.

The lack of a single conceptual basis for trade secret protection and the inconsistent application of its constituent elements has created confusion among courts; adding the variable of employee disclosure further complicates trade secret protection analysis.

56. Abandonment occurs when the owner no longer intends to exert his legal right to protect confidential material. Timely Prods. Corp. v. Arron, 523 F.2d 888 (2d Cir. 1975); Underwater Storage, Inc. v. United States Rubber Co., 371 F.2d 950 (D.C. Cir. 1966), cert. denied, 386 U.S. 911 (1967); Note, Protection and Use of Trade Secrets, 64 Harv. L. Rev. 976, 977 (1951).


57. This question must be decided as a factual matter. See Note, supra note 56, at 977.


IV. TRADE SECRET PROTECTION AND THE EMPLOYMENT RELATIONSHIP

A. Generally

Employers may protect their trade secrets either by exacting a non-disclosure contract from each key employee, or by relying on the common law of agency. Under the common law of agency, the employee has a duty not to reveal any confidential information which he acquired through his employment. Confidential information is held in trust for the employer. When the agency relationship ends, the former agent may freely compete with the former employer as long as he does not use trade secret information acquired in the course of the former employment.

Courts have had difficulty, however, balancing the employee's right to change jobs with the employer's interest in protecting trade secrets.
under the common law of agency. Because the common law recognizes the former employee's right to practice any chosen calling, an employer may not unreasonably restrain the manner in which an employee uses knowledge, skill and experience acquired during his employment. The employee does not incur liability, therefore, when the former employer merely alleges that the employee's general skill and knowledge "belonged" to the employer as a trade secret. When the employee's skill, knowledge, and experience are inextricably combined with the employer's trade secrets, however, the question of liability becomes more difficult to determine. The former employer may not completely enjoin the former employee from seeking employment in the same field. Nevertheless, if the former employer proves that he will suffer irreparable damage if the former employee uses particular knowledge or skills, courts will usually enjoin the employee from revealing that information.

65. Public policy favors free competition by giving the employee a right to use his skill and knowledge for his own benefit and for the benefit of the public. On the other hand, courts wish to promote inventiveness by protecting employer's trade secrets from misappropriation. See C. McManis, supra note 24. See also U.S Const. Art I, § 8, cl. 8 (patent clause protects inventiveness while promoting free competition).


68. See supra notes 64-66 and accompanying text.


A few courts have refused to grant the former employer any relief, even though he could prove that he confidentially imparted the knowledge or skill to his former employee. See Reed, Roberts Assocs., Inc. v. Strauman, 40 N.Y.2d 303, 308-09, 353 N.E.2d 590, 593-94, 386 N.Y.S.2d 677, 680-81 (1976) (former employer cannot restrain former employee from using unique variation of gen-
Because of the uncertainty of common law protection, employers often acquire protection through contracts which limit the employee's right to disclose confidential information. Courts usually find nondisclosure agreements valid and enforceable. If the agreement is not reasonably necessary to protect the employer's interest, however, courts will find it invalid.

B. Trade Secret Protection in the Computer Industry Employment Relationship

The difficulties employers encounter in attempting to protect their trade secrets are particularly acute in the computer industry. The problem of protecting computer hardware and computer software from acquisition by competing firms has caused considerable debate among commentators. Since the mid-1940's the computer industry has
grown substantially.75 As software increasingly replaces hardware functions,76 research and development incentives continue to rise in the software industry.77 Unfortunately, with this rapid expansion of technology has come an equally rapid increase in software misappropriation by employees and users.78

75. Scientists developed the first electronic computer using vacuum tubes in 1946. This computer used hard-wire control boards and machine code (i.e., only hardware) to program the computer. See supra note 1. In the early 1950's, Remington and IBM each developed a commercial computer using some internal programs written in symbolic code (i.e., software). Brooks, Perfecting and Protecting Rights in Employee Inventions, in COMPUTER FINANCE AND LEASING: RECENT TRENDS IN FINANCING AND MARKETING 611, 621 (M. Berwind ed. 1982). During this period manufacturers "gave away" the software as part of the hardware package. Id. at 621-22. In 1969, the practice of giving software away ended as firms which manufactured only software moved into the field. Since that year, the software industry has expanded remarkably. Due to this rapid expansion, figures are difficult to acquire. One author estimated, however, that the industry only spent $3 billion developing computer software in 1967. Kayton, Foreword to SOFTWARE PROTECTION at 1 (Patent Group ed. 1969). In 1976, experts estimated the value of computer programs in use at approximately $43.1 billion, and projected the figure to rise to $79.7 billion by 1980. Parker v. Flook, 437 U.S. 584, 587 n.7 (1978) (based on Brief for Computer & Business Manufacturing Association as Amicus Curiae).

