Marquette Intellectual Property Law Review

Volume 2 | Issue 1 Article 3

1998

Trade Secrets and the New Realities of the Internet Age

Ari B. Good
DePaul University College of Law

TRADE SECRETS AND THE NEW REALITIES OF THE INTERNET AGE

ARI B. GOOD*

INTRODUCTION

The dawn of the Internet as a communications and business tool presents new questions in the evolution of intellectual property law. The "Internet" is a shorthand term for the vast international network of computers linked by modems, that connects individuals from many nations via phone lines, and enables them to share an incredible array of information and ideas quickly and relatively inexpensively. Originally conceived as a communications system for military purposes,[1] the Internet became a pathway along which information flows in a place commonly referred to as cyberspace.

The explosive growth in the exchange of information brings new challenges to the relevance and application of trade secret law. The dependence to create, store, record, and transmit information on computers gave rise to new forms of civil and criminal wrongdoing, and presents significant questions as to how proprietary information can best be protected in an information age. The risks of industrial espionage in this environment have increased exponentially as businesses rely more heavily upon computers for the exchange of information.[2] Trade secret law must continually evolve as new questions arise in a "networked" world.

This Article will address trade secret law as it applies in this computer age. Part I will examine the background of trade secret law.

---

* J.D. 1997, DePaul University College of Law. I wish to thank Professor Roberta R. Kwall for her guidance in the creation and publication of this Article.

1. *See* Reno v. American Civil Liberties Union, ___ U.S. ___, 117 S. Ct. 2329, 2334 (1997) (reviewing the history and evolution of the Internet).

2. The phrase "industrial espionage" generally refers to the theft of proprietary business information. The end of the Cold War and increasing global economic competition stemming from the trend towards world free trade has prompted many nations to direct their intelligence efforts against United States corporations in an effort to compete for resources and influence. *See* Daniel W. McDonald et al., *Intellectual Property and the Internet*, 13 No. 12 COMPUTER LAW. 8 (1996).

Three principal legal texts have codified and simplified the definition of a trade secret and the circumstances under which trade secrets are misappropriated: the Restatement of Torts, the Uniform Trade Secrets Act, and most recently, the Restatement (Third) of Unfair Competition. Part I considers the continuing applicability of all three of these legal texts in the protection of proprietary information in an Internet age.

The definition contained in the Restatement of Torts is still widely used in identifying trade secrets and in defining the elements of the tort of misappropriation.[3] Nevertheless, varying approaches to misappropriation cases prompted the National Conference of Commissioners on Uniform State Laws to create the Uniform Trade Secrets Act (UTSA), which codified well reasoned trade secret case law into statutory form.[4] UTSA provides uniform definitions of the principal elements of trade secret law and was drafted with a view towards making the law more predictable in a world where state and national borders have declining significance. This uniformity has been at least partially achieved, as UTSA has been widely adopted into the legislation of the majority of American jurisdictions.[5]

---

3. *See, e.g.,* Wilson v. Electro Marine Sys., Inc., 915 F.2d 1110, 16 U.S.P.Q.2d (BNA) 1605 (7th Cir. 1990) (applying New York law in diversity case, which relies upon the Restatement of Torts); Ruckelshaus v. Monsanto Co., 467 U.S. 986 (1984) (utilizing the Restatement of Torts in defining a "trade secret").

4. *See* UNIFORM TRADE SECRETS ACT Prefatory Note (amended 1985), 14 U.L.A. 433 (1990) [hereinafter UTSA].

5. UTSA Table of Jurisdictions (amended 1985), 14 U.L.A. 433 (1990). Forty one states have, at the time this article was written, adopted state legislation based upon the UTSA or other general trade secret statutes. *See* ALA. CODE § 8-27-1 et seq. (1993); ALASKA STAT. § 45.50.910 et seq. (Michie 1996); ARIZ. REV. STAT. ANN. § 44-401 et seq. (West 1994); ARK. CODE ANN. § 4-75-601 et seq. (Michie 1996); CAL. CIV. CODE § 3426 et seq. (West 1997 & Supp. 1998); COLO. REV. STAT. ANN. § 7-74-101 et seq. (West 1990 & Supp 1997); CONN. GEN. STAT. ANN. § 35-50 et seq. (West 1997); DEL. CODE ANN. tit. 6, § 2001 et seq. (1993); D.C. CODE ANN. § 48-501 et seq. (1997); FLA. STAT. ANN. § 688.001 et seq. (West 1990); GA. CODE ANN. § 10-1-760 et seq. (1994); HAW. REV. STAT. ANN. § 482B-1 et seq. (Michie 1985 & Supp. 1992); IDAHO CODE § 48-801 et seq. (1997); 765 ILL. COMP. STAT. ANN. 1065/1 et seq. (West 1993); IND. CODE ANN. § 24-2-3-1 et seq. (Michie 1996); IOWA CODE ANN. § 550.1 et seq. (West 1997); KAN. STAT. ANN. § 60-3320 et seq. (1994); KY. REV. STAT. ANN. § 365.880 et seq. (Banks-Baldwin 1993); LA. REV. STAT. ANN. § 51:1431 et seq. (West 1987); ME. REV. STAT. ANN. tit. 10, §1542 (West 1964); MO. CODE ANN., COM. LAW § 11-1201 et seq. (1990); MASS. GEN. LAWS ANN. ch. 93, § 42 et seq. (West 1997); MINN. STAT. ANN. § 325C.01 et seq. (West 1995); MISS. CODE ANN. § 75-26-1 et seq. (1991); MONT. CODE ANN. § 30-14-401 et seq. (1997); NEB. REV. STAT. § 87-501 et seq. (1994); NEV. REV. STAT. ANN. § 600A.010 et seq. (1994); N.H. REV. STAT. ANN. § 350-B:1 et seq. (1995); N.M. STAT. ANN. § 57-3A-1 et seq. (Michie 1978); N.C. GEN. STAT. § 66-152 et seq. (1996); N.D. CENT. CODE § 47-25.1-01 et seq. (1978); OHIO REV. CODE ANN. § 1331.51 (Anderson 1993); OKLA. STAT. ANN. tit. 78 § 85 et seq. (West 1995); OR. REV.

The Restatement (Third) of Unfair Competition represents the most recent simplification of trade secret law. This Restatement was expressly intended to be used in conjunction with UTSA for guidance in evaluating the widely different factual scenarios that give rise to claims for the misappropriation of trade secrets.[6] While trade secrets have historically been analyzed in connection with other commercial torts,[7] the Restatement of Unfair Competition text treats the law of trade secrets as a distinct body that plays an essential role in encouraging innovation and maintaining minimum standards of commercial morality.[8] While each of the three principal trade secret texts differ somewhat in its approach to trade secret law, all consider the value and secrecy of proprietary information in identifying a protectible trade secret.

Part II of this Article examines the legal challenges presented by the widespread use of the Internet as it relates to the protection of valuable trade secrets. The very benefit that society reaps from this new technology, the near instantaneous exchange and transmission of information, also constitutes an added problem as computerized information becomes more difficult to protect. The first principal challenge posed by the Internet to trade secret law lies in determining what constitutes reasonable efforts by the holder of the trade secret to keep information secret in an Internet age.[9] A trade secret holder must demonstrate that

---

STAT. § 646.461 et seq. (1995); R.I. GEN. LAWS § 6-41-1 et seq. (1992); S.C. CODE ANN. § 39-8-1 et seq. (Law Co-op. 1976) (39-8-1 to 9 repealed by 1997 Act No. 38, § 1 eff. May 21, 1997); S.D. CODIFIED LAWS § 37-29-1 et seq. (Michie 1994); UTAH CODE § 13-24-1 et seq. (1997); VA. CODE ANN. § 59.1-336 et seq. (Michie 1950); WASH. REV. CODE ANN. § 19.108.010 et seq. (West 1989); W. VA. CODE ANN. § 47-22-1 et seq. (1996); WIS. STATS. §134.90 (1995-96); *see also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1915) Articles - Statutory note: Alabama and Massachusetts have trade secrets statutes that are not based upon UTSA. Michigan, Missouri, New Jersey, New York, Pennsylvania, Tennessee, Texas and Wyoming protect trade secrets under the common law.

6. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. b (1995) (noting that the new RESTATEMENT (THIRD) OF UNFAIR Competition is "applicable to actions under the Uniform Trade Secrets Act as well as to actions under common law.").

7. *See, e.g.,* GEORGE J. ALEXANDER, COMMERCIAL TORTS 205-229 (1973) (discussing trade secret law as a species of "commercial tort").

