January 1994

Toward a Clearer Standard of Protectable Information: Trade Secrets and the Employment Relationship

Miles J. Feldman

Follow this and additional works at: https://scholarship.law.berkeley.edu/btlj

Recommended Citation

Link to publisher version (DOI)
https://doi.org/10.15779/Z385386

This Article is brought to you for free and open access by the Law Journals and Related Materials at Berkeley Law Scholarship Repository. It has been accepted for inclusion in Berkeley Technology Law Journal by an authorized administrator of Berkeley Law Scholarship Repository. For more information, please contact jcera@law.berkeley.edu.
COMMENT

TOWARD A CLEARER STANDARD OF PROTECTABLE INFORMATION: TRADE SECRETS AND THE EMPLOYMENT RELATIONSHIP

MILES J. FELDMAN†

Table of Contents

I. INTRODUCTION ......................................................................................................... 152

II. THE TRADE SECRET LAW IN THE EMPLOYMENT CONTEXT CREATES TENSIONS BETWEEN COMPETING INTERESTS. .................................................................................. 153
   A. Definition of a Trade Secret ................................................................................. 153
   B. Secrecy .............................................................................................................. 154
   C. The Problem of Concurrent Interests ................................................................. 155
   D. The Conflict Between the Rights of the Employer and the Rights of the Employee is Particularly Acute in Technology Industries. .................................................................................. 156
   E. Trade Secret Law Offers Potentially Much Broader Protection than Copyright or Patent Law. .......................................................... 158
   F. Emergence of Trade Secret Law in the Computer Industry .................................. 159

III. THE CURRENT STATE OF TRADE SECRET LAW GENERATES UNCERTAINTY ........................................................................................................ 161
    B. Liability for Misappropriation of a Trade Secret .............................................. 163
    C. The Tension Between Protectable “Know How” and Unprotectable “General Knowledge and Skill” ...................................................... 164
    D. Lack of Clarity in the Law of Trade Secrets Hinders Innovation and Frustrates the Purpose of the Law. ............................................... 170

© 1994 Miles J. Feldman.
† J.D. Candidate 1994, Boalt Hall School of Law, University of California at Berkeley; B.A., University of California, Berkeley. I wish to thank Dana M. Newman, General Legal Counsel, Magnasync/Moviola Corp.; Professor Stephen R. Barnett; Ryan S. Bezerra; and Albert and Brenda Feldman.
IV. STRATEGIES FOR GENERATING MORE CERTAINTY IN THE LAW OF TRADE SECRETS IN THE HIGH TECHNOLOGY EMPLOYMENT CONTEXT. ........................................... 173

A. The UTSA Should be Revised to Deal More Directly with the Issue of Concurrent Interests. ...................................................... 173

B. The Dissolution Theory Is Problematic Because the Main Remedy in Trade Secret Law is Injunctive Relief. ..................... 177

C. The Criminal Approach is Not Practical and Shifts the Enforcement from the Parties ..................................................... 178

D. Employment Contracts and Non-Disclosure Agreements .......................................................... 179

V. CONCLUSION ..................................................................................... 182

I. INTRODUCTION

The business of innovation is increasingly competitive, as products quickly become obsolete in the face of rapidly evolving technology. Essential to the success of the technology-based firm are skilled employees with the knowledge and experience necessary to convert information into marketable products. The fast pace of development in the computer industry causes a high rate of employee turnover because companies need to compete for workers proficient in the latest technology. While this increase in employee mobility promotes competition, it also means that employers lose valuable information to their competitors. This problem is particularly acute in the computer industry.

The law of trade secrets protects certain types of confidential information from wrongful disclosure or use. Applied to the employment relationship, the employer’s interest in proprietary confidential information must be balanced against an employee’s right to use his or her skills to earn a living. Trade secret law attempts to strike a balance between these competing concerns. However, trade secret law turns upon an uncertain distinction between trade secrets, which are protectable, and an employee’s own knowledge and skill, which the employee may take to a new job. This uncertainty frustrates the goals of promoting innovation by employers through protection of legitimate trade secrets and allowing employees mobility in their chosen field.

The task of this Comment is to: (1) outline the uncertainties in the law of trade secrets, (2) identify the guidelines courts have used to distinguish protected trade secrets from unprotected employee knowledge and experience, and (3) propose a revision in the Uniform
Trade Secrets Act\(^1\) that reformulates the standard for defining a trade secret by including a specific balancing test to distinguish an employer's protectable "know how" from the employee's unprotectable "general knowledge and skill." This revision will make the law more certain and allow courts reasonable discretion in deciding each case on its specific facts.

II. THE TRADE SECRET LAW IN THE EMPLOYMENT CONTEXT CREATES TENSIONS BETWEEN COMPETING INTERESTS.

The trade secret law protects an employer's confidential information from misappropriation by an employee. Yet an employee has the right to market his or her general knowledge and experience to new employers. A conflict arises where the employee's knowledge and experience is inextricably tied to the trade secrets that belong to a former employer.

A. Definition of a Trade Secret

The Restatement (First) of Torts\(^2\) served as the pattern for state trade secret law until 1979, when the National Conference of Commissioners on Uniform Laws approved the Uniform Trade Secrets Act\(^3\) (UTSA). To date, thirty-six states and the District of Columbia have adopted the UTSA with different variations.\(^4\) In addition to the Restatement (First) of Torts and the UTSA, the recently drafted Restatement of Unfair Competition\(^5\) covers trade secret law.

The Restatement (First) of Torts (Restatement (First)) defines a trade secret as: "any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."\(^6\) The information must be secret: "Matters of public knowledge or of general knowledge in an industry cannot be appropriated by one as his secret." The UTSA defines a trade secret as:

---

2. Restatement (First) of Torts § 757 (1939).
3. UTSA, supra note 1.
4. The following states have adopted the UTSA: Alabama; Alaska; Arizona; Arkansas; California; Colorado; Connecticut; Delaware; District of Columbia; Florida; Hawaii; Idaho; Illinois; Indiana; Iowa; Kansas; Kentucky; Louisiana; Maine; Maryland; Minnesota; Mississippi; Montana; Nebraska; Nevada; New Hampshire; New Mexico; North Dakota; Oklahoma; Oregon; Rhode Island; South Dakota; Utah; Virginia; Washington; West Virginia; Wisconsin. ARIZ. REV. STAT. ANN. § 44, ch. 4, art. 1 (1993).
6. Restatement of Torts, supra note 2, cmt. b.
information, including a formula, pattern, compilation, program, device, methods, technique, or process, that: (i) 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 (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.7

Unlike the Restatement (First) definition, which emphasizes the use of information, the UTSA focuses on the information and expands the definition of a trade secret to include programs, methods, techniques, and processes.8 The UTSA also protects information that has either potential or actual value, and eliminates the requirement that a trade secret be used continuously in the holder's business. Therefore, the UTSA has expanded the definition of what constitutes a trade secret.

The proposed Restatement of Unfair Competition, which is currently being circulated in draft form, takes the more expansive approach of the UTSA. It defines a trade secret as "any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others."9

B. Secrecy

Secrecy, or confidentiality, has emerged as one of the core concepts in trade secret law. It is well-recognized that an employee in the computer industry is entitled to use experience gained while working for a company in subsequent employment. If, however, an employee possesses confidential information or knowledge gained at the employer's expense, the employee has a duty to maintain its secrecy. This principle was applied in one case to prohibit the employee from using technical knowledge of a computer system gained through an employer's training course, or from taking a competitive position that inevitably required the employee to use the protected knowledge.10 The employee was free to apply his knowledge of the computer industry, as long as he did not service the employer's system.

7. UTSA, supra note 1, § 1.
8. Thus, trade secret law protects information and expression that is specifically not protected by the Copyright Act. 17 U.S.C. § 102(b) ("In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.").
9. RESTATEMENT OF UNFAIR COMPETITION, supra note 5, § 39 (emphasis added).
Where the employer fails to take reasonable precautions to protect the secrecy of its computer operations, an employee has no duty to maintain confidentiality. Further, absent reasonable precautions, an employee’s knowledge of the company’s computer system may be considered unprotected general knowledge and experience. In one frequently-cited case, the Supreme Court of Minnesota held that the absence of an understanding not to disclose particular information about the employer’s computer system rendered that information part of the employee’s general skill and experience. The court reasoned that the employer’s failure to take reasonable precautions to protect the confidentiality of its alleged trade secret was such that “the defendant employees could not be expected to have known what was confidential and what was not, what was unfair to disclose and what was not.” To assert trade secret rights in information, the firm or individual must maintain the information at some minimal level of confidentiality or secrecy.