76. Prior to 1975, software accounted for only 10-20% of the cost of a computer with a main frame system. Brooks, supra note 75, at 622. With the development in 1975 of the microcomputer, software costs increased to 30-40% of the total cost of a system. Id. As the hardware size decreases, software absorbs its tasks, thereby increasing its share of the costs. In the next five years, analysts expect hardware costs to drop by 80% as software continues to replace hardware functions. Id.

Today's microcomputer, at a cost of perhaps $300, has more computing capacity than the first large electronic computer, ENIAC. It is 20 times faster, has a larger memory, is thousands of times more reliable, consumes the power of a light bulb rather than that of a locomotive, occupies 1/30,000 of the volume and costs 1/10,000 as much.


77. "In an industry whose product declines in price by 25 percent a year, the motivation for doing research and development is clearly high. A year's advantage in introducing a new product or new process can give a company a 25 percent cost advantage over competing companies." Noyce, supra note 76, at 68.

There is also an acute shortage of qualified personnel capable of creating and improving computer programs. Today, the industry demands at least 50,000 more programmers than the market provides each year. Missing Computer Software, Bus. Wk., Sept. 1, 1980, at 46-56. Furthermore, experts project a labor cost increase of 60% over the next five years. Brooks, supra note 75, at 623.

78. See, e.g., 11 Charged in Theft of IBM Disk Designs, COMPUTERWORLD, July 11, 1973, at 27, col. 2; Girl Charged in Program Threat, COMPUTERWORLD, Aug. 1, 1973, at 1, col. 3; More
Employers have attempted to use patents to protect their software from misappropriation, but the patentability of software remains uncertain. In the 1970's, the Supreme Court denied patent protection to computer software. More recently, the Court has sustained patents that possessed a software component. Nevertheless, because the Court has not expressly overruled earlier decisions denying patent protection for software, lower courts may continue to deny such protection. Moreover, many programs lack the elements of novelty and nonobviousness required by statute to attain patent protection.

Employers have also tried to use federal copyright law to protect their software. Before 1980, the protection of computer programs under the 1976 Copyright Act was questionable. In 1980, Congress

---


To acquire patent protection an inventor must demonstrate that the invention is a "new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof", that the invention has not already been thought of by others; and that the invention was not obvious to one familiar with prior art. 35 U.S.C. §§ 101-03 (1976 & Supp. IV 1980).

80. In Gottschalk v. Benson, 409 U.S. 63 (1972), the Court found that a process for converting binary coded decimal numbers into pure binary numbers performed completely within the computer did not constitute patentable subject matter. The Court viewed the process as simply a mathematical algorithm, and analogized it to the unpatentable discovery of a law of nature. Four years later the Court avoided the patentability issue by declaring that an arguably innovative computer bookkeeping system could not acquire patent protection because similar systems existed in prior art. Dann v. Johnston, 425 U.S. 219 (1976). The Court further reinforced this line of authority in Parker v. Flook, 437 U.S. 584 (1978), in which the claimants had devised a computer program that applied an algorithm to a problem and then acted to correct the problem. The Court, relying on Gottschalk, held that the addition of a post-solution activity did not render the process patentable.


83. 17 U.S.C. § 102(a) (1976 & Supp. IV 1980). The federal copyright statute protects the originator's work from duplication by unauthorized persons if it is fixed in any tangible medium from which it can be perceived, reproduced or otherwise communicated. Id. § 102(c).