8. *See* Kewanee Oil v. Bicron Corp., 416 U.S. 470, 481-82, 181 U.S.P.Q. (BNA) 673, 678 (1974). *Kewanee Oil* set forth the policy considerations that underlie trade secret law, including the preservation of commercial morality through punishing "wrongful" conduct, rewarding the inventor by protecting his or her invention, and guarding the privacy rights of businesses. *See also* Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 155, 9 U.S.P.Q.2d (BNA) 1847, 1854 (1989) (citing with approval the *Kewanee Oil* description of the policies underlying trade secret laws rationale in passing upon the preemption of Florida statute by Federal patent laws).

9. *See* UTSA § 1(4) (ii) (amended 1985), 14 U.L.A. 438 (1990) (definition of a trade secret requires the owner of the secret information to have taken "efforts which are reasonable under the circumstances to maintain secrecy").

the holder has taken reasonable efforts to protect the information in order to establish the existence of a protectible trade secret in the first place.[10] The steps that a trade secret holder is required to make to maintain this secrecy will change as the Internet becomes part of everyday education, communication, and commerce.

The second challenge that the Internet age presents is the danger of misappropriated information becoming generally known through its introduction into cyberspace.[11] Because a trade secret loses all legal protection once it is generally known, the speed with which such information can become a part of the public domain will require ever greater efforts at maintaining secrecy. The law must continue to adapt while addressing the close questions of when wrongfully acquired or disclosed information has become a part of the public domain through new technological realities.

In Part III, specific proposals are set forth for adjusting trade secret law to deal effectively with the legal issues surrounding trade secrets on the Internet. One recent case, *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*,[12] is examined as precedent for future litigation that will consider the new boundaries of the public domain as it applies to trade secrets. Physical, procedural, and technological innovations in the protection and management of secret information are considered as means through which such information can peacefully exist in an Internet age.

I. TRADE SECRET DEFINED

A. Blending Legal Concepts - Trade Secrets' "Dual Personality" As Both Property and Tort

The first step in analyzing trade secret law is to identify whether the owner of proprietary information has established the existence of a protectible trade secret. Whether a particular intellectual property is entitled to the law's protections is a highly fact-specific inquiry.[13] Three principal legal texts define trade secrets: The Restatement of Torts,[14]

---

10. *Id.*

11. *See id.* § 1(4) (i) (definition of a trade secret as information which is "not . . . generally known").

12. 923 F. Supp. 1231 (N.D. Cal. 1995).

13. *See, e.g.*, Amoco Prod. Co. v. Laird, 622 N.E.2d 912, 916, 30 U.S.P.Q.2d (BNA) 1515, 1609 (Ind. 1993) ("'Trade secret' is one if the most elusive and difficult concepts to define").

14. RESTATEMENT OF TORTS § 757 (1939).

USTA,[15] and the Restatement (Third) of Unfair Competition.[16] While these texts provide a somewhat different definition of what constitutes a trade secret, each bears two important textual and functional similarities to the others.

First, all three recognize both a property and a tort dimension to a protectible trade secret.[17] While a trade secret is commonly referred to as its owner's intellectual property, the determination of whether a protectible trade secret exists is often made by considering the defendant's tortious conduct with respect to the stolen secret.[18] This approach to trade secret law can loosely be termed the "tort first" perspective. In other words, a court will infer the existence of a protectible property interest in the hands of the secret holder by virtue of the defendant's wrongful methods to acquire it.

Conversely, other courts focus first upon the nature of information at issue. Only *after* the plaintiff satisfies the burden of proving the existence of a protectible secret, that is, a property interest protectible under trade secret law, is the nature of the defendant's conduct considered. This approach can be termed a "property first" mode of analysis. As discussed below, these two approaches, while historically merely a difference in emphasis,[19] may have greater significance in the age of the Internet where protecting one's property has become more difficult as the incidence of tortious conduct, including industrial espionage, continues to climb.

Second, these three principal legal texts should not be considered in isolation because courts often rely upon more than one of these trade secret definitions in analyzing misappropriation claims.[20] The Restatement of Torts, the first comprehensive summary of trade secret law, is still consulted by courts for guidance in defining a trade secret in juris-

---

15. UTSA (amended 1985), 14 U.L.A. 433 (1990).

16. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995).

17. See, for example, *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 178-80, 17 U.S.P.Q.2d (BNA) 1780, 1784 (7th Cir. 1991) for an excellent discussion of the different elements of trade secret law. Judge Posner discusses approaching trade secret law as a property concept versus as a tort concept. This is really a difference in emphasis as both legal principles are utilized in analyzing trade secret misappropriation claims.

18. *See, e.g.*, Ferranti Elec. Inc. v. W.J. Harwood, N.Y.S.2d 612 (N.Y. Sup. Ct. 1964) (discussing the defendant's improper means of acquiring the plaintiff's trade secrets in misappropriation suit but finding no violation).

19. *See infra* notes 120-133 and accompanying text.

20. *See, e.g.*, Valco Cincinnati, Inc. v. N&D Mach. Serv., Inc., 492 N.E.2d 814 (Ohio 1986) (utilizing both UTSA and Restatement of Torts remedial provisions in analyzing a claim for the misappropriation of trade secrets).

dictions that have adopted legislation patterned after UTSA.[21] The Restatement (Third) of Unfair Competition was intended to be used in conjunction with state versions of UTSA[22] and is often cited as a reference that provides guidance in applying the relevant state statute.[23] The precise differences between these legal texts and how each has contributed to the evolving body of trade secret law is discussed more fully below.

1. Early Trade Secret Case Law Interpretations

The early cases examining claims for the misappropriation of trade secrets illustrated both the property first and the tort first approaches to defining a protectible interest in valuable proprietary information. *Elaterite Paint & Manufacturing Co. v. S.E. Frost Co.*[24] illustrates the former approach. In *Frost*, the court considered a cause of action brought by a paint manufacturer against a direct competitor for the misappropriation of trade secrets.[25] The plaintiff's paint was manufactured using the mineral elaterite, a process he claimed was specific to his business and not generally known throughout the rest of the paint manufacturing industry.[26] Just over a year after the parties initial agreement was signed, the defendant left the plaintiff's business to begin manufacturing paint in direct competition with his former employer.

The court noted that "equity recognizes a secret in trade as property" in denying the plaintiff's claim to an injunction against further use

21. RESTATEMENT OF TORTS § 757 cmt. b (1939). The Restatement of Torts sets forth six factors that aid the determination as to the existence of a protectible secret, principles that are often incorporated into the analysis of courts sitting in both UTSA and non-UTSA jurisdictions alike. *See, e.g.*, Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 898, 220 U.S.P.Q. (BNA) 811, 816-17 (Minn. 1983) (using pre-UTSA case law which had relied upon the Restatement of Torts in interpreting the statutory language of UTSA). *But see*, Precision Screen Machs., Inc. v. Elexon, Inc., 1996 U.S. Dist. LEXIS 12487, at *12 (N.D. Ill. Aug. 26, 1996) (not reported in Federal Supplement) (common law claim for trade secret misappropriation preempted by the Illinois Trade Secrets Act, 765 ILL. COMP. STAT. 1065/8 (West 1993)).

22. *See supra* note 5 and accompanying text.

23. *See, e.g.*, Religious Tech. Ctr. v. Netcom On-line Communication Servs., Inc., 923 F. Supp. 1231, 1250 n.21 (N.D. Cal. 1995) ("Although California has adopted UTSA, courts also look to the Restatement [of Unfair Competition] to help interpret UTSA."). This case is discussed extensively in the context of how the explosive development of the Internet is changing the applicability of trade secrets law. *See infra* notes 232-256.

24. 117 N.W. 388 (Minn. 1908).

25. *Frost*, 117 N.W. at 389 (competition obtained trade secret formulae and processes by enticing plaintiff's former employees to work for them).

26. *Id.* at 389.

by the defendant of his trade secrets.[27] An injunction is appropriate, the court reasoned, where a trade secret is used in violation of a confidential relationship, or in a breach of contract claim.[28] The relationship between the employer and employee constituted a confidential relationship,[29] and the employment contract between the parties expressly identified the manufacturing processes as the plaintiff's property.[30] In upholding the lower court's finding for the plaintiff, the *Frost* court found that the defendant had no knowledge of the plaintiff's processes before working for him, and by comparing the substantial similarities between the parties' products, concluded that the defendant had used the plaintiffs' trade secrets.[31] The *Frost* decision, therefore, illustrates the property first approach as the court first ascertained whether the plaintiff's process was a trade secret before considering the defendant's wrongful conduct.

Conversely, the early case of *E.I. DuPont de Nemours v. Masland*[32] identified a cause of action for the misappropriation of trade secrets based primarily upon the breach of a confidential relationship.[33] The plaintiff sought to enjoin a former employee from using or disclosing supposedly secret processes relating to the manufacture of artificial leather which the defendant learned as part of the employment relationship.[34] The defendant responded that although he was in direct competition with the plaintiff, his techniques were based only upon methods and processes that were generally known. Hence, the defendant did not use any of his former employer's trade "secrets."[35] The lower court's injunction prohibited the defendant from disclosing any of the specific processes during his defense at trial.[36]

---

27. *Id.*

28. *Id.* at 390.