C. The Problem of Concurrent Interests

The central policy conflict in employment trade secret cases is between the employer’s interest in protecting its proprietary information and the employee’s right to use his or her knowledge and skill to earn a living.

This problem can be characterized as “concurrent interests.” The concurrent interests in information potentially covered by trade secret law are best illustrated by cases in which, during the term of employment, an employee acquires skills, information, and knowledge that become unavoidably integrated into her professional identity. The same skills, information, and knowledge can be characterized as the employer’s, because the employer has made investments by training the employee and developing the information. When the employee uses her skills in new employment, some of those skills may be unalterably tied to the trade secret information of the former employer. An employee who changes jobs, but remains in the same profession, may find it impossible to avoid drawing upon the skills and the experience developed at the previous job. Both parties’ interests include private ethical and legal

---

11. See Fishing Concepts v. Ross, 226 U.S.P.Q. (BNA) 692, 695 (D. Minn. 1985) (commenting that the law of trade secrets only protects secret information; where the employer voluntarily reveals information about its computer system, there is no trade secret).


13. Id. at 702.

conceptions of ownership, investment, and the freedom to pursue one's profession.

Public policy considerations such as fostering innovation, advancing science and technology, and promoting free competition serve as the basis for trade secret law. Because of its broad reach, trade secret law's impact on technological innovation is great. Trade secret protection may, however, limit or discourage innovation. Broad legal protection for confidential information benefits an employer and encourages innovation and investment in new technology, because the firm that invests in the research and development of new ideas is protected from "free riders" who can exploit its investment. At the same time, limited protection frees technical workers to use their knowledge and skill in various competing employment opportunities.

Trade secret jurisprudence should enable both employer and employee to pursue their innovative goals by offering clear legal standards that enable the parties to distinguish between protectable and unprotectable skills, information, and knowledge.

D. The Conflict Between the Rights of the Employer and the Rights of the Employee is Particularly Acute in Technology Industries.

The concurrent interest problem is particularly acute in technology-based industries. The computer industry is an archetypal environment for trade secret disputes and concurrent interest problems for two reasons: high employee mobility, and the computer industry's heavy reliance on research and development, which is in turn dependent on information. The highly specialized skills involved and the volatile computer product market combine to cause a great deal of mobility among workers in the computer industry. There is intense competition for employees proficient in the latest technology.

15. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 481 (1974) (the "encouragement of invention" is one of the policies behind trade secret law); E.I. duPont de Nemours & Co. v. American Potash & Chem. Corp., 200 A.2d 428, 437 (Del. Ch. 1964) (trade secret protection tends to encourage "substantial expenditures to find or improve ways and means of accomplishing commercial and industrial goals").

16. This dilemma represents the basic conundrum in all of intellectual property law: the tension between securing rights for innovators by granting them monopolies and the need for the open exchange of information. Cf. Stephen Breyer, The Uneasy Case for Copyright, 84 Harv. L. Rev. 281 (1970); Zechariah Chaffee, Reflections on the Law of Copyright, 45 Colum. L. Rev. 503, 506-511 (1945); see also, Sony Corp. of Am. v. Universal City Studios, 464 U.S. 417, 429 (1984) (stating that congressional interpretation of the intellectual property clause of the Constitution "involves a difficult balance between the interests of authors and inventors in the control and exploitation of their writings and discoveries on the one hand, and society's competing interests in the free flow of ideas, information and commerce on the other").
Because the pace of change in the computer business and computer applications is so rapid, members of the industry change jobs very quickly. According to a 1989 Computer Weekly survey, only catering staff change jobs more often than those working in the computer industry.\textsuperscript{17} The instability is caused by several factors. Voluntary and involuntary departure programs, such as the one IBM used in 1991, are becoming widespread in high-tech firms needing to down-size to stay competitive. In addition many computer firms have had no opportunity to develop employee loyalty due to their relative youth. Finally, a growing pool of independent contractors in the computer work force has made long-term employment with a single firm more unusual.

Hiring employees in high-technology firms often places the employer in a difficult predicament. The scientists and engineers who come to a high-technology company do so with considerable experience and knowledge of their own. In the computer industry, most firms hire these employees because they have knowledge of and experience with particular processes. These processes are, however, often considered proprietary by the employee's prior firm. This exposes firms to potential liability each time it hires a new employee.

In a computer firm, ideas and methodologies are viewed by management as property. Often, knowledge is evaluated solely in terms of market access. More simply, ideas are the primary assets of a computer firm.

In contrast, computer industry employees view information in terms of idea development and career advancement.\textsuperscript{18} Most employees within the computer industry view ideas and methodologies not as property, but as means towards discoveries. The scientific community that produces most high-tech workers is process oriented, and emphasizes the disclosure of discoveries through publication or lecture so that discoveries may be duplicated and verified by others. For scientists and engineers, success is measured by progress and development, rather than in market terms. Thus, employees of computer firms with scientific backgrounds are not accustomed to maintaining the secrecy of scientific discoveries. Further, they may be disinclined to stop publishing or otherwise disclosing their inventions for fear of foreclosing the possibility of an academic career.\textsuperscript{19}

A recent Federal Bureau of Investigation probe presents an extreme example of industry employees' devotion to the information itself. The

\textsuperscript{17} Jonathan Greer-Armytage, \textit{Survey: Staff Mobility}, COMPUTER WEEKLY, July 27, 1989, at 86.


\textsuperscript{19} \textit{Id}. 
Bureau recently investigated a former Apple Computer Corporation engineer for software theft in connection with the Nu Prometheus League. The group is named after the Greek god who stole fire from the gods and gave it to man. The former Apple engineer was served with a grand jury subpoena as a suspect in the on-going investigation of the League’s unauthorized mailing of Apple software to other software developers. The group’s goal, that “the genius of a few Apple employees benefit the entire world,” is apparently motivated by a desire to share philosophical information. The attitudes of the Nu Prometheus League highlight the opposing views of information taken by employees and management. These divergent views exacerbate the concurrent interests problem.

E. Trade Secret Law Offers Potentially Much Broader Protection than Copyright or Patent Law.

Trade secret law is rooted in state common law. Unlike patents, copyrights, and trademarks, it is not preempted from state regulation under the mandate of Constitution’s intellectual property clause.

In Kewanee Oil Co. v. Bicron Corp., the United States Supreme Court held that state trade secret law is not preempted by federal patent law, although protection might overlap. The Kewanee Court reasoned that trade secret law does not interfere with the federal policies behind patent law because it deals with a limited subject matter, offers less protection, and focuses on conduct rather than on technology.

Nor is trade secret law preempted by federal copyright law. In 1992, the United States Court of Appeals for the Second Circuit held in Computer Associates International v. Altai that state law trade secret claims that arise in connection with copyright infringement are not preempted by federal copyright law. The Computer Associates court reasoned that state trade secret law is not preempted by the federal Copyright Act.

21. Id.
22. Id.
23. Id.
26. Id. at 490-93.
27. 982 F.2d 693 (2d Cir. 1992) [hereinafter Computer Associates].
28. Id.
because trade secret claims require proof of an element not included in a copyright infringement claim.\textsuperscript{29}

The independence of state trade secret law from the Copyright and Patent Acts is significant for several reasons: (1) trade secret law creates de facto monopolies over information that are potentially infinite, while copyright and patent law provide monopolies for only a limited duration;\textsuperscript{30} (2) trade secrets can exist without fixation, novelty, or originality;\textsuperscript{31} and (3) trade secret law has emerged from a conflicting body of common law and through relatively insulated state legislative efforts,\textsuperscript{32} while the Patent and Copyright Acts were subjected to rigorous congressional debates before becoming federal law.