84. See Data Cash Sys., Inc. v. JS&A Group, Inc., 480 F. Supp. 1063 (N.D. Ill. 1979)
expressly amended the 1976 Act\textsuperscript{85} to include computer programs.\textsuperscript{86} This amendment eliminated questions of coverage in situations involving copying by mechanical methods.\textsuperscript{87} The amendment did not, however, solve the problem of protecting programs that did not fulfill the originality, authorship and fixation requirements of the Act.\textsuperscript{88}

The uncertainty of traditional statutory protection for computer software has caused many firms to seek trade secret protection.\textsuperscript{89} If a

\begin{center}
\textbf{TABLE I. EFFECTIVENESS OF SOFTWARE PROTECTION}
\end{center}

<table>
<thead>
<tr>
<th>Method</th>
<th>Weighted Response (Scale of 0-5)</th>
<th>Percent Using</th>
<th>Effective Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patent</td>
<td>0.54</td>
<td>4</td>
<td>2.2</td>
</tr>
<tr>
<td>Copyright</td>
<td>1.48</td>
<td>20</td>
<td>29.6</td>
</tr>
<tr>
<td>Trade Secret</td>
<td>2.31</td>
<td>21</td>
<td>48.5</td>
</tr>
<tr>
<td>Object program</td>
<td>3.54</td>
<td>30</td>
<td>106.2</td>
</tr>
<tr>
<td>Know-how</td>
<td>2.46</td>
<td>13</td>
<td>32.0</td>
</tr>
<tr>
<td>Cryptography</td>
<td>1.24</td>
<td>40</td>
<td>49.6</td>
</tr>
<tr>
<td>Other</td>
<td>3.28</td>
<td>17</td>
<td>55.8</td>
</tr>
</tbody>
</table>

To rate the effectiveness of the methods of protection used, each organization that used a specific method was asked to categorize the method as follows: not at all effective, rarely effective, somewhat effective, fairly effective, very effective, completely effective. Table I shows a weighted average to the response, where not at all effective is "0" and completely effective is "5". The second column is the percent using the method, and the third column is obtained by multiplying the first two together.

Bigelow, \textit{supra} note 74, at 120 (emphasis in original).
program affords a firm an opportunity to gain a competitive advantage in the industry and the firm succeeds in maintaining secrecy, the program constitutes a trade secret and may be protected under the common law of trade secrets.

While the common law of trade secrets protects software, whether its protection redounds to the benefit of the employer or employee remains uncertain. Courts addressing this question have uniformly applied a two part test: whether the computer program deserves trade secret protection; and, whether the employee had a contractual or common law duty not to disclose the information.

Although courts apply a uniform test, they reach varying results. Of the courts which find software protectable as a trade secret, a majority grant protection to the employer regardless of who developed the program. A minority of courts that grant software trade secret protec-

90. See supra notes 37-59 and accompanying text.
91. Id.
tion, however, hold that when an employee develops the trade secret, he has no duty to keep the information confidential. 95 On the other hand, a majority of courts that deny trade secret protection to computer programs conclude that an employee incurs no liability for disclosing information regarding a program to third parties. 96 A few courts, however, protect such information from disclosure by an employee, even in the absence of a trade secret. 97

An example of a case in which a court found employees who developed a program liable for impermissible disclosure of their former employer’s trade secrets is Telex Corp. v. International Business Machines Corp. (IBM). 98 In this case, Telex induced several of IBM’s key employees to join its firm. These former IBM employees revealed to Telex a new source code 99 which they had helped develop for IBM. By hiring away IBM’s key employees, Telex saved $10 million in development costs. 100 The court ruled that the source code constituted a trade secret, 101 and that the employees had breached their express contract with IBM and the confidential relationship they had developed with that

---


99. Source code refers to the instructions the programmer gives the computer. The computer takes this code and generates an object code. Lay people can read source code; they cannot read object code.

100. Id. at 911 n.10.

101. Id. at 929.
company. The court found that as a result of the misappropriation, IBM lost its competitive advantage in this area.

Courts have also granted employers the benefits of trade secret protection in cases involving trade secrets which the defendants did not develop or design. For example, the court in Computer Print Systems, Inc. v. Lewis found a former officer of the plaintiff liable for copying a computer program designed to expedite direct mail advertising, and for delivering the program to a customer of the plaintiff.