29. *Frost*, 117 N.W. at 389-90.

30. *Id.* at 390.

31. *Id.* The court found a violation of the trade secret holder's intellectual property rights on the basis of the defendant's access to the protected process and the substantial similarity between the plaintiff's and the defendant's final product. This method of analysis, access plus substantial similarity equals infringement, is used in copyright infringement suits which consider whether the defendant had "reproduced" a protected work. *Cf.* Computer Assocs. Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 701 (2d Cir. 1992) (holding access plus substantial similarity constitutes copyright infringement).

32. 244 U.S. 100 (1912).

33. *Id.* at 102.

34. *Id.* at 101.

35. *Id.*

36. *Id.* at 101-02.

In upholding the lower court's injunction, Justice Holmes stated, "the word property as applied to . . . trade secrets is an unanalyzed expression of certain secondary consequences of the primary fact that the law makes some rudimentary requirements of good faith."[37] In other words, a trade secret is property in the hands of its owner is secondary to the truly actionable element of misappropriation, the defendant's breach of confidence. The opinion placed its principal emphasis on the importance of acting in good faith in one's commercial relationship, irrespective of what was appropriated.[38]

These two cases are representative of the two principal legal approaches to the question of what constitutes a trade secret. In *Frost*, using the property first approach, the court evaluated the wrongful *act* on the basis of physical *evidence* created through use of the protected intellectual property. In *Masland*, the court, using the tort first approach, placed good faith ahead of the proof of a concrete, protected property right. Drawing the inference that the *Frost* court drew on the basis of tangible evidence, however, may present a far greater challenge in an information age.

Trade secret law often relates to and protects proprietary information which may never take a physical form. Unlike a film, a book, or a can of paint, a protected process may never be embodied in a thing that permits physical comparison.[39] A secret customer list or a formula for a chemical compound, once misappropriated, may be hidden or altered before it could ever be offered into evidence. This situation is especially relevant where, for example, a precious industrial secret is never

37. *Masland*, 244 U.S. at 102.

38. *Id.* Judge Holmes perhaps de-emphasized the importance of the property right too much by declaring that "[t]he property may be denied but the confidence cannot be . . . ." More recent cases, however, typically begin with the question of whether there is truly a protectible secret; a plaintiff cannot assert legal rights in generally known processes or inventions. *See, e.g.*, Buffets v. Klinke, 73 F.3d 965, 967-68, 37 U.S.P.Q.2d (BNA) 1449, 1451 (9th Cir. 1996) (inferring that the question of whether information has been misappropriated depends upon the existence of a protectible trade secret in the first place).

39. Decisions that have found liability for the misappropriation of trade secrets have often inferred the misappropriation based upon the physical evidence at issue, which permits a comparison of the similarity of a plaintiff's and a defendant's products. *See, e.g.*, Forro Precision, Inc. v. International Bus. Mach. Corp., 673 F.2d 1045, 1057, 215 U.S.P.Q. (BNA) 299, 306 (9th Cir. 1982) (upholding jury verdict which found liability for trade secret misappropriation on the basis of a "direct comparison" between the plaintiff's and defendant's engineering drawings). *But see* People v. Gopal, 217 Cal. Rptr. 487, 494 (Cal. App. 1985) (possession of a stolen object embodying trade secrets not equivalent to the theft of the trade secrets themselves).

put into actual production before it is misappropriated, but was nevertheless the product of substantial research and investment.[40]

Proceeding from a tort first perspective may be equally problematic in the computer age. Justice Holmes's statement that "the property may be denied, but the confidence cannot be"[41] risks holding a person liable for the misappropriation of that which was never protected in the first place. As illustrated below, UTSA guards against such an unjust result in requiring the plaintiff to first demonstrate that the information at issue was the subject of reasonable measures to protect its secrecy and that it was not generally known.[42]

In summary, an analysis of a trade secret claim from either a strictly tort based or property based perspective would reveal only half the picture. The legal elements which define a trade secret operate together to identify a particular class of information which is protected from unscrupulous business practices.

2. Attempts at Uniformity—The Restatement of Torts

The Restatement of Torts represents an early attempt to set forth concrete criteria through which the existence of a protectable trade secret could be determined. Section 757 of the Restatement provides "[a] trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors[43] who do not know or use it."[44] Article (b) sets forth six factors used in identifying whether information is a truly a trade secret. Generally, these factors consider the degree to which the information is generally known or readily available outside of the claimant's particular business, the inherent value of

40. Also note that, under the definitions in the Restatement (Third) of Unfair Competition and in UTSA, the secret's economic value need only be actual or potential. *See infra* notes 75-76. The industry plaintiff in the hypothetical above would therefore not only need to retrieve some evidence of the defendant's wrongful misappropriation, but would also need to show that such information would have conferred an economic benefit had it been actually used in the plaintiff's business. The ease with which digital information can be manipulated presents potential problems of proof in trade secrets cases.

41. *Masland*, 244 U.S. at 102.

42. The court will often infer from the plaintiff's efforts that the information was worth protecting, for example, that it has value and was not generally known. *See* Amoco Prod. Co. v. Laird, 622 N.E.2d 912, 30 U.S.P.Q.2d (BNA) 1515 (Ind. 1993).

43. *See, e.g.*, W.R. Grace & Co. v. Hargadine, 392 F.2d 9 (6th Cir. 1968) (a trade secret may arise by virtue of the time, research and investment required to acquire or create the proprietary information).

44. RESTATEMENT OF TORTS § 757 cmt. b (1939).

the information, and what measures the claimant has taken to guard the information's secrecy.[45]

The Restatement also sets forth the ground for finding a misappropriation of trade secrets. A person who uses or discloses the trade secret of another without privilege to do so is liable if:

(a) he discovered the secret by improper means,[46] or

(b) his disclosure or use constitutes a breach of confidence reposed in him by the other in disclosing the secret to him,[47] or

(c) he learned the secret from a third person with notice of the facts that it was a secret and that the third person discovered it by improper means or that the third person's disclosure of it was otherwise a breach of his duty to the other,[48] or

---

45. Restatement of Torts section 757 comment b provides that a court should examine:

(1) the extent to which the information is known outside the particular business,

(2) the extent to which it is known by employees and others involved in the particular business,

(3) the extent of measures taken by the particular business to guard the secrecy of the information,

(4) the value of the information to the particular business and to its competitors,

(5) the amount of effort or money expended by the particular business in developing the information, and

(6) the ease or difficulty with which the information could be properly acquired or duplicated by others, in determining the existence of a trade secret.

Id.

46. RESTATEMENT OF TORTS § 757 (1939). The Restatement's definitions are unclear as to what forms of "discovery" are permissible or whether a trade secret that is disclosed to another but never used in competition with the plaintiff is a form of "misappropriation." *See* Gale R. Peterson, *Trade Secrets in an Information Age*, 32 HOUS. L. REV. 385 (1995). This uncertainty has since been dispelled by case law that notes that trade secret law does not extend to information acquired through "reverse engineering" or through independent discovery. *See infra* notes 87-89.

47. Some courts interpreted "use" broadly, finding liability even where the defendant had not yet entered into direct competition with the plaintiff. *See, e.g.*, University Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518, 541-542, 183 U.S.P.Q. (BNA) 705 (5th Cir. 1974) (finding "use" by the defendant where it received stolen computer tapes from its agent, showed the materials on these tapes to another company in an effort to develop a similar computer system, and installed the computer programs for its own internal use on its computers); *see also* Sikes v. McGraw-Edison Co., 665 F.2d 731, 213 U.S.P.Q. (BNA) 983 (5th Cir. 1982), *cert. denied*, 458 U.S. 1108 (1982) (finding "use" where the defendant employed the plaintiff's trade secret in the process of improving his own); Surgidev Corp. v. Eye Tech.. Inc., 828 F.2d 452, 456, 4 U.S.P.Q.2d (BNA) 1090 (8th Cir. 1987) (actual use of a trade secret is not required to show misappropriation where there was evidence of prior use, plus evidence that the defendant had an intent to further use the confidential information in the future).

48. RESTATEMENT OF TORTS § 757 (1939). The question of notice is also discussed in connection with recovering trade secrets that have been posted on the Internet.