F. Emergence of Trade Secret Law in the Computer Industry

Trade secret protection for computer programs is fast emerging as one of the preeminent grounds for asserting legal rights in software.\textsuperscript{33} One of the primary protections for computer software is the federal Copyright Act.\textsuperscript{34} The application of the Copyright Act to computer software has, however, come under severe criticism from commentators and practitioners, who now describe state trade secret law as new and valuable protection for computer software.\textsuperscript{35} The perception that the Copyright Act alone does not provide adequate protection for computer software is partly due to the differences between computer software and other forms of expression covered by the Copyright Act. In the context of the computer industry, establishing protectable expression can be difficult.\textsuperscript{36}

Trade secret law, in contrast to copyright law,\textsuperscript{37} protects ideas that have not been fixed in a tangible medium. The most common trade secret claim in the computer industry deals with the alleged misappropriation

\begin{footnotes}
\item[29.] Id. at 717.
\item[30.] See 35 U.S.C. § 154; see also supra notes 1-15.
\item[31.] See Computer Associates, 982 F.2d at 717; see also supra notes 1-15.
\item[32.] See supra notes 2-9.
\item[33.] See, e.g., Victoria Slind-Flor, More Trade Secret Wars, NAT'L L.J., Mar. 22, 1993, at 1, 34; Michael Greenberger & Robert Wasserman, Keeping Secrets, TEXAS LAWYER, June 14, 1993 at 24 (arguing that recent developments in copyright law suggest that software developers should not rely on copyright protection alone, but should protect valuable software as trade secrets) [hereinafter Keeping Secrets].
\item[34.] 17 U.S.C. §§ 1-810 (1988).
\item[35.] See Keeping Secrets, supra note 33, at 1, 34.
\item[36.] Several recent cases illustrate the complexity and difficulty of establishing protectable expression. See Atari Games Corp. v. Nintendo of Am., 975 F.2d 832 (Fed. Cir. 1992); Sega v. Accolade, 785 F. Supp. 1392 (N.D. Cal. 1992).
\item[37.] 17 U.S.C. § 102(a) (1973).
\end{footnotes}
of computer software. Computer programs have qualified as trade secrets under both the common law definition of a trade secret and the UTSA definition. The UTSA includes the word "program" in its definition of a trade secret. Some states have gone further and amended the definition to specifically cover computer programs. For example, the Idaho statute adds "computer program" to the definition, Montana added "computer software," Alabama omitted "program" but added "computer software," and Nebraska added "code."

For a computer program to be granted trade secret protection, it must be "secret," or not generally known in the industry. Several courts have, however, held that a "unique combination" of programs that are individually generic and publicly known may be protected as a trade secret. In Computer Associates International v. Bryan, the Eastern District of New York held that a trade secret may consist of an accumulation of generic computer programs in the public domain which are linked together in a way not generally known outside the firm. The court reasoned that 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 and operation of which, in unique combination, affords a competitive advantage. Trade secret law can thus protect an enormous amount of information that is not protectable by other means.

38. Trade secret issues also arise with respect to computer hardware, and "shrink-wrap" licenses for widely-distributed software. JAGER, supra note 14, § 9.02[1]-[3].


41. UTSA, supra note 1, § 1.

42. IDAHO CODE § 48-801 (1993).

43. MONT. CODE ANN. § 30-14-402 (1985).


47. Id.

In Computer Associates v. Altai, the Second Circuit noted: “Precisely because [the] trade secret doctrine protects the discovery of ideas, processes, and systems which are explicitly precluded from coverage under copyright law, courts and commentators alike consider it a necessary and integral part of the intellectual property protection extended to computer programs.” 49 The Computer Associates court echoed Milgrim, who stated “[trade secret protection remains a ‘uniquely valuable’ weapon in the defensive arsenal of computer programmers.” 50 Therefore, trade secret law can provide perpetual monopolies over computer programs and surrounding information wholly apart from the heavily legislated copyright and patent laws. Such protection can have a direct impact on technological innovation in this country.

III. THE CURRENT STATE OF TRADE SECRET LAW GENERATES UNCERTAINTY.

The concurrent interest problem and the potential for unrestricted liability, which was created without the extensive policy debates that characterized federal intellectual property legislation, 51 are exacerbated by a legal doctrine steeped in uncertainty and imprecision. The lack of a definitive rule in this area has led the courts to engage in fact-specific, case-by-case analysis, resulting in little uniformity among the computer trade secret decisions. This leaves firms and industry professionals with little or no guidance on how to assess trade secret protection or liability.

The origins, the conflicting theories of liability from which the law developed, and the ill-defined distinction between what is protectable and unprotectable frustrate the legal and social policies that serve as the basis for trade secret law. Knowledge and information are divided between the vague categories of general knowledge and skill, which an employee may freely use in subsequent employment, and know how, which an employer may protect as a trade secret. These categories neither further predictability of trade secret law nor help to establish what is or is not protectable information.

A. Origins of Trade Secret Law: Property or Relationships?

The overall lack of clarity in trade secret jurisprudence can be traced, in part, to the concepts from which the law evolved. Trade secret

---

law is rooted in two distinct legal theories, property and tort, that each raise duties based on special relationships. The emerging view among many state courts is that trade secrets involve rights in property. In 1984, the Supreme Court in *Ruckelshaus v. Monsanto* recognized that trade secrets, although intangible, qualify as property rights and may be protected by the takings clause of the fifth amendment. The *Ruckelshaus* court noted that trade secrets share many of the characteristics of tangible forms of property, such as assignability, the ability to form the res of a trust, and the ability to be passed to a trustee in bankruptcy.

Earlier courts took an entirely different view of the legal foundations of trade secret protection, finding that trade secret protection is based on the existence of a confidential relationship between the parties. An example of the relationship-based conception of trade secret law is Justice Holmes’s opinion in *E.I. DuPont de Nemours Powder Co. v. Masland*. In *Masland*, Justice Holmes expressed the view that property is not the starting point in trade secret analysis. Rather, Justice Holmes stated:

> 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 denied but the confidence cannot be. Therefore the starting point for the present matter is not property or due process of law, but that the defendant stood in confidential relations with the plaintiffs, or one of them.

Significantly, some state courts still agree with this view, and have adopted the principle that trade secret protection is based on a confidential relationship. The relationship between employer and employee is a quintessential example of a confidential agency relationship, in which the employee has a duty to refrain from disclosing

52. MILGRIM, supra note 14, § 1.01 ("[C]ourts have overwhelmingly supported the property view.").
54. Id. at 1002.
56. 244 U.S. 100 (1917).
57. Id. at 102.
58. See, e.g., Wiebold Studio v. Old World Restorations, 484 N.E.2d 280, 284 (Ohio App. 1985) ("The employer who has discovered or developed trade secrets is protected against unauthorized disclosure or use, not because he has a property interest in the trade secrets, but because the trade secrets were made known to the employee in a confidential relationship.").
the employer's confidential information in a way which would harm the employer.\textsuperscript{59}

There are thus two opposing theories of trade secret protection—one emphasizing the nature of the plaintiff's property rights in secret information and the other emphasizing the tort of a defendant's misconduct. The view of trade secrets as property focuses on the status of the information itself, because the party who asserts trade secret rights must establish that the information at issue has been preserved as a protectable trade secret. In contrast, the view of trade secret misappropriation as a tort stresses the conduct of the defendant in breaching a duty to maintain the confidentiality of the trade secret.

Commentators have long complained that courts do not agree on the proper legal rationale for granting trade secret protection.\textsuperscript{60} It could be argued that both theories are reflected in the law because the law requires that a plaintiff prove the existence of a trade secret as well as misappropriation by the defendant.\textsuperscript{61} However, the divergent views on the legal rationales have created jurisprudential difficulties and fostered the uncertainties that exist within trade secret law.\textsuperscript{62}

\section*{B. Liability for Misappropriation of a Trade Secret}

Although the law is not settled, the trend regarding misappropriation is to impose liability, not only for the wrongful use or disclosure of another's trade secret, but also for improper acquisition of another's trade secret. The common law approach imposes liability upon one who discloses or uses another's trade secret if the secret was discovered by improper means.\textsuperscript{63} This approach is based on the tort theory of trade secret protection and focuses on acquisition by "improper means," which is equivalent to breach of a confidential relationship.\textsuperscript{64}

\begin{itemize}
\item \textsuperscript{59} See Ungar Elec. Tools v. Sid Ungar Co., 192 Cal. App. 2d 398, 403 (1961) (noting that courts protect the use of confidential information acquired by an employee in the course of his employment).

\item \textsuperscript{60} Laura Wheeler, \textit{Trade Secrets and the Skilled Employee in the Computer Industry}, 61 WASH. U. L.Q. 823, 826-27 (1982); see MILGRIM, supra note 14, at 1-6 to 1-7 n.15.

\item \textsuperscript{61} See UTSA, \textit{supra} note 1.