The minority rule imposes no duty on the part of an employee who develops a trade secret to keep that information confidential. In Structural Dynamics Corp. v. Engineering Mechanics Research Corp., 107 individual defendants, working under nondisclosure contracts for Structural Dynamics, developed a general purpose isoparametric computer program. Subsequently, they resigned and established their own competing business. The court found that because the individual defendants developed the program, they had no general duty to keep it confidential. Nevertheless, the court felt compelled to decide

---

102. Id.
103. Id. at 911, 929.
106. The court stressed that the plaintiff had expended a great deal of money in developing the program, and that the program gave the plaintiff a competitive advantage in the market. The court admitted, however, that direct mail programs are common knowledge in the industry. One may, therefore, question the soundness of the court's decision to grant trade secret protection in this case. See supra notes 37-59 and accompanying text. See also Com-Share Inc. v. Computer Complex, Inc., 338 F. Supp. 1229 (E.D. Mich. 1971) (defendant liable for disclosing information to third party in violation of contract between plaintiff and defendant specifically forbidding disclosure). aff'd, 458 F.2d 1341 (5th Cir. 1982).
108 Id. at 1106.
109. Id.
110. Id. at 1112.
in favor of the employer because the individual defendants had signed reasonable nondisclosure agreements.\footnote{111}{While no cases involving computer software follow \textit{Structural Dynamics}, its reasoning is not unique. \textit{See}, \textit{e.g.}, Wexler v. Greenberg, 399 Pa. 569, 160 A.2d 430 (1970) (where defendant was hired expressly to reverse engineer competing firm's products, formulas derived belonged to him as part of his knowledge). \textit{See also supra} note 97. The \textit{Structural Dynamics} decision is particularly well-reasoned because of the court's thoughtful analysis of the competing interests involved — society's need for useful knowledge, the employer's need for secrecy to motivate inventiveness, and the interests of technically skilled employees whose job mobility may become severely restricted by acquisition of trade secrets. 401 F. Supp. at 1111.}

\textit{Jostens, Inc. v. National Computer Systems}\footnote{112}{318 N.W.2d 691 (Minn. 1982).} similarly illustrates a situation in which a court denied trade secret protection for a computer program. In this case, the individual defendant, pursuant to a nondisclosure agreement, developed a software system for the plaintiff from three commercially available subsystems.\footnote{113}{\textit{Id.} at 701.} Subsequently, he developed a similar system for the corporate defendant, and the plaintiff sued for misappropriation of its confidential information.\footnote{114}{\textit{Id.} at 703.} The court held that the plaintiff could not protect the program as its trade secret because the system composed a part of the individual defendant's own skill and knowledge.\footnote{115}{\textit{Id.} at 701-03. The court acknowledged that the combination was not generally known to the public, the plaintiff intended to keep it secret, and the system did provide a demonstrable competitive advantage to the plaintiff. The combination, however, customized existing technology and did not cause plaintiff to incur large expenses. Therefore, it did not constitute a trade secret. \textit{Id.} at 703. The Minnesota legislature has defined trade secrets by statute. \textit{See} Uniform Trade Secrets Act, Minn. Stat. \textsect 325C.01 subdiv. 5 (1980).}

Because of the uncertain dividing line between the employer's pro-

\begin{itemize}
  \item \textit{Id.} at 701.
  \item \textit{Id.} at 703.
  \item \textit{Id.} at 701-03. The court acknowledged that the combination was not generally known to the public, the plaintiff intended to keep it secret, and the system did provide a demonstrable competitive advantage to the plaintiff. The combination, however, customized existing technology and did not cause plaintiff to incur large expenses. Therefore, it did not constitute a trade secret. \textit{Id.} at 703. The Minnesota legislature has defined trade secrets by statute. \textit{See} Uniform Trade Secrets Act, Minn. Stat. \textsect 325C.01 subdiv. 5 (1980).
  \item The Oklahoma Supreme Court decided a similar case in 1980. \textit{See} Amoco Prod. Co. v. Lindley, 609 P.2d 733 (Okl. 1980). In this case the defendant-employee developed, over his employer's objection, on his own time and at his own expense, a well-logging computer program. The court denied trade secret protection to the employer for the program and held that the employer had a right to disclose it. The court refused to bind defendant to his nondisclosure contract. \textit{See also} Electronic Data Sys. Corp. v. Kinder, 360 F. Supp. 1044 (N.D. Tex. 1973) (defendant developed for his employer one of two existing programs for processing medicaid forms; held employer has no recourse when defendant goes to work for employer's competitor and implements only the other existing program), \textit{aff'd}, 497 F.2d 222 (5th Cir. 1974); National Sur. Corp. v. Applied Sys., Inc., 418 So. 2d 847 (Ala. 1982) (defendant developed computer programs for employer, left and started own business in same field; court held programs convertible personal property and defendants liable for same).
  \item Arguably, some of the cases cited above do not involve trade secrets as defined in this Note. \textit{See supra} notes 37-59 and accompanying text. Courts nevertheless held the individual defendants liable. \textit{See} Structural Dynamics Corp. v. Engineering Mechanics Research Corp., 401 F. Supp. 1102 (E.D. Mich. 1975) (no trade secret except that protected by contract); Cybertek Computer
pectable rights in a specific program design or combination and the programmer's skill and experience, the cases involving trade secret protection in the computer industry employment relationship present particularly difficult questions. Courts, while attempting to balance these competing interests, have been unable to achieve a uniform and equitable solution.