(d) he learned the secret with notice of the facts that it was a secret and that its disclosure was made to him by mistake.[49]

A great number of trade secret cases decided under the Restatement deal with the question of misappropriation in the context of the employer/employee relationship. Because employment relationships often involved the exchange of information for the purpose of the everyday operation of the business, cases limit their discussion with respect to the nature of the information at issue in the case.[50] For example, the court in *Ferranti Electric Inc. v. Harwood*[51] noted that "courts have consistently placed emphasis not so much upon the thing allegedly taken as upon the manner in which it was taken and the breach of faith involved."[52] In placing emphasis on the nature of the relationship between the parties, these decisions infer that valuable information passed from employer to employee and that is necessary to compete in a competitive marketplace is sufficiently confidential to qualify as a secret. The precise contours of the wrongful conduct of a renegade employee often depended upon the nature of the industry at issue,[53] or the precise nature of the secret's value to its holder.[54]

The court in *Wilkin v. Sunbeam Corp.*,[55] for example, considered the question of whether a confidential relationship existed between the parties which prohibited the unauthorized use or disclosure of a trade secret.[56] The court found that the plaintiff lost no trade secrets where she

---

49. *Id.*

50. *See* W.R. Grace & Co. v. Hagardine, 392 F.2d 9, 14 (6th Cir. 1968) ("Breach of confidence is the essence of the basic definition of trade secret liability in RESTATEMENT OF TORTS, § 757 (1939)."); Metal Lubricants Co. v. Engineered Lubricants Co., 411 F.2d 426, 162 U.S.P.Q. (BNA) 584 (8th Cir. 1969) ("The Restatement of Torts, Sec. 757, comment a, relates that a trade secret is protected against 'employment of improper means to procure the trade secret....'").

51. 251 N.Y.S.2d 612, 619 (N.Y. App. Div. 1964).

52. *Id.* at 619.

53. *See, e.g.*, Atlantic Wool Combing Co. v. Norfolk Mills, 357 F.2d 866, 868-869, 148 U.S.P.Q. (BNA) 571, 573 (1st Cir. 1966) (The defendant misappropriated the design of a wool "combing" machine. The court noted that the plaintiff had designed the machine for his particular use, had informed the manufacturer not to disclose its specifications to any others, and that the misappropriation took place "in a small industry within which... traditionally undertakes to keep the details of its processes secret."). *But see* Venn v. Goedert, 319 F.2d 812, 815, 138 U.S.P.Q. (BNA) 415, 416-17 (8th Cir. 1963) (no misappropriation of plaintiff's cookie recipes where recipes were easily discoverable through experimentation by any skilled baker).

54. *See* Metal Lubricants v. Engineered Lubricants, 411 F.2d 426, 428, 162 U.S.P.Q. (BNA) 584, 586 (8th Cir. 1969) (holding no misappropriation of customer lists by the defendant where the consumers for metal lubricants were of general knowledge).

55. 377 F.2d 344, 153 U.S.P.Q. (BNA) 386 (10th Cir. 1967).

56. *Id.* at 346, 153 U.S.P.Q. (BNA) at 388.

submitted an idea for a sandwich maker to the defendant, a manufacturer of household appliances, absent an agreement that the concept for the sandwich maker was proprietary in nature.[57] The court specified the elements for the misappropriation of a trade secret as: (1) the existence of a novel idea,[58] (2) which is disclosed to the defendant in confidence, and (3) which is adopted and used by the defendant.[59] Because the plaintiff's idea was not disclosed in confidence, the defendants committed no misappropriation when they refused plaintiff's proposals and then began manufacturing a similar device.[60]

Notwithstanding that the misappropriation of a trade secret is widely regarded as a commercial tort, the property first approach to examining claims for misappropriation arose in the case of *E.I. DuPont de Nemours v. Christopher.*[61] The *Christopher* court considered the question of what constitutes wrongful conduct with reference to the secret nature of the information itself. In *Christopher*, the defendants flew an airplane over the plaintiff's manufacturing facility, under construction at the time, for the purpose of taking aerial photographs of the facility.[62] The plaintiff claimed to have developed a highly secret but unpatented process for producing methanol, a process which gave them a competitive advantage over other producers.[63] While the fly-over was not by itself wrongful conduct, the court considered the nature of the secret information and the defendant's apparent goal of acquiring it in holding the defendant liable for misappropriation.[64] The court noted that a skilled person would have been able to deduce the secret process from the aerial photos taken by the defendant's agent, potentially eliminating the plaintiff's competitive advantage.[65] The plaintiff sought damages for

57. *Id.* at 347, 153 U.S.P.Q. (BNA) at 388.

58. *Id.* at 346, 153 U.S.P.Q. (BNA) at 388. It should be noted that the plaintiff's complaint also pleaded patent infringement, which the court denied since no patent had issued on the plaintiff's idea at the time she submitted it to Sunbeam. The court emphasized in the opinion that no property right existed without the patent, and therefore the only cause of action the plaintiff had was for the defendant's tortious conduct. The law has also changed with respect to novelty cases decided under UTSA, expressly holding that novelty in the patent sense is not required for a plaintiff to have a protectible trade secret. *See* W.R. Grace & Co. v. Hargadine, 392 F.2d 9, 14 (6th Cir. 1968) ("Further, novelty in the sense it is used in patent law is clearly not a requirement of a trade secret.").

59. *Wilkin*, 377 F.2d at 346, 153 U.S.P.Q. (BNA) at 386.

60. *Id.* at 346-47, 153 U.S.P.Q. (BNA) at 387-88.

61. 431 F.2d 1012, 166 U.S.P.Q. (BNA) 421 (5th Cir. 1970).

62. *Id.* at 1013, 166 U.S.P.Q. (BNA) at 422.

63. *Id.*

64. *Id.* at 1014-17, 166 U.S.P.Q. (BNA) at 422-25.

65. *Id.*

the loss it had already sustained from the circulation of the photos and an injunction against any further circulation.[66]

The court referred to the Restatement of Torts in defining the improper means of acquiring a trade secret.[67] Protection of a trade secret was not limited to a breach of a confidential relationship, but also applied to wrongful *acquisitions* of protected information.[68] In holding that aerial photography constituted such improper means, the court distinguished proper channels for discovering technical or business information.[69] The inspection and analysis of a competitor's secret process through the process of reverse engineering, for example, does not destroy the value of the plaintiff's discovery.[70] The time, effort, and money required to conduct such an inspection ensured that the defendant would not gain an unfair advantage in deciphering the valuable information.[71] Similarly, trade secret law does not prohibit one from utilizing information which is discovered independently of the plaintiff.[72]

In sum, the *Wilkin* and *Christopher* decisions illustrate the determination of whether wrongful conduct has occurred is a function of *both* the secret nature of the information and the means the defendant uses in acquiring it. In granting relief against certain means of acquiring a valuable secret and not against others, a court acts to preserve minimum standards of commercial morality. The *Christopher* court reasoned that tolerating industrial espionage would dampen the spirit of inventiveness by stripping those who hold secrets of their ability to seek redress for unfair competitive methods.[73] While the holder of a trade secret must employ reasonable methods to guard against foreseeable disclosure of the information, an impenetrable fortress is not required

66. *Christopher*, 431 F.2d at 1014, 166 U.S.P.Q. (BNA) at 422.

67. *Id.* at 1014, 166 U.S.P.Q. (BNA) at 423.

68. *Id.* at 1015, 166 U.S.P.Q. (BNA) at 423.

69. *Id.*

70. *Id; see also* People v. Gopal, 217 Cal. Rptr. 487, 492 (D.Cal. 1985) (stating that reverse engineering is an accepted and lawful practice in industry in considering a claim of trade secret misappropriation in the computer industry).

71. *Christopher*, 431 F.2d at 1015-16, 166 U.S.P.Q. (BNA) at 423-24.

72. *Id.* at 1015, 166 U.S.P.Q. (BNA) at 423. This is a central difference between patent law and trade secret law. While a patent grants the plaintiff rights against any unauthorized duplication during the monopoly period, the rights of a trade secrets holder are effective only as against wrongful conduct. This underscores the importance of considering the tortious nature of the defendant's conduct in defining the limits of the plaintiff's property rights in trade secret law.

73. *Id.* at 1016, 166 U.S.P.Q. (BNA) at 424.

to qualify for the law's protections.[74] The scope of *how* secret information must be kept is discerned by analyzing USTA.

3. The Uniform Trade Secrets Act

The second principal addition to authoritative texts digesting the fundamental principles of trade secret law was UTSA. UTSA was drafted to codify the better reasoned trade secret decisions decided under the Restatement of Torts, and to better define what forms of information constitute protectible trade secrets.[75] One commentator has suggested that UTSA continues to emphasize the deterrence of reprehensible commercial conduct, while simultaneously laying a more detailed foundation for determining the nature of the property interest sought to be protected.[76] UTSA defines a trade secret as:

> [I]nformation, including a formula, pattern, compilation, program, device, method, technique or process that:
>
> (i) derives economic value, actual or potential, from not being generally known to, or readily ascertainable by, the public or to 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.[77]

UTSA explicitly states the principal legal requirements that "value" and "secrecy" must be demonstrated by a plaintiff in order to establish the existence of a protected trade secret.