\item \textsuperscript{62} See supra note 60.

\item \textsuperscript{63} \textit{RESTATEMENT (FIRST) OF TORTS}, \textit{supra} note 2. The Restatement also imposes liability when: "(2) the disclosure/use constitutes a breach of confidence which arose as a result of the other's disclosure of the trade secret; or (3) the trade secret was learned from a third person with notice of its secrecy and of the third person's having discovered it through improper means, or that the third person's disclosure was otherwise a breach of duty to the other; or (4) the secret was learned with notice of its secrecy and that it was disclosed by mistake." \textit{Id.}

\item \textsuperscript{64} This concept was articulated by Justice Pitney in the seminal case of International News Serv. v. Associated Press, 248 U.S. 215, 235-45 (1918).
\end{itemize}
In contrast, the UTSA imposes liability for misappropriation based on the acquisition of another's trade secret by a person who knows or has reason to know that the trade secret was acquired by improper means.\textsuperscript{65} This is broader than the common law approach, which required an actual use of the trade secret.\textsuperscript{66} The UTSA also imposes liability for misappropriation based on the disclosure or use of another's trade secret without express or implied consent.\textsuperscript{67} This type of misappropriation is entirely consistent with the prior common law. In addition, the UTSA imposes liability when, at the time of disclosure or use, the person knew or had reason to know that his knowledge of the trade secret was either derived from someone who used improper means to acquire it, acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use, or derived from someone who owed a duty to the plaintiff to maintain its secrecy or limit its use.\textsuperscript{68} These provisions, which are based on a duty of confidentiality, are readily applicable to cases involving former employees. Finally, the UTSA imposes liability for misappropriation for disclosure or use of a trade secret where, before a material change of his position, the person disclosing or using the trade secret knew or had reason to know that the information was a trade secret and that knowledge of it had been acquired by accident or mistake.\textsuperscript{69}

Thus, the common law and the UTSA differ on whether mere acquisition of trade secret, without actual use, is enough to trigger liability. This is crucial to cases involving employment in the computer industry, because employees will inevitably bring potential trade secret information into their new firms. As a result, under the common law approach, liability may exist even absent any malicious act of misappropriation. The draft Restatement of Unfair Competition essentially follows the UTSA with respect to liability for appropriation of a trade secret. Both impose liability for the simple acquisition of another's trade secret by improper means.\textsuperscript{70}

\textsuperscript{65} Under the UTSA, misappropriation is also centered around breach of a duty of confidence and the use of "improper means," yet with some crucial differences from the Restatement of Torts standard. The UTSA defines "improper means" to include theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means. Reverse engineering or independent derivation alone do not constitute improper means. UTSA, \textit{supra} note 1, §§ 1(1)-(2).

\textsuperscript{66} Droeger v. Welsh Sporting Goods Corp., 541 F.2d 790, 792-93 (9th Cir. 1976) (holding that it is the defendant's wrongful use of the plaintiff's trade secret which gives rise to liability for damages).

\textsuperscript{67} UTSA, \textit{supra} note 1, § 1(2)(ii)(A).

\textsuperscript{68} Id. § 1(2)(ii)(B).

\textsuperscript{69} Id. § 1(2)(ii)(C).

\textsuperscript{70} \textit{Restatement Of Unfair Competition, supra} note 5, § 40.
C. The Tension Between Protectable "Know How" and Unprotectable "General Knowledge and Skill"

Traditionally, courts have separated protectable and unprotectable information by using the term "know how" to denote protectable information and "general knowledge and skill" to denote non-protectable information. However, these terms do little to clarify or delineate the boundaries of trade secret protection. One commentator defines "know how" as referring to information that enables one to accomplish a particular task or to operate a particular device or process. Others define "general skill" as personal knowledge based on an employee's education, ability, and experience, and general to the trade as a whole, as opposed to knowledge peculiar to the employer.

Courts recognize that the meaning of "know how" is unclear and sometimes overlaps the unprotectable general knowledge of an employee. In 1985, the Third Circuit commented that: "the concept of 'know how' is ... a very fuzzily defined area, used primarily as a short-hand device for stating the conclusion that a process is protectable. It covers a multitude of matters, however, which in the broad sense are not protectable, e.g., an employee's general knowledge and skill." Distinguishing know how and general skill is particularly difficult in the high technology area.

For example, in a recently filed trade secret dispute between manufacturers of ultrasound diagnostic equipment, Advanced Technology sued Siemens Medical Systems, who hired an engineer away from Advanced Technology. The engineer designed ultrasound probes, the crucial component that emits and receives the impulses from an

---

74. Id.
75. Dynamics Research Corp. v. Analytic Sciences Corp., 400 N.E.2d 1274, 1286-87 (Mass. App. 1980) (holding that plaintiff employer was not entitled to restrain the defendant's use of knowledge gained while working on the plaintiff's system, as plaintiff failed to keep the system sufficiently secret).
unborn child that make ultrasound technology useful. Advanced Technology was successful in gaining a temporary restraining order to entirely prevent the engineer from working on such probes at his new employer, despite the fact that the design of them was his field of expertise. This ruling effectively prevented the engineer from engaging in his area of specialization—ultrasound probes.

1. **THE RESTATEMENT OF TORTS AND THE UTSA**

The Restatement of Torts, which is still followed by many jurisdictions, offers no clear rule regarding what constitutes "general knowledge." The Restatement comes closest to addressing this issue, albeit indirectly, through its articulation of one of the factors that compose the test for whether information constitutes a trade secret: "the extent the information is known outside of the business." The present formulation of the UTSA also does not adequately confront the problem of defining the terms "general knowledge and skill" or "know how." The UTSA expanded the definition of a trade secret to expressly include "programs" and "know how." Nevertheless, the definition is circular; the designation "know how" merely denotes protectable information. The UTSA does not specifically define "know how," and, like the Restatement of Torts, the UTSA is silent as to what constitutes unprotectable "general knowledge" and skill. This absence of an express definition has led to an inconsistent and often unfair application of trade secret law in the courts.

2. **INCONSISTENCY IN TRADE SECRET DECISIONS**

*Structural Dynamics Research Corp. v. Engineering Mechanics Research Corp.* was a trade secret action in which Engineering Mechanics employed a former Structural Dynamics employee. The dispute centered around computer software that Structural Dynamics developed to implement isoparametric elements in structural analysis. The Eastern District of Michigan stated in dictum that no duty to refrain from using or disclosing information arises where the trade secret is created through the employee's initiative. In such a case, the employee has an interest in the information that is at least equal to that of the employer; the knowledge is

77. Id.
78. RESTATEMENT OF TORTS, *supra* note 2.
79. Id.
80. UTSA, *supra* note 1, § 1 cmt.
82. Id.
part of his skill and experience. 3 The court held, however, that the employees were liable for subsequent use or disclosure of the technology because they had signed an express "Employee Patent and Confidential Information Agreement." 4

The Fifth Circuit followed this reasoning in Plains Cotton Co-op v. Goodpasture Computer Services, 5 where the defendant employee[s] developed particular ways to use the software. The software, Telcot, was designed to provide information regarding cotton prices and availability to the members of a cotton growing trade association. 6 The Plains Cotton court found that the defendant[s] had brought significant expertise in software development to the plaintiff firm. 7 Based on this finding, the court denied the plaintiff's motion for a preliminary injunction to prevent the defendant[s] from using the software functions in other applications. 8 Although the court acknowledged that the defendant employees had access to Telcot's object and source code, 9 the court found no evidence of copying, because the defendants used their expertise to develop the new software at the defendant firm. 90

The same reasoning appeared again in Universal Analytics v. MacNeal-Schwendler Corporation, 91 which involved a trade secret claim brought pendant to an antitrust claim under the Sherman Act. 92 In Universal Analytics, both parties employed some of the same employees simultaneously. The federal district court reasoned that "[s]ecrets acquired and developed as a result of a long employment in the particular trade may be carried over and put to use by the new employer." 93

The line of authority established in Structural Dynamics, Universal Analytics, and Plains Cotton allows employees who substantially participate in the development of computer software to continue using the experience gained in their previous firm, even where the new firm's software is similar in application to the previous firm's software. This line of cases is not, however, the only approach.