V. SOLUTIONS AND RECOMMENDATION

Congress has failed to respond effectively to the continued judicial confusion apparent in the computer employment cases. In the early 1970's there were unsuccessful attempts to legislatively establish an employee ownership right in patentable inventions and a compensation system for this right. Because of significant opposition, no plans exist for enacting federal legislation on this subject.

In the face of Congressional inaction and judicial uncertainty, some commentators have urged a uniform statutory solution. The American Bar Association has developed a Uniform Trade Secret Act. The states, however, generally have not adopted the Act. Furthermore, the Act merely codified the position of the Restatement of Torts without clarifying the factors which should influence a finding of trade secret protection for either the employer or employee.

---

116. See supra notes 100-116 and accompanying text.
117. See H.R. 1483, 92 Cong., 1st Sess (1971); H.R. 15512, 91st Cong., 1st Sess. (1969). Congress modeled this act after a similar German law. See Kowarzik, Employee Invention Under German Law, 54 J. PAT. OFF. Soc'y, 807, 809 (1972). Although the proposed law dealt solely with patentable inventions, the element of "ownership" is common to both trade secret and patent protection.
118. R. Milgrim, supra note 29, § 5.02(4), at 5-37 n.61.1.
120. UNIF. TRADE SECRETS ACT §§ 1-12, 14 U.L.A. 537-551 (1982 Master ed.).
122. See 4 RESTATEMENT, supra note 38.
123. The Uniform Trade Secret Act only covers tort theories of recovery. UNIF. TRADE
Similarly, the individual states have not developed their own statutory solutions to this problem. Approximately one third of the states have enacted statutes which apply exclusively to the theft of trade secrets. Other states have expanded their theft or larceny statutes to include the theft of trade secrets. The majority of these statutes define trade secrets narrowly to include only scientific and technical information embodied in tangible form. Because of this narrow definition, these statutes do not address the problem of misappropriation of intangible business trade secrets.

Colorado’s statute most comprehensively covers trade secret theft. This statute protects tangible and intangible scientific and business trade secrets. Unlike the other statutes which base the degree of culpability on the value of the trade secret misappropriated, the Colorado statute provides one clearly defined penalty for all violations.
well-publicized criminal statute of this variety may most effectively deter errant employees.

Only Florida has an intellectual property statute which directly classifies the misappropriation of computer programs as a felony, but coverage is restricted to the theft of tangible programs.131

While criminal statutes may sufficiently deter employees to significantly reduce misappropriation, socially valuable inventions could be concomitantly discouraged. Therefore, a few states have passed civil trade secret statutes.132 The most effective of these statutes imposes treble damages upon receivers of stolen trade secrets who knew or should have known that the secrets were stolen.133 This statute could reduce employers’ incentives to actively seek employees from competitors with the intent of gaining access to the competitors’ trade secrets.

Three states recently enacted “Freedom to Create” statutes134 which attempt to encourage invention by clearly delineating the situations in which an employee may expect to keep the product of his efforts.135 One of these statutes requires an employee hired for both specific and general inventive positions to assign an invention36 to the employer if it relates to the business of the employer.137 The other two acts apply the same rule to employees in specific inventive positions,


132. CAL. CIVIL CODE §§ 980-85 (West 1954) (provides exclusive property rights in employer in inventions not disclosed to the public); CONN. ANTI-TRUST ACT, Pub. Act 608 (1972) (provides treble damages and injunctive relief); MONT. CODE ANN. § 39-2-102 (1981) (everything employee acquires during employment, except compensation, belongs to employer); MASS. ANN. LAWS ch. 93, §§ 42, 42A (Supp. 1970) (provides tort liability along same lines as its criminal statute; provides both damages and injunctive relief); N.M. STAT. ANN. § 40-A-16-23 (Supp. 1969) (provides for treble damages against purchaser of stolen trade secret who knew or should have known it was stolen).