In contrast to the Restatement of Torts, USTA replaces the Restatement requirement that a trade secret be continually used in one's business in order to be protected. USTA accomplishes this by modifying somewhat the concept of value, requiring that a trade secret confer upon its holder either actual or potential value.[78] UTSA's definition of trade secret echoes the Restatement of Torts' requirement, however, that the value of the information must derive from its not being gener-

---

74. *Id.*

75. UTSA Prefatory Note (amended 1985), 14 U.L.A. 433 (1990).

76. *See* Peterson, *supra* note 46, at 396 ("UTSA is premised on deterring breaches of good faith and the use of reprehensible means of learning another's secret."). UTSA better defines the property interest sought to be protected. That the information had been the subject of reasonable measures to protect its secrecy and had not been generally known (thus not a secret at all) prior to the alleged misappropriation is required.

77. *See* UTSA § 1(4) (amended 1985), 14 U.L.A. 433 (1990).

78. *Id.* at cmt. b; *see also* Sikes v. McGraw-Edison Co., 665 F.2d 731, 213 U.S.P.Q. (BNA) 983 (5th Cir. 1982) (stating that a temporary advantage may suffice as sufficiently concrete to constitute a protectible trade secret), *cert. denied*, 458 U.S. 1108 (1982).

ally known. Part (ii) of the definition also expressly requires that the information be subject to reasonable efforts to maintain secrecy. As with section 757 of the Restatement of Torts, the precise meanings of each of these terms of art are factual questions which vary from case to case. Cases decided under UTSA are also compatible with the Restatement (Third) of Unfair Competition which, as discussed below, further refine UTSA's definitions.[79]

UTSA also makes clear that the wrongful acquisition of a trade secret, the theft of protected information, is independently actionable from the disclosure or use of a trade secret.[80] The definition of misappropriation is designed to cover cases dealing with industrial espionage, as well as traditional breaches of confidential relationships in which wrongful acquisition are not at issue, such as nondisclosure agreements between employers and employees. Misappropriation is defined as:

> (i) *acquisition* of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means, or
>
> (ii) *disclosure or use* of a trade secret of another without express or implied consent by a person who
>
> (A) used improper means to acquire knowledge of the trade secret; or
>
> (B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was:
>
> (I) derived from or through a person who had utilized improper means to acquire it;
>
> (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
>
> (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
>
> (C) before a material change of his [or her] position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.[81]

One principal benefit of the widespread adoption of UTSA has been, not surprisingly, a greater uniformity between states as to what

---

79. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40, cmt. a (1995).

80. *See* UTSA § 1(2) (i)-(ii) (amended 1985), 14 U.L.A. 433 (1990); *see also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. a (1985).

81. UTSA § 1(2), (ii) (A)-(C) (amended 1985), 14 U.L.A. 433 (1990) (emphasis added) (brackets in original).

constitutes the misappropriation of a trade secret. Such uniformity is desperately needed as information is more easily transmitted across state boundaries through the use of modern communications technology. UTSA permits people and companies whose businesses are national or international in scope to better predict the legal regime under which the information will be protected, and to most efficiently take steps to fit within the definitions contained in UTSA's provisions for the legal protection of trade secrets.

4. The Restatement (Third) Of Unfair Competition

The Restatement (Third) of Unfair Competition represents the most recent advance in the clarification and codification of trade secret law.[82] Section 39 provides a simplified definition of a trade secret: "A trade secret is 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."[83] Section 39 does not enumerate categories of information which are potentially protectible as a trade secret. This revision avoids possible confusion that such categories represent an exclusive list.[84] Like UTSA, section 39 provides that a trade secret need only confer "an actual or potential" competitive economic advantage upon its holder in order to be protectible.[85] Section 39 protects forms of trade secrets such as negative information including procedures, processes, or ideas which do not work, and inchoate plans or formulae.[86]

Section 40 of the Restatement defines misappropriation:

> One is subject to liability for the appropriation of another's trade secret if:

---

82. *See* R. Mark Halligan, Esq., *Restatement of the Law [Third], Unfair Competition - A Brief Summary*, (visited May 17, 1997) <http://www.execpc.com/~mhallign/unfair.html>.

83. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995).

84. The Restatement (Third) of Unfair Competition section 39 clarified UTSA's definition, which provides that "trade secret means information, *including* a formula, pattern, compilation, program, device, method, technique or process . . . ." (emphasis added). *See supra* note 77 and accompanying text. UTSA definition only requires that the trade secret be some form of information, not limiting what form it is in.

85. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995).

86. *See* Mettalurgical Indus., Inc. v. Fourtek, Inc., 790 F.2d 1195, 1202-03, 229 U.S.P.Q. (BNA) 945, 950 (5th Cir. 1986) (questioning whether there is any true difference in the value of positive information (for example, information which defines what works and negative information)).

(a) the actor *acquires* by means that are improper under the rule stated in [section] 43[87] information that the actor knows or has reason to know[88] is the other's trade secret; or

(b) the actor *uses or discloses* the other's trade secret without the other's consent and, at the time of the use or disclosure,

(1) the actor knows or has reason to know that the information is a trade secret that the actor acquired under circumstances creating a duty of confidence owed by the actor to the other under the rule stated in [section] 43;[89] or

(2) the actor knows or has reason to know that the information is a trade secret that the actor acquired by means that are improper under the rule stated in [section] 43; or

(3) the actor knows or has reason to know that the information is a trade secret that the actor acquired from or through a person who acquired it by means that are improper ... or whose disclosure ... constituted a breach of a duty of confidence owed to the other under the rule stated in [section] 41; or

(4) the actor knows or has reason to know[90] that the information is a trade secret that the actor acquired through an accident or mistake, *unless* the acquisition was

---

87. Section 43 provides: "'Improper means' of acquiring another's trade secret under the rule stated in [section] 40 include theft, fraud, unauthorized interception of communications, inducement of or knowing participation in a breach of confidence, and other means either wrongful in themselves or wrongful under the circumstances of the case. Independent discovery and analysis of publicly available products or information are not improper means of acquisition." RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 (1995). The actor's conduct under this definition need not necessarily be independently tortious, but is of course included in the non-exhaustive list of wrongful methods of acquiring a trade secret. The second sentence of this definition limits the trade secret holder's rights as applying only to those who use wrongful means — rather than reverse engineering or inspection — to acquire the secret information.

88. The "reason to know" language expressly eliminated the pure heart, empty head defense to trade secret misappropriation. *See* Peterson, *supra* note 46.

89. *Compare* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 with UTSA § (1) (2) (ii) (A-C) (amended 1985), 14 U.L.A. 433 (1990) (defining liability for the use or disclosure of a trade secret where the recipient knows that the secret was wrongfully acquired).

90. That an actor can be liable for misappropriation if he or she has "reason to know" is a clarification over the definitions contained in both the Restatement of Torts and UTSA. Comment d of § 40 provides that "if a reasonable person in the position of the actor would have inferred that he or she was in wrongful possession of another's trade secret, the actor is subject to liability for any subsequent use or disclosure." RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. d (1995). This may have a significant impact on misappropriation suits brought in the Internet context, in which a wrongfully "posted" trade secret can potentially be retrieved by giving notice to potential recipients of the information. *See* IMED Corp. v. System Eng'g Assocs. Corp., 602 So.2d 343 (Ala. 1992).

> the result of the other's failure to take reasonable precautions to maintain the secrecy of the information.[91]

Section 40 was intended by its drafters to be applied to common law actions in tort or restitution for the appropriation of another's trade secret.[92] Section 40 is analogous to UTSA in that the wrongful acquisition of a trade secret is independently actionable from the wrongful use or disclosure of the secret. The Restatement contains innovations over prior law. For instance, section 41 creates a separate duty of confidence which applies to the myriad of transactions which disclose trade secrets.[93] Section 43 provides an updated definition of improper means, which includes the unauthorized interception of communications such as e-mail transmissions.[94] Because of these innovations, the Restatement provides USTA jurisdictions with additional guidance in defining trade secrets and analyzing claims for misappropriation. All three of these legal texts incorporate many of the same legal concepts and are consistent in identifying the two cornerstones to trade secret protection: the requirements of value and secrecy.