83. Id. at 1114-1116.
84. Id.
85. 807 F.2d 1256, 1263 (5th Cir. 1987)
86. Id. at 1258.
87. Id.
88. Id.
89. Id.
90. Id.
92. Id. at 1177.
93. Id. at 1178; see also Sarkes Tarian, Inc. v. Audio Devices, Inc., 166 F. Supp. 250 (S.D. Cal. 1958); Josten's, Inc. v. National Computer Sys., Inc., 318 N.W.2d 691, 701, 702 (Minn. 1982).
The Court of Appeals for North Carolina recently upheld a preliminary injunction in Barr-Mullin, Inc. v. Browning. The Barr-Mullin court found that a prima facie case of misappropriation existed where the defendant helped to develop and service computer software during his employment with plaintiff, then subsequently developed similar software after leaving the plaintiff employer's firm. The software was developed for the woodworking industry to optimize the way lumber is cut. The employee, a former vice president of engineering at the plaintiff firm, claimed that he had independently derived the subsequently developed software. The court reasoned that the employee's contribution to the defendant's software development demonstrated his knowledge of the alleged trade secret and proved that he had access to copies of the source code prior to his resignation. Contrary to Plains Cotton, the Barr-Mullin court made no mention of the employee's rights to his knowledge and skills in its reasoning. Further, the Barr-Mullin court held that access to the original software prevented the defendant employee's assertion of independent development.

Other cases challenge the logic of Structural Dynamics, Universal Analytics, and Plains Cotton. In the recent case of Avtec Systems, Inc. v. Peiffer, Avtec asserted trade secret rights in a computer program that the defendant developed as a marketing tool while employed by Avtec. The employee used the program as a demonstration and marketing device several times on plaintiff's behalf. The Eastern District of Virginia found that the plaintiff acquired a trade secret in the program's use for demonstrations and marketing in a manner similar to an employer's possession of "shop rights" in an employee's invention. The court held that the use of the program by the defendant was a

95. Id. at 228.
96. Id.
97. Id.
98. Id. at 230.
99. Id.
101. Id. at 1320.
102. Id.
103. The doctrine of shop rights permits an employer to use an idea submitted by an employee, without compensation to the employee, to the extent that the idea pertains to the employer's business and was generated on company time using company materials and personnel. JAGER, supra note 14, § 8.02. The issue of employers' and employees' respective rights regarding employee inventions also arises in patent and copyright law, and is regulated by statute in some states See, e.g., CAL. LAB. CODE § 2870; ILL. REV. STAT. ch. 140, § 301; MINN. STAT. ANN. §181.78; N.C. GEN. STAT. § 66-57.1; WASH. REV. CODE ANN. § 49.44.140.
misappropriation of his former employer’s trade secret.¹⁰⁴ Like the Barr-Mullin court, the Avtec Systems court made no mention of an employee interest in the information used to create the software, even though the employee substantially assisted in developing it.¹⁰⁵ These cases demonstrate the pattern of inconsistency present in trade secret decisions involving computer software.

There is so much confusion in this area that nearly identical facts can produce different conclusions. Compare two cases that arose in the chemical industry: Wexler v. Greenberg¹⁰⁶ and Basic Chemicals v. Benson.¹⁰⁷ In Wexler, defendant Greenberg was head chemist at plaintiff’s chemical company, where he developed various formulas for plaintiff in the course of his duties. Greenberg came to know all of the plaintiff’s formulas, as well as their methods and costs of production. Greenberg left his job with the plaintiff to work for one of plaintiff’s distributors, which soon began to manufacture the same products it had formerly bought from plaintiff.¹⁰⁸ The Pennsylvania Supreme Court held that Greenberg did not violate any confidential relationship “in disclosing or using formulas which he developed or were developed subject to his supervision . . . this information forms part of the technical knowledge and skill he has acquired by virtue of his employment with [the plaintiff] and which he has an unqualified privilege to use.”¹⁰⁹

Faced with an almost identical set of facts, the Supreme Court of Iowa reached the opposite result in Basic Chemicals v. Benson. In Basic Chemicals, the court held that the employee-developed formulas used by plaintiff were trade secrets.¹¹⁰ The Basic Chemicals court found that the protectability of the information was not affected by the fact that Benson, the employee and defendant, developed the formulas; Benson’s right to use the secrets in competition with Basic Chemicals was no greater than any other employee’s.¹¹¹ The court’s reasoning rested on the fact that Benson had previously referred to the formula as his employer’s “know

¹⁰⁴. 805 F. Supp. at 1320. In one closely watched case currently being litigated, IBM is seeking an injunction barring a former employee specially skilled in the field of magnetic resonance heads for computer disk drives from working for a competitor in a position involving development of magnetic resonance disk drive heads, as he would inevitably disclose IBM’s trade secrets in this technology. Seagate Technology v. IBM Corp., 962 F.2d 12 (8th Cir. 1992).
¹⁰⁵. Id.
¹⁰⁷. 251 N.W.2d 220 (Iowa 1977).
¹⁰⁸. 160 A.2d at 433-436.
¹⁰⁹. Id. at 437.
¹¹⁰. 251 N.W.2d at 230.
¹¹¹. Id. at 229-30.
Consequently, the court barred Benson from using the formulas in later employment.

Another example of different results being based on similar facts is evident when AMP Inc. v. Fleischhacker is compared with Air Products & Chemicals v. Johnson. Each case involved a high-level managerial employee who used knowledge of marketing and business operations gained while employed by the plaintiff in a subsequent position with the plaintiff's competitor. In AMP, the Seventh Circuit, following Illinois law, held that the former employer was not entitled to injunctive relief because the business and technical information at issue was general knowledge, widely known in the industry. AMP found that, although an employee derives some benefits from his access to the collective experience of his or her employer, "[s]uch information comprises general skills and knowledge acquired in the course of employment. Those are things an employee is free to take and use in later pursuits." In contrast, the Air Products court ruled that information known to the employee, including knowledge of market opportunities, research and development projects, and pricing methods, was not "generally known in the industry" and was thus protectable as a trade secret. The Air Products court enjoined the employee from working for the plaintiff's competitor. Although both courts applied the same common law definition of a trade secret, the end results were diametrically opposed.

The uneven application of trade secret law in the context of employment in the computer software and technical fields, illustrated by the above cases, can frustrate both an employee's ability to obtain new employment and an employer's right to hire skilled employees. When an employee changes jobs within the same profession or trade, it is often impossible for him or her to avoid using skills and experience gained in previous positions. The exception from trade secret protection for employee skill and knowledge is essential to fostering employee mobility and the competitive basis of our free market economy: "[a]ny other rule

112. Id.
113. 823 F.2d 1199 (7th Cir. 1987).
115. 823 F.2d at 1205-06.
116. Id.
117. 442 A.2d at 1122.
118. C.f. Maloney v. E.I. DuPont de Nemours & Co., 352 F.2d 936, 939 (D.C. Cir. 1965) (stating in the context of employment contracts that employers "will wish to avoid even the threat of [trade secret] litigation").
119. See, e.g., E.I. Du Pont de Nemours & Co. v. American Potash & Chem. Corp., 200 A.2d 428, 437 (Del. Ch. 1964) (acknowledging the inherent conflict created when an employee is asked "to work in a trade secret area and thereby circumscribe his possible future liberty of action and the use of the knowledge and skills which are inextricably interwoven with his knowledge of the trade secrets").
would force a departing employee to perform a prefrontal lobotomy on himself or herself." 120 The current state of the law leaves firms and employees with little guidance as to what a new employee may bring to a new position at a competing firm.

D. Lack of Clarity in the Law of Trade Secrets Hinders Innovation and Frustrates the Purpose of the Law.

The uncertain state of trade secret law has a very real impact on computer and other technology-based firms that cannot readily distinguish protectable information from non-protectable information. As a consequence, the engagement or disengagement of employees subjects firms to unknowable risks and does not allow for proper risk allocation and decision-making. The uncertainty in trade secret law creates societal costs as well, because high litigation expenses reduce resources available for the development of new technology.

Litigating intellectual property disputes is expensive. For example, in the recent patent and trade secrets litigation over data-compression software between Microsoft and Stac Electronics, Stac spent approximately $500,000 per month—nearly $7 million for the entire trial. 121 Gary Clow, Stac's chief executive officer, stated, "I've got the most expensive legal education in the United States." 122 The case "transformed Stac from a company banking on its technology to a company praying for its lawyers." 123 Another trade secret dispute occurred between Titan Linkabit Corporation and Conquest Technologies after Conquest hired former Titan employees. 124 According to Conquest's founder, Titan's suit was merely an attempt to put his start-up out of business before it got off the ground by burying it in litigation costs. 125 Litigation thus drains valuable capital. The uncertainty in the area of trade secret law further aggravates the situation because companies do not know where they stand with respect to potential liability.