134. CAL. LAB. CODE §§ 2870-72 (West 1979); MINN. STAT. ANN. § 181.78 (1978); WASH. REV. CODE § 49.44(2)-(3) (1974 & Supp. 1979). These statutes govern only ownership rights under employee invention agreements.

135. Like the failed federal statute, these state statutes apply only to patentable inventions and are therefore not directly applicable to the present problem. These statutes do suggest, however, one viable solution to the misappropriation of trade secrets.

136. WASH. REV. CODE § 49.44(2)-(3) (1974 & Supp. 1979). It does not include employees hired for non-inventive positions. Inventions of non-inventive position employees are not assignable to the employer.

137. Id.
but do not require employees hired for general inventive purposes to assign their inventions.

While these statutes add very little to the existing common law, they mark a small advance in the right direction. The statutes clearly delineate the groups of employees who must assign their inventions to the employer pursuant to an employee invention agreement. Because most key employees in the computer industry must sign such employment agreements, legislatures should expand state statutes to encompass ownership of trade secrets. 138

Combining a reasonable employee nondisclosure agreement with a statutory 139 definition of the parties' ownership rights could eliminate the confusion presently existing in the application of trade secret law to the employment relationship. 140 For instance, in addition to the general language of the "Freedom to Create" acts, a broader statute could require that the employer and employee meet periodically and sign an agreement stating which projects the employer considers trade secrets.

This type of statute could also protect an employee from loss due to a lack of bargaining power. An employee who believed that specific trade secrets did not "belong" to the employer could petition an arbitrator whose identity could have been established in the original employee nondisclosure agreement. Finally, the statute could prohibit retaliatory firing, so that employees would not be deterred from exercising their rights through the fear of losing their jobs. By statutory

138. While confidential information constituting a trade secret may not pass the strict standard of patentability, it does give the employer a competitive advantage if he succeeds in keeping it secret. Employees usually develop the trade secret for the employer. Under a statute similar to those discussed above, both the employer and employee would better understand their respective positions upon entering the employment relationship.

139. A federal or model state statute would promote uniformity. Key employee mobility extends beyond state lines and therefore a uniform law is imperative.

140. Several practical problems inhere in this proposal. First, no figures are available on the number of computer industry employees who change employment each year. Thus, this proposal seeks to correct an admittedly unquantified problem. Second, an explicit, detailed, frequently updated contract could increase the adversarial nature of the employment relationship. Third, this proposal would highlight the admitted lack of trust which initially prompted action.

The greatest difficulty with private enforcement systems is their cost. Unless a firm can maintain these system costs for less than it would cost to litigate cases concerning misappropriation of trade secrets by key employees, it will have no incentive to implement these programs. Most likely, only firms with large research and development departments will find such a system economically feasible because the cost of such a program would be less than their projected litigation costs.
delineation of trade secret ownership in the employment relationship, private control costs would be reduced.

Alternatively, employers and employees could expand the use of reasonable employee nondisclosure agreements. A firm with a large research and development department might find it profitable to appoint a supervisor to oversee and review on-going projects to determine those which need trade secret protection; after this initial determination the supervisor could prepare a nondisclosure agreement to be signed by employees involved with these projects. If an employee believed that an item did not deserve nondisclosure protection, he could invoke an arbitration procedure similar to the one outlined in the statutory solution set forth above. In firms with smaller research and development departments, existing departmental project supervisors could follow the suggested procedure.

Conclusion

In distinguishing between the knowledge, skill and ability which belong to an employee programmer, and the concept, method or process developed by the employee which belongs to the employer, the courts have failed to articulate a clear standard for balancing competing social policies. Courts have generally favored the interests of the employer without thoroughly considering whether the work product involved warranted elevation to trade secret status. Thus, employers and employees alike are uncertain as to their legal rights. This uncertainty has deterred invention and research and development, and has encouraged unfair practices. The combined statutory and contractual solution suggested in this Note would promote competing social policies and would interject an element of certainty into the employment relationship in the computer software industry.

Laura Wheeler