B. The Cornerstones Of Trade Secret Protection—Case Law Analysis of the "Value" Requirement For The Existence Of A Protectible Trade Secret

As noted above, the first fundamental characteristic of information considered to constitute a trade secret requires that the information have value derived from it being a secret, and which confers upon its holder a competitive economic advantage. The decision rendered by the Indiana Supreme Court in *Amoco Production Co. v. Laird* ("*Laird*")[95] represents an excellent example of a UTSA jurisdiction's approach to defining value as a function of the secrecy of the information. In other words, the competitive benefit that the trade secret owner enjoys must derive from it not being generally known or readily ascertainable through proper means by competitors. Generally known information, while it may be valuable to the industry as a whole, confers no *particular* advantage on the trade secret holder and thus cannot truly be considered a secret at all. The value and secrecy requirements, therefore, should not be viewed in isolation, but rather as interrelated

---

91. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 (1995) (emphasis added).

92. *See supra* notes 90-91; RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. a (1995).

93. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 41 (1995).

94. *Id.* § 43.

95. 622 N.E.2d 912, 30 U.S.P.Q.2d (BNA) 1515 (Ind. 1993).

concepts which separate trade secrets from other forms of valuable intellectual property.

The *Laird* opinion focused specifically upon the legal standard that governs a court's determination of whether information is "not readily ascertainable by . . . proper means."[96] Plaintiff Amoco Production Co. ("Amoco") filed suit against defendant Laird for the misappropriation of information relating to proposed oil sites in portions of the Midwest.[97] Amoco used information contained in its confidential corporate library, literature from the United States Geologic Survey, and aerial searches using specialized microwave radar to compile a surface map of potential oil deposits, investing $150,000 to conduct the microwave radar study.[98] An Amoco employee passed facsimiles of the proposed exploration sites to defendant Laird, an oil exploration financier. Amoco sought damages and injunctive relief when the employee's disclosure to Laird was discovered, claiming trade secret protection for the location of the potential oil deposits.[99]

The court began its analysis by first considering a trade secret as defined by the Indiana Uniform Trade Secrets Act.[100] The court noted that the initial inquiry, whether the information embodied in Amoco's maps constituted a trade secret, was dependent upon this information fitting within the statute's definitions.[101] Specifically, the trade secret's value must have been derived from its exclusivity to Amoco. It was necessary for Amoco to show that the information was not readily ascertainable to the defendant without a similar expenditure of the same amount of time, effort, and money.[102] The court rejected the defendant's contention that the information contained in Amoco's maps did not constitute a trade secret because Amoco had failed to show: (1) that

96. *Id.* at 915, 30 U.S.P.Q.2d (BNA) at 1517.

97. *Id.* at 913, 30 U.S.P.Q.2d (BNA) at 1515.

98. *Id.* at 914, 30 U.S.P.Q.2d (BNA) at 1516.

99. *Id.*

100. IND. CODE ANN. § 24-2-3-2 (Michie 1996). The Indiana Act adopted verbatim the definition of a "trade secret" found in UTSA, which provides, as noted above, that a trade secret is "information . . . that [is] . . . not . . . readily ascertainable by proper means." UTSA § 1 (4) (I) (amended 1985), 14 U.L.A. 433 (1990 and Supp. 1997). *See Laird*, 622 N.E.2d at 915, 30 U.S.P.Q.2d (BNA) at 1517.

101. *Laird*, 622 N.E.2d at 915, 30 U.S.P.Q.2d (BNA) at 1517.

102. *Id.* Readily ascertainable refers both to the value of the information as well as its secrecy. UTSA is premised upon the assumption that information which is not readily ascertainable is secret (provided the plaintiff has made a reasonable attempt to keep the information secret and that the secret information is valuable). Whether this logical chain holds up depends upon the particular facts in issue.

it was not economically infeasible[103] [sic] for Laird to have identified the location of the oil fields other than through the use of the plaintiff's maps, and (2) that the oil reserves information could not have been created by means other than Amoco's business operations.[104] The court rejected the premise that trade secret status must be denied to all information except for that which was discoverable only through Herculean efforts by the defendant.

The court noted that neither the case law decided under UTSA nor the Act itself considered the defendant's economic ability to discover the information as relevant to the readily ascertainable inquiry.[105] Instead, whether information was readily ascertainable depends upon whether the information sought to be protected as secret was "available in trade journals, reference books, or other published materials."[106] The court's analysis focused on the availability of the information generally, rather than the relative ease with which any *particular* defendant could acquire the information.[107]

In setting forth the standard for when information is readily ascertainable, the court surveyed the thirty-nine jurisdictions that had adopted UTSA,[108] noting that UTSA represented a codification of better reasoned trade secret cases that had preceded it.[109] Additionally, the court based its decision in part on the definitions contained in section 757 of the Restatement of Torts, which provided "helpful guidance [in determining] whether the information in a given case constitutes 'trade secrets' within the definition of the statute."[110] The sixth factor in comment b to section 757, "the ease or difficulty with which the information could be properly acquired or duplicated by others,"[111] was particularly relevant to the facts at issue. In summary, Amoco's information constituted a trade secret within the meaning of the statute in part because the map was not readily ascertainable through proper means.[112]

---

103. *Laird*, 622 N.E.2d at 915-16, 30 U.S.P.Q.2d (BNA) at 1516-18 (the court rejected the defendant's approach as inconsistent with the letter and spirit of UTSA).

104. *Id.* at 915, 30 U.S.P.Q.2d (BNA) at 1516.

105. *Id.* at 917, 30 U.S.P.Q.2d (BNA) at 1518-19.

106. *Id.* at 916, 30 U.S.P.Q.2d (BNA) at 1518 (quoting IND. CODE ANN. § 24-2-3-2 (1982)).

107. *Id.* at 920-21, 30 U.S.P.Q.2d (BNA) at 1520-21.

108. *Laird*, 622 N.E.2d at 917 n.3, 30 U.S.P.Q.2d (BNA) at 1519 n.3.

109. *Id.* at 917, 30 U.S.P.Q.2d (BNA) at 1518-19.

110. *Id.* at 918, 30 U.S.P.Q.2d (BNA) at 1519 (quoting Optic Graphics, Inc. v. Agee, 591 A.2d 578, 585 (Md. App. 1991)).

111. *See supra* note 45 and accompanying text.

112. *Laird*, 622 N.E.2d at 919-21, 30 U.S.P.Q.2d (BNA) at 1520-21.

The court made several additional observations regarding the types of information that could qualify as a trade secret in granting relief to Amoco. First, the court noted that simply because the information *could* be independently discovered without resort to wrongful conduct was no defense to a claim of misappropriation.[113] Second, trade secret law recognizes that not every part of the body of information claimed as a trade secret needs to be secret in and of itself.[114] Specifically, trade secret law recognizes that a compilation of facts that, by themselves, would be a part of the public domain, could qualify as a trade secret provided the information conferred a competitive economic benefit upon its holder.[115] Amoco's maps represent a compilation of facts which are, if viewed individually, both publicly available or readily ascertainable by proper means.[116] As a unitary whole, however, the map gave Amoco a competitive edge in locating previously undiscovered oil reserves.

Finally, the court flagged the policy considerations which supported its interpretation of whether information is "readily ascertainable" by members of the public within the meaning of the state trade secret statutes. Protecting Amoco's proprietary information helped maintain the standards of commercial ethics and commercial innovation.[117] Recalling a trade secret's property dimension, the court noted that "[i]n protecting individual property rights in trade secrets, the purpose of trade secrets law has also been . . . the promotion of the development of new products and technology."[118] Thus, the *Laird* decision effectively addressed a number of questions regarding statutory interpretation rele-

113. *Id.* at 918-19, 30 U.S.P.Q.2d (BNA) at 1519 (citing Television Communication Sys., Inc. v. Saindon, 522 N.E.2d 1359, 1365 (Ill. App. Ct. 1988)).

114. *Id.* at 919-20, 1520; *see also* Peterson, *supra* note 46, at 433 (citing Machen, Inc. v. Aircraft Design, Inc., 828 P.2d 73 (Wash. App. 1992). Peterson cites the *Machen* case for the proposition that even if the arrangement or design of the constituent parts of a machine cannot qualify as trade secrets, the whole product may be protectible. Nevertheless, the "protected" product is still subject to the requirement that it be maintained in secrecy. The *Machen* court denied protection to the product, a braking system for airplanes, where the plaintiff had disclosed the product at a trade show.

115. *Laird*, 622 N.E.2d at 920, 30 U.S.P.Q.2d (BNA) at 1521. ("[W]e find that, taken together, the integration of pertinent site information and resultant projections as to potential oil reserves constitutes a unique compilation of information not previously known in the marketplace.").

116. *Id.* at 920, 30 U.S.P.Q.2d (BNA) at 1520-21.

117. *Id.* at 921, 30 U.S.P.Q.2d (BNA) at 1521 (citing Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 481, 181 U.S.P.Q. (BNA) 673, 678 (1974)).

118. *Id.*, 30 U.S.P.Q.2d (BNA) at 1521 (citing IMED Corp. v. Systems Eng'g & Assocs. Corp., 602 So.2d 344, 346 (Ala. 1992)).

vant to trade secret causes of action decided under UTSA or the equivalent state law.

C. *Efforts Which Are "Reasonable Under The Circumstances" To Maintain Secrecy*

The second cornerstone in defining a protectible trade secret is the element of secrecy.[119] UTSA codified the relative secrecy standard, which originally developed under the case law dealing with the Restatement of Torts' definition of a trade secret.[120] Under the relative secrecy standard, information that is known or used by others in a particular industry does not alone indicate lack of trade secret status if it remains secret from those to whom it has potential economic value.[121] Indeed, businesses would be seriously burdened if information could never be shared within an industry pursuant to employer-employee relationships, licensing, product demonstrations, and the like.

The requirement that a plaintiff alleging misappropriation of a trade secret need only demonstrate that the information was kept relatively secret serves as a means for identifying a particular class of information, or trade secrets, which has been sufficiently protected by its owners to merit the law's protection. In this respect, secrecy has remedial significance, such as when information is properly kept and then stolen, the information becomes the subject of a cause of action for misappropriation. That the information is in fact kept secret, however, also suggests that there was a reason for doing so: the information was valuable. The fact that the owner of a trade secret has taken reasonable efforts to protect the information is evidence of the competitive value of the information. The Seventh Circuit, in *Rockwell Graphic Systems, Inc. v. DEV Industries, Inc.*,[122] considered this secrecy/value nexus in considering what constitutes reasonable efforts to preserve one's trade secrets.

In *Rockwell Graphics*, the plaintiff ("Rockwell"), a manufacturer of printing presses sued DEV, a rival company founded by former Rockwell employees, for the misappropriation of trade secrets. Rockwell's practice was to subcontract the manufacture of different parts of its presses to other companies, which required Rockwell to provide bidders with "piece part" drawings that specified the dimensions of the part re-

119. UTSA § 1(4)(ii) (amended 1985), 14 U.L.A. 433 (1990) (defining trade secret as "information . . . [which] is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.").

120. *See* Peterson, *supra* note 46, at 428-29.

121. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. f (1995).

122. 925 F.2d 174, 17 U.S.P.Q.2d (BNA) 1780, 1782-83 (7th Cir. 1991).

quired.[123] These drawings were then used to create the valuable parts that were ultimately assembled and sold to Rockwell customers. The drawings contained Rockwell's trade secrets that were disclosed in confidence during the course of subcontracting the manufacture of the specified parts.[124] DEV defended against Rockwell's assertions that it had misappropriated Rockwell's trade secrets by claiming that Rockwell had failed to take "reasonable efforts" to protect the sensitive information contained in the drawings and was therefore precluded from asserting that the drawings constituted trade secrets.[125]

Rockwell undertook several measures to keep the drawings secret during the process of submitting them to sub-contractors.[126] The drawings were stored in a vault which could be accessed only by authorized Rockwell employees. These employees were required to enter into nondisclosure agreements and to sign the drawings in and out of the vault as the drawings were needed.[127] The only outsiders who were permitted to see the drawings were the sub-contractors, who were also required to sign confidentiality agreements. Additionally, the copies of the drawings that the sub-contractors were provided bore a "confidential" designation. While the sub-contractors were permitted to keep the provided copies for the purposes of future bidding for Rockwell jobs, Rockwell had apparently never suffered an abuse of this confidence prior to bringing suit against DEV.[128]

In reversing the district court's determination that Rockwell had failed to take reasonable measures to protect the information contained in the piece part drawings, the court noted that a limited disclosure of confidential information did not necessarily eradicate the information's trade secret status.[129] While Rockwell could have done more to protect the secrecy of its drawings, the court found that Rockwell had taken reasonable measures to protect its proprietary information.[130] In making this determination, a trade secret's dual personality in tort and property law was revisited by the court — concepts that illustrate both

123. *Id.* at 175, 17 U.S.P.Q.2d (BNA) at 1781.
124. *Id.* at 175-76, 17 U.S.P.Q.2d (BNA) at 1781-82.
125. *Id.* at 176, 17 U.S.P.Q.2d (BNA) at 1781-82.
126. *Id.*
127. *Rockwell Graphics*, 925 F.2d at 177, 17 U.S.P.Q.2d (BNA) at 1782-83.
128. *Id.*
129. *Id.* at 177, 17 U.S.P.Q.2d (BNA) at 1782-83.
130. *Id.* at 180, 17 U.S.P.Q.2d (BNA) at 1785.

the evidentiary and remedial significance of the reasonable measures requirement.[131]

The court noted that taking reasonable efforts to protect information served a remedial purpose by opening the door to recovery for the defendant's *wrongful conduct.*[132] Security measures are reasonable where they are sufficient under the circumstances to minimize the probability that DEV could have produced Rockwell's press parts *without* using its trade secrets.[133] Second, Rockwell's reasonable efforts also constituted evidence of the value of the information itself, the property which trade secret law was designed to protect.[134] In the end, the court determined that the two approaches to determining a defendant's liability for the misappropriation of a trade secret represented only a difference in emphasis,[135] and that Rockwell had taken reasonable precautions against the unauthorized use or disclosure of its trade secrets under either approach. The significance of the *Rockwell* decision lies in the fusion of the interrelated trade secret concepts of wrongful disclosure, the value of a secret to its holder, and reasonable measures to preserve confidentiality, all of which must be considered in making the fact-specific determination of when a trade secret has been misappropriated.

An important case that considered the question of secrecy in the computer context was *Integral Systems, Inc. v. Peoplesoft, Inc.*[136] Like the *Rockwell* decision, *Peoplesoft* considered what evidence a plaintiff must adduce in order to show that reasonable measures were undertaken to protect trade secrets disclosed in the context of a confidential relationship, which in this case was the employment relationship.[137] Plaintiff Integral was a software development firm that specialized in creating human resource management software for larger companies. An employee left Integral to form the defendant corporation, and thereafter developed a similar, though not identical, human resources system. Integral filed suit based on the findings of an independent con-

131. *Id.* at 178, 17 U.S.P.Q.2d (BNA) at 1783-84.

132. *Rockwell Graphics*, 925 F.2d at 178, 17 U.S.P.Q.2d (BNA) at 1783-84.

133. *Id.* at 178-79, 17 U.S.P.Q.2d (BNA) at 1783-85.

134. *Id.* at 179, 17 U.S.P.Q.2d (BNA) at 1784-85.

135. *Id.* at 178, 17 U.S.P.Q.2d (BNA) at 1783-84.

136. No. C-90-2598-DLT, 1991 WL 498874 at *3 (N.D. Cal. July 19, 1991) (not reported in Federal Supplement).

137. *Peoplesoft*, 1991 WL 498874, at *3; *see also* UTSA, § 1(2) (amended 1985), 14 U.L.A. 433 (1990) ("Misappropriation" means acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means).

sultant which identified three areas of similarity between the plaintiff's and defendant's software.[138]

The *Peoplesoft* court first considered the nature of the information at issue, noting at the outset that the Integral's computer software could constitute a protected trade secret.[139] The trade secret could consist of the individual units of the computer program, its overall "architecture," structure, or combination thereof, so long as the program otherwise met the value and secrecy requirements.[140] Here, the court evaluated whether the information allegedly taken by the employee was secret in light of the "limited pool of knowledge" that was available to developers of similar products.[141]

The court examined the utility of the parts of the computer program at issue in passing upon whether the information was generally known, a finding which would have precluded Integral from asserting that the program was a trade secret.[142] If some feature of the human resource software alleged by Integral to be secret was essential to the operation of any like program, then that information was generally known among other developers of the same types of programs.[143] The court recog-

138. *Peoplesoft*, 1991 WL 498874, at *3. The consultant compared (1) the payroll module, a grouping of commands within a computer program, of the two companies' programs, (2) the terminal displays (screen displays) of the programs, (3) the security features which the respective systems employed, and (4) the overall functionality of each of the systems. The report concluded that the two products were similar, and that Peoplesoft's lack of intermediate documentation (for example, evidence of independent development) demonstrated that Peoplesoft's program was based upon Integral's trade secrets.

139. *Id.* at *13.

140. *Id.*; Integrated Cash Mgmt. Serv. v. Digital Trans., 920 F.2d 171, 173-74, 17 U.S.P.Q.2d (BNA) 1054, 1056 (2nd Cir. 1990).

141. *Peoplesoft*, 1991 WL 498874 at *14.

142. *Id.*

143. The court's consideration of the function of the information in the operation of the system is somewhat analogous to the doctrine of functionality in the context of trademark law and the concept of originality in copyright law. All generally describe the same phenomenon, that legal protection is not extended to ideas but only to the expression of ideas under the different legal regimes. Trade secret law differs in that ideas *are* protectible (even if not novel in the patent sense), but only if they are not generally known. Here, the existence of similar programs on the market using similar technology demonstrate that the claimed trade secret is known throughout the industry. *Cf.* Qualitex Co. v. Jacobson Prods. Co., Inc., 514 U.S. 159, 34 U.S.P.Q.2d (BNA) 1161 (1995) (the color of a dry-cleaning pad may be serve as a trademark provided it has acquired secondary meaning); Feist Pubs., Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 18 U.S.P.Q.2d (BNA) 1275 (1991) (denying copyright protection to a compilation of telephone numbers lacking the requisite originality under the 1976 Copyright Act); *see also* Murray v. National Broad. Co., Inc., 844 F.2d 988, 6 U.S.P.Q.2d (BNA) 1618 (2nd Cir. 1988) (denying trade secret status to a concept for a television show which was not sufficiently "novel" to demonstrate that the idea was not already part of the public domain). *But see,* Atlantic Wool Combing Co. v. Norfolk Mills, Inc., 357

nized that members of the software industry frequently changed jobs or started companies of their own, and that common use of the functional elements of a computer program served the socially beneficial purpose of speeding innovation and increasing the total amount of knowledge in the industry.[144] The court ultimately concluded that Integral's program contained elements which entitled it to trade secret protection.[145]

Next, the court addressed the question of whether Integral had taken reasonable efforts to protect its proprietary information. The court did not require "extreme and unduly expensive procedures" to protect information as a trade secret.[146] Integral employed measures designed to preserve the confidentiality of its systems including requiring employees to sign confidentiality agreements that prohibited the unauthorized use or disclosure of its trade secrets, restricting access to the main building, and employing a password system for employee access to the company's mainframe computer. Taken together, the court concluded that Integral had taken reasonable efforts to protect its trade secrets.[147]

Integral's claim for confidentiality ended when the court found that, notwithstanding its intent to have kept its information secret, Integral abandoned its reasonable efforts in disclosing its program's source code in connection with a product demonstration at a university.[148] The court ultimately concluded that while a waiver of confidentiality as to a single client did not eliminate trade secret status per se, it weakened Integral's case as to the secret nature of its information.[149] The court ultimately denied Integral's petition for a preliminary injunction against defendant Peoplesoft on grounds that Integral was unlikely to have been able to demonstrate the existence of protectible trade secrets at trial.[150]

Viewed together, the *Rockwell* and *Peoplesoft* decisions set forth a legal framework for a court's consideration of what constitutes reasonable measures to keep information secret. Taking precautions to guard the information one claims as a trade secret has both remedial and evidentiary significance. Similarly, the reasonable measures inquiry incor-

---

F.2d 866, 148 U.S.P.Q. (BNA) 571 (1st Cir. 1966) (novelty in the patent sense not required to demonstrate the existence of a trade secret; plaintiff must merely demonstrate that idea sought to be protected was not common knowledge).

144. *Peoplesoft*, 1991 WL 498874 at *14.
145. *Id.* at *16.
146. *Id.* at *14-15.
147. *Id.* at *15.
148. *Id.* at *14-15.
149. *Peoplesoft*, 1991 WL 498874 at *14-15.
150. *Id.* at *16.

porates questions of the information's value and secrecy, interrelated concepts used to ascertain the existence of a protectible trade secret. Whether the court bases its analysis upon the wrongful measures undertaken by the defendant as evidence of the reasonableness of the plaintiff's precautions, or upon the nature of the information itself and its relative value in the industry, the result, according to the rationale in *Rockwell*, will generally come out the same.

The age of the Internet, however, may alter the analysis of whether a trade secret holder has truly taken "reasonable efforts" to protect the information. As discussed below, the ease with which computerized information can be published to millions of Internet users presents new questions as to how to best address the wrongful conduct against which reasonable efforts must be directed in the computer environment. The ease with which secrecy may be destroyed on the Internet must factor into the chain of inferences that a court draws from the plaintiff's reasonable efforts.

Because a court is always required to work backwards in considering whether reasonable measures have been taken, courts must be careful not to assume that misappropriated information has less *value* merely because the *means* for misappropriating it have become so much more powerful. The power and scope of the Internet to disseminate information quickly and without centralized control or regulation must factor into an equitable consideration of what is considered reasonable against these odds. Similarly, courts must be careful to consider the contours of wrongful conduct specific to the computer environment, an area that incorporates virtual or intangible transactions potentially having a profound impact on the maintenance and use of trade secrets. How the Internet will affect the consideration of the reasonable efforts inquiry is discussed in Part II, below.

II. CHALLENGES TO TRADE SECRET LAW IN THE AGE OF THE INTERNET

A. What Is The Internet?

The Internet, a loose term which describes the vast *inter*national *net*work of computers linking millions of people worldwide, represents one of the most significant technological advances in human communication since Gutenberg's printing press. The Internet consists of a "web" of millions of computers organized into local networks, which in

turn are linked to larger networks, and so on.[151] Computer users access this web of information through the use of Internet access providers, which are powerful computers designed to connect individual users to the larger network. Initially developed by the United States Department of Defense, the network was at its inception used primarily by scientists and academicians as a means of sharing research among large groups of people.[152] In recent years, the Internet has grown exponentially as people both young and old exchange electronic mail, text, sound, graphical images, and nearly every other conceivable form of information with the use of a computer,[153] a modem, and a telephone line.

B. The Implications Of The Internet For Trade Secret Law

1. A Theoretical Framework: Do Old Laws Apply To New Technologies?

Before considering the precise application of trade secret law to contemporary realities in the computer world, it is useful to consider whether the information age calls for new laws at all.[154] How one approaches the question of how trade secret law should apply to the Internet depends upon how narrowly or broadly one defines whether an issue of law is truly new.[155] At the greatest level of generality, existing intellectual property laws are well equipped to deal with new technological realities, particularly the protection of information that is somehow valuable to the owner or possessor. At the most specific end of the spectrum, most trade secret jurisprudence has become largely irrelevant because existing precedent considered questions of confidentiality and disclosure in communications media differently than that involving the Internet. Separating whether existing law is sufficient to deal with new legal issues requires consideration of whether the harm that trade secret laws are designed to prevent is reduced, magnified, or unaffected by new technological realities.

---

151. For a closer look at the specifics, history and a plain English guide to the operation of the Internet, see JOHN R. LEVINE ET AL., THE INTERNET FOR DUMMIES (3d ed. 1996).

152. Reno v. American Civil Liberties Union, ___ U.S. ___, 117 S. Ct. 2329, 2334 (1997).

153. *Id.*

154. *See* I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993 (1994).

155. *Id.*

One consideration in determining whether historical legal analogies apply to the Internet age is whether the outcome of a particular legal problem is affected by the information medium that is at issue. Contrast, for example, a suit brought for the invasion of privacy and a suit for defamation.[156] In the case of a defamation suit, the outcome of the litigation does not depend upon the medium in which the defamatory message is sent.[157] The harm that the law is designed to prevent, unjust damage to the plaintiff's reputation, is the same whether the message is sent by ordinary mail, fax, e-mail, or through publication on a computerized bulletin board system (BBS).[158] Arguably, the speed with which this harm could occur, or the size of the audience to whom the defamatory information is published, could vary with the medium used.[159] These factors would primarily be relevant only to the type of proof offered by the plaintiff in proving the elements of the case, or in fashioning a remedy upon a successful showing of defamation.[160]

In contrast, and as in the case of an invasion of privacy, the harm that the law is designed to prevent is directly affected by the means used to inflict it. How deeply one's privacy is invaded varies greatly between an invasive phone call or an offensive letter as opposed to a mass publication of embarrassing or confidential information via the Internet. In cases such as these, existing privacy laws may be insufficient to deal with the harm, having been written largely without the concept of instantaneous communication capabilities in mind.

A second principal in considering new legal questions is the growing role of intermediaries in cyberspace,[161] which are Internet providers or BBS[162] operators whose systems serve as conduits for wrongful conduct.

---

156. *See id.* at 999-1003.

157. *Id.* at 999-1000.

158. *Id.*

159. *See* Hardy, *supra* note 154, at 999-1000.

160. *Id.* at 999-1003.

161. *See id.* at 1000-06. An intermediary is defined as some individual or entity which could potentially have control over what passes through the Internet. Intermediaries would include a large commercial Internet provider, such as America OnLine or Compuserve, an employer who reads his or her employees e-mails, the operator of a bulletin board system, defined below, etc. Some authors have suggested that any meaningful regulation of cyberspace will ultimately require intermediaries to bear the brunt of liability for wrongful conduct committed over