The uncertain status of what constitutes unprotectable employee knowledge and skill is inefficient because it results in both over-deterrence and under-deterrence. The deterrent effect arises from the remedies under trade secret law, which sanction an employee's improper use or acquisition of information, and deter the employee, as

120. AMP v. Fleischhacker, 823 F.2d at 1205 (quoting Fleming Sales Co. v. Bailey, 611 F. Supp. 507, 514 (N.D. Ill. 1985)).
121. Craig Rose, Microsoft May Gain From Stac's Win, SAN DIEGO UNION-TRIBUNE, Mar. 1, 1994, at Cl [hereinafter Microsoft May Gain].
122. Id.
123. Id.
125. Id.
well as a prospective employer, from appropriations that trigger a cause of action. The ambiguity in the law frustrates this deterrent effect because the uneven application of an ambiguous doctrine creates rules which either permit too much misappropriation, or overly restrict employee mobility. Under-deterrence allows the employee to unfairly exploit confidential information gained in a former position for the benefit of himself or a new employer. Over-deterrence impedes the employee who has a legitimate right to use knowledge gained through employment. A more certain rule would help to adjust the risks of litigation so that neither misappropriating employees nor over-protective employers may take advantage of the rule’s lack of clarity.

Over-deterrence occurs in a situation when the parties lack an understanding of what constitutes a trade secret. For example, the possibility of litigation may discourage an employee from using his or her skills and experience to pursue a position at another firm. This creates over-deterrence because it inhibits an employee’s ability to change jobs, which creates an economic inefficiency. The fear of a potential trade secret suit may also over-deter potential employers from hiring a competitor’s former employees, even in industries with high employee mobility.¹²⁶

Ambiguity in the law also creates under-deterrence. The absence of a distinct legal rule gives both employees and their prospective employers an incentive to capitalize on information that is not rightfully theirs. The employer may not be able to assess whether the information is protectable as a trade secret. Moreover, the parties will be uncertain as to who will ultimately prevail in litigation. The uncertainty of prevailing combined with the high costs of litigation reduces the risk of loss to the employee who then has a greater incentive to misappropriate. A more certain rule would help to adjust the risks of litigation so that neither party will take advantage of an unclear rule.

Finally, greater clarity is necessary because the number of trade secrets suits being brought by employers is rapidly growing.¹²⁷ The lack of clear rules prevents quick resolution of trade secret disputes, which can be very costly and have a significant impact on the reputation and viability of a firm.¹²⁸ The time consumed and prestige lost in such suits drain computer firms’ resources as much as the monetary costs of the litigation.

¹²⁶. *AMP*, 823 F.2d at 1205 (quoting Harley & Lund Corp. v. Murray Rubber Co., 31 F.2d 932, 934 (2d Cir. 1929): “[I]t has never been thought actionable to take away another’s employee, when the defendant wants to use him in his own business, however much the plaintiff may suffer. It is difficult to see how servants could get the full value of their services on any other terms . . . .”).
¹²⁸. See *Advanced Tech*, *supra* note 76, at 1-4; *Microsoft May Gain*, *supra* note 121, at C1.
The well-publicized dispute between Symantec, a Silicon Valley software producer, and Borland International is a good illustration. Symantec now faces both civil and criminal suits for trade secret misappropriation because it hired Eugene Wang, a senior executive at Borland, who is accused of misappropriating trade secrets. Symantec's stock plunged on news of the dispute and its chief executive officer, Gordon Eubanks, claimed that he spends about one hour per day on the dispute. This time would have been spent more efficiently on the company's business.

IV. STRATEGIES FOR GENERATING MORE CERTAINTY IN THE LAW OF TRADE SECRETS IN THE HIGH TECHNOLOGY EMPLOYMENT CONTEXT.

A. The UTSA Should be Revised to Deal More Directly with the Issue of Concurrent Interests.

Federal regulation of trade secrets is not the answer. Congress has failed to respond to the continued judicial confusion in the area of trade secret law with respect to the problem of concurrent interests in the employment context. National legislation would likely be politically difficult. A more realistic strategy is that of the UTSA, which was formulated by the American Bar Association. The UTSA has helped to bring some uniformity to the law, but it has not been adopted by all states. The main problem with the UTSA is that it merely codifies the Restatement (First) of Torts when identifying trade secrets and resolving the problem of concurrent interests. The UTSA should be revised to meet the needs of the modern employment relationship. Once the revisions have been implemented, all of the fifty states should adopt the UTSA.

Resolving uncertainty in trade secret law presents a significant challenge to policy makers. An effective approach must evenly apply trade secret protection to increase certainty in the employment relationship in high technology areas. To ensure even application and consideration of the concurrent interest problem, the current standards articulated by the UTSA should be changed to incorporate a secondary test that balances employer and employee interests. While such an approach is not novel, it would acknowledge the tension between an

130. Id.
131. Wheeler, supra note 60, at 843.
132. See Wheeler, supra note 60, at 843, 846 (proposing that statutes be expanded to encompass a definition of parties' ownership rights in trade secrets, and noting that a federal statute is warranted though not likely).
employer’s right to protect its investments and an employee’s right to practice her profession.

It would be difficult—if not impossible—to construct a single definition of "general knowledge" or "know how" that would apply in all cases. Thus, trade secret analysis in the employment context must balance relevant considerations. A few courts have employed balancing tests in the past; but to promote consistency and fairness, the courts should look at the facts of a case within an established, uniformly applied framework.

1. BASIS FOR THE TEST

The newly-drafted Restatement of Unfair Competition significantly advances the development of the trade secret law because it sets forth several relevant considerations and expressly addresses the issue of whether information comprises an employer’s protectable trade secret or an employee’s general skill, knowledge, training, and experience. Yet the proposed Restatement falls short of resolving the outstanding issues; it only discusses the factors to be considered in delineating employer/employee interests in information in comment d to section 42, which covers employee liability. Thus, the proposed draft only tacitly addresses the problem of identifying general knowledge and know how as metaphors for employee and employer interests.

The factors outlined in the proposed Restatement include: (1) whether the information at issue is specialized and unique to the employer’s business or is "widely known in the industry or derived from skills generally possessed by persons employed in the industry"; (2) the

133. See, e.g., In re Innovation Constr. Sys., 793 F.2d 875, 879 (7th Cir. 1986) (supporting a balance between the competing interests of employers in precluding employees from exploiting specialized knowledge gained through their employment and employees in the general use of their skills and training); Amoco Prod. Co. v. Lindley, 609 P.2d 733, 745 (Okla. 1980) (noting that courts balance the equities between the right of the company to use its employees and resources to its advantage against the right of the highly developed mind and skill of the employee).

The Amoco court also set forth several factors to be considered:

how many of the innovative elements in the newly developed process are available in the prior art; how closely tied is the development to intrinsic knowledge of the innovator ... is it possible to sort out the process from the inner workings of a man’s knowledge; did the company treat the innovation with the requisite secrecy to place others on notice of its claim ... [o]ther considerations are time and money and company facilities used in its production, and the employer’s own knowledge thereof.

Id.

134. Section 42 of the Restatement of Unfair Competition provides, “An employee or former employee who discloses or uses a trade secret owned by the employer or former employer in breach of a duty of confidence is subject to liability for appropriation of the trade secret ...” RESTATEMENT OF UNFAIR COMPETITION, supra note 5, § 42.
"relative contribution of the employer and the employee to the development of the information"; (3) whether "other competitors have been unsuccessful in independent attempts to develop the information"; (4) whether the employee, upon termination of the employment, appropriates some "physical embodiment" of the information; and (5) whether the information is "so closely integrated with the employee's overall employment experience that protection would deny the employee the ability to obtain employment commensurate with the employee's general qualifications."135

This analysis functions as a valuable default rule, which comes into play when there is no confidentiality agreement between the parties. These factors help to articulate and identify the concurrent interests of employers and employees and take into account the highly fact-specific nature of trade secret disputes involving former employees. By focusing on the nature of the information itself, as well as on the conduct of both the employer and the employee, the test acknowledges the competing goals of protection of confidential information and promotion of employee mobility. Courts should use these factors to guide their determinations, allowing parties to anticipate their trade secret rights and duties and to plan accordingly.

The balancing test should not be part of the plaintiff's prima facie case, but becomes relevant only after the plaintiff alleges the existence of a trade secret and the employee raises the defense that the information forms part of his general knowledge and skill. The plaintiff must prove some basic level of secrecy or confidentiality before the court addresses the concurrent interest problem; absent confidential information, there is no need to balance. In addition, the plaintiff must show misappropriation of the confidential information. Only after the plaintiff has shown the existence of a protectable trade secret should the court seek to identify the concurrent interests by addressing the issue of general knowledge versus know how.

2. TEST FOR DELINEATING "GENERAL KNOWLEDGE AND SKILL" FROM "KNOW HOW"

Under this test, a court should determine whether information is a protectable trade secret or part of the employee's general knowledge and skill by weighing the following factors:

(1) Did the employee develop the disputed information? This factor incorporates the Wexler line of cases, which recognize an employee's interest in information or a process which he or she originated. If, however, the employee signed an agreement assigning all rights in any inventions to the employer, the fact

135. Id. at cmt. d., p. 95.
that the employee developed the information will not support a finding that the information is part of the employee's own general skill and knowledge.

(2) Is the information unique to the employer’s business? This factor helps to determine whether the information is part of the collective knowledge of individuals employed in the industry.

(3) Have competitors been unsuccessful in independent attempts to develop the disputed information? This factor helps to clarify the second factor because a competitor’s failure to develop or produce the information indicates that it is particular to the employer and may thus qualify as a trade secret.

(4) Has the employee, upon termination of the employment, appropriated some physical embodiment of the information, such as a written formula, blueprint, plan, or list? If so, this points toward a finding that the information is a trade secret. When, to the contrary, an employee draws on information in his memory, the information is more likely part of the employee’s general knowledge and experience. A defendant's reliance on memory should not, however, preclude trade secret protection in every case. A protectable trade secret is not always written down or otherwise recorded. In contrast to copyright law, the distinction between knowledge of a concept or idea and a fixed expression of information is unimportant because trade secret law expressly protects intangible information such as methods, techniques, and processes that an employee may have memorized.

(5) Is the information so closely integrated with the employee’s overall experience that granting trade secret protection would deny the employee the ability to obtain employment commensurate with his or her general qualifications? This last factor addresses the public interest in employee mobility.

The balancing test should be flexibly applied, with no one factor being determinative. All factors should be given relative weight by the court. This is necessary because the variety of factual scenarios which trade secret litigation presents requires flexibility.

The suggestion that courts should engage in a balancing test in cases involving employee knowledge may be disquieting to some. After all, it only adds to an already extensive list of elements that must be established to prevail on a claim for misappropriation of trade secrets. Such a

136. AMP Inc. v. Fleischhacker, 823 F.2d 1199, 1204-05 (7th Cir. 1987) (refusing to grant an injunction for the employer in the absence of any evidence that the defendant employee “ever systematically recorded, copied, compiled, or even purposefully memorized any of AMP’s confidential business information. . . .”).

137. See, e.g., Allen v. Johar Inc., 823 S.W.2d 824, 827 (Ark. 1992) (finding that whether the information used was written down or memorized is immaterial; the proper issue is whether it is protectable as a trade secret).

balancing test, it may be argued, does not help to clarify the law but instead makes the law more complex. The answer to such an argument is that the balancing test clarifies the existing factors and gives notice to potential litigants of the application of the factors. As a result, the balancing approach, which is based on the UTSA and the Restatement of Unfair Competition, would streamline trade secret law by adding clarification and specificity and by fostering more fair and efficient results.139

The parties may contract around these factors, if they so desire. The balancing test operates as a default rule, providing direction when there is no agreement between the parties.

The nature of the conflict between employers and employees suggests this solution. The tension between employee mobility and the protection of rights in confidential information cannot be reconciled with a single bright-line rule because it is impossible to satisfy both interests at the same time. Surely, an employee is not free to take a job in his field of expertise if his former employer is able to enjoin him from using knowledge and experience gained while working for the former employer. Conversely, an employer’s rights in confidential information lose much of their value if that same information is being used by a former employee who is now working for a competitor.

The balancing test proposed in this Comment would provide better guidance to employers and employees as to their respective rights, and would assist courts deciding trade secret cases in reaching fair and consistent results. Further, the balancing test will help minimize trade secret misappropriation and groundless trade secret cases while promoting employee mobility and employer development.

B. The Dissolution Theory Is Problematic Because the Main Remedy in Trade Secret Law Is Injunctive Relief.

Various commentators have suggested solutions to the underlying policy dilemma present in current trade secret law. In 1988, Suellen Lowry presented a compelling argument in which she characterized the problem of the competing interests in trade secret law as cases of “inevitable disclosure.”140

These are the hard cases where employees acquire skills and knowledge directly related to an employer’s trade secrets then seek

139. A similar factor-based approach is used by the Ninth circuit in trademark infringement cases brought under the Lanham Act for determining likelihood of confusion. See, e.g., AMF Corp. v. Sleekcraft Boats, 599 F.2d 341, 348-49 (9th Cir. 1979).
employment at another firm.\textsuperscript{141} Lowry asserted that in these situations, the information will inevitably be disclosed. Lowry argued that in “inevitable disclosure” trade secret cases, the problem should be seen as involving a dissolution of concurrent property interests, such as in the law of tenancies in common and community property.\textsuperscript{142} She argued for a new regime patterned on marital dissolutions.\textsuperscript{143} Under Lowry’s proposal, courts would engage in a valuation of the trade secret, and then would allocate the value between the parties.\textsuperscript{144} The court would, in effect, create a licensing scheme.\textsuperscript{145}

There are three problems with this approach. First, the primary remedy sought in trade secret cases is injunctive relief. Any type of an enforced license frustrates the purpose of an injunction which is to completely restrict the employee or the new firm from using the protected information. An injunction is an important remedy because the original firm could be ruined by the mere disclosure of the confidential information to its competitors. Second, Lowry’s proposal could be abused by a firm that first sought a license but was refused, then sued for one under dissolution theory. Third, arriving at appropriate valuations of concurrent trade secret interests will be difficult. Judicial valuations that use market values of information may not be accurate, because the plaintiff firm may not have made a profit before the misappropriation. Because of the difficulty in making valuations, Lowry’s approach does not further predictability before litigation.

C. The Criminal Approach is Not Practical and Shifts the Enforcement from the Parties

In some states, criminal sanctions, in addition to civil liability, are available against a former employee who steals scientific or technical information.\textsuperscript{146} While several recent appellate cases have upheld convictions under these statutes,\textsuperscript{147} criminal trade secret cases are much less common than civil suits; the law concerning what constitutes a trade

\textsuperscript{141} Id.
\textsuperscript{142} Id.; see also Bruce Alan Kugler, Limiting Trade Secret Protection, 22 Val. U. L. Rev. 725, 757 (1988) (proposing that trade secrets should be categorized as either “property quality” or “nonproperty quality” using a quasi-patent analysis, and that “property quality” trade secrets would require only implied notice to the employee and be protected for an unlimited amount of time, while “nonproperty quality” trade secrets would require actual notice to the employee and have a restricted period of protection).
\textsuperscript{143} Id.
\textsuperscript{144} Id.
\textsuperscript{145} Id.
\textsuperscript{146} See, e.g., CAL. PENAL CODE § 499c (b) (West 1988); TEX. PENAL CODE ANN. § 31.05 (West 1989).
secret under various penal codes is still developing. As discussed above, both criminal and civil cases involving the use of electronic mail by two top executives at Symantec Corporation, a Silicon Valley software firm, are pending.\footnote{148}{Tom Abate, Symantec Chief Charged in Trade Secrets Case, S.F. EXAMINER, Mar. 5, 1993, at A-1 [hereinafter Chief Charged].} The computer industry is closely following the Symantec case due to its possible impact on the definition of a trade secret under criminal law.\footnote{149}{Ken Siegmann, 2 Symantec Execs Indicted in Secrets Case, S.F. CHRONICLE, Mar. 5, 1993, at D1; Chief Charged, supra note 148, at A-1.}

While increased criminalization of trade secret law would function as a potent deterrent to misappropriation, it may create more problems than it resolves. For example, it would further deter employee mobility in the computer industry. At the same time, it does not adequately address the problem of securing enforceable rights for employers engaged in technological innovation.

The competing concurrent interests in information also make it difficult to assess criminal culpability, because ownership in the information is subject to uncertainty. Moreover, the limited resources of most prosecutors’ offices makes criminal enforcement possible only in the clearest cases. Donald Ingraham, Assistant District Attorney for Alameda County, has commented that if a company believes they have a trade secret dispute, “the first step is not to call the local district attorney’s office.” His office turns away over half of the trade secret cases reported on the initial call.

D. Employment Contracts and Non-Disclosure Agreements

One way a firm can achieve certainty about what is a protected trade secret is to draft non-competition and non-disclosure agreements. A majority of courts will enforce a covenant restricting an employee from competing with a former employer so long as it is reasonable in scope, territory, and duration, and is necessary for the protection of the employer.\footnote{150}{JAGER, supra note 14, § 13.01[2].} Some jurisdictions, however, take a more strict view and ban all restrictions on an individual’s ability to engage in a profession.\footnote{151}{See, e.g., CAL. BUS. & PROF. CODE § 16600 (West 1987) (“every contract by which anyone is restrained from engaging in a lawful profession, trade or business of any kind is to that extent void”).}

Covenants not to compete are distinct from non-disclosure or confidentiality agreements, which prohibit only an employee’s unauthorized disclosure of an employer’s confidential information, and which are generally upheld.\footnote{152}{JAGER, supra note 14, § 13.01[1].}
Contractual agreements regarding confidentiality and ownership of technological information can be critical to the determination of liability in computer industry trade secrets cases. Besides helping to define exactly what it is that an employer considers to be its trade secret, a written nondisclosure agreement serves notice to an employee of the confidential nature of the employer's proprietary information. While the mere existence of such a contract will not be determinative, it greatly increases the probability that an employer will obtain relief for breach of contract, even where the confidential information or technology does not qualify as a trade secret.

In most computer trade secret cases in which the employee signs a nondisclosure agreement, the computer programs at issue are found to be trade secrets and the courts rule in favor of the employer. For example in Healthcare Affiliated v. Lippany, Healthcare Affiliated hired Lippany to develop computer programs for hospital management systems. Lippany signed a contract agreeing that any processes or methodologies developed by him during his employment with the plaintiff were the property of the plaintiff and agreeing to preserve the confidentiality of plaintiff's methodologies (which included a computer system defendant developed). The Western District of Pennsylvania granted a preliminary injunction in favor of the plaintiff, based on the defendant's having agreed that his efforts toward developing and enhancing the plaintiff's computer systems would inure to the plaintiff's benefit: "Equity will not permit him to appropriate plaintiff's systems, methodologies and programs for his own personal benefit."

Having key employees sign a confidentiality agreement which states that any computer system, methodology, or product information

---

153. See, e.g., Cybertek Computer Prods. v. Whitfield, 203 U.S.P.Q. (BNA) 1020, 1023 (Cal. Super. Ct. 1977) (Employee Nondisclosure Agreement executed by former employee which provided that all techniques and methods relating to plaintiff employer's computer system were trade secrets and confidential was given "considerable weight" in the court's finding that defendant was liable for disclosing and utilizing substantial aspects of plaintiff's system in the development of a similar system for a competitor).


157. Id. at 1155-56.
now in existence, or that may be developed by an employee, is confidential and not to be disclosed to anyone outside of the company without appropriate controls to insure its confidentiality, is vital to a high-technology company's success in maintaining trade secret protection for its computer operations. Courts have tended to uphold such agreements, which provide a basis for contractual remedies; moreover, a valid nondisclosure agreement can facilitate proving the confidential relationship necessary for trade secret protection of the information at issue.

1. Problems with Confidentiality Agreements

The problem with confidentiality agreements is that they are not always available to new or smaller firms, which have only limited access to legal counseling. Disputes usually arise after the employment relationship has ended, whereas confidentiality agreements must be secured at the outset of the employment relationship when its termination is often not contemplated by either party. Additionally, employees generally do not anticipate changing firms when they are signing non-disclosure agreements. There is also the problem of trying to protect the unknown—it may be impossible to define the trade secret at the outset of the employment relationship, because the underlying research and development has not yet been done.

Scientists and engineers who understand the mercurial nature of the technology industry are reluctant to sign confidentiality agreements because they do not want to sacrifice their future mobility. This can cause problems for emerging firms who need to attract top technical workers. In larger firms, technical workers do not have the leverage to abstain from executing an agreement because they have less bargaining power. In these situations, employees are generally not compensated for their decreased mobility.

Employees who have signed confidentiality contracts may discover that potential new employers are skittish about hiring them because they fear litigation.\footnote{Magee Harett, \textit{Wait! Don't Sign That Employment Contract}, EDN, Nov. 14, 1991, at 57.} For example, an employee with a confidentiality agreement with Microsoft will not be an attractive hire to a company with a small litigation budget because Microsoft has a legal department of over 50 lawyers and has a reputation for aggressive litigation.\footnote{Microsoft May Gain, supra note 121, at C1.
2. **RECOMMENDATIONS FOR DRAFTING EMPLOYMENT NONDISCLOSURE AGREEMENTS**

To provide protection for confidential proprietary information, a firm should use an employment nondisclosure agreement which includes the following provisions:

1. All aspects of information not published or generally known in the industry are to be treated as the employer’s confidential or proprietary information until they become publicly available.
2. Employees agree that they will not discuss confidential information outside of the workplace. All publications or presentations dealing directly or indirectly with the confidential information must be cleared by the employer in advance.
3. All documents containing confidential information must be stamped “Proprietary Information” or “Company Confidential,” and may be distributed only to those who have a need for the information in their work. Documents should not be reproduced unnecessarily, and should be disposed of in a manner which ensures that they will not be available to unauthorized persons. Employees agree to return all tangible forms of confidential information to the firm upon termination or at the firm’s request.
4. Employees agree to disclose and assign to the employer all rights in all inventions or ideas relating to their work at the firm or that are aided by the use of the firm’s equipment, facilities, or supplies.
5. Employees agree to hold in confidence, and not use or disclose without the firm’s written authorization, any information obtained or created during the period of employment, which pertains to any aspect of the firm’s business and is unknown to actual or potential customers.
6. Employees represent that they have not brought and will not bring or use in the performance of their duties any proprietary or confidential information, whether or not in writing, of a former employer without that employer’s written authorization.
7. The agreement survives the employee’s employment at the firm.

**V. CONCLUSION**

In the context of the employment relationship, trade secret law has become one of the primary tools for protecting computer software and other high-technology information. Protecting an employer’s exclusive trade secret rights in properly guarded confidential information is critical to technological development and economic growth, especially in computer and technology based firms. Yet trade secret protection must not be used as a weapon by employers to restrain employee mobility or the development of new technologies.
Trade secret law remains uncertain and subject to uneven application. Such uncertainty creates difficulties for firms because they cannot readily distinguish between protectable and non-protectable information.

In response, the UTSA should be revised to include a specific test to determine whether information is part of an employee’s general knowledge and experience or an employer’s protectable trade secret. Such a test will balance competing social policies using the specific considerations articulated in the proposed Restatement of Unfair Competition. This approach will inject more certainty into the law and promote fair competition in those cases where the parties have not clarified their respective rights by contract.
Perilous Knowledge
The Human Genome Project and Its Implications
TOM WILKIE
Physicist and writer Wilkie offers a lively, compelling history of this scientifically fascinating and politically contentious undertaking. Beginning with the discovery of DNA by James Watson and Francis Crick in 1953, Wilkie's narrative unfolds with the intrigue of a detective story. He reviews in nontechnical terms the many step-by-step developments from different scientific teams that finally made it seem possible to sequence the human genome. He goes on to consider the potential social consequences, good and bad, of learning to manipulate the human genetic code.
$20.00 cloth

Justice and the Human Genome Project
Edited by TIMOTHY F. MURPHY and MARC A. LAPPÉ
The Human Genome Project is an expensive, ambitious, and controversial attempt to locate and map every one of the approximately 100,000 genes in the human body. Beginning with an account of the utopian dreams and authoritarian tendencies of historical eugenics movements, the essays in this book probe the potential social uses and abuses of detailed genetic information. “In my view, [Murphy] has written the most incisive general critical essay on the Human Genome Project yet to appear.”
—Troy Duster, Director, Institute for the Study of Social Change, University of California, Berkeley
$28.00 cloth

At bookstores or order toll-free 1-800-822-6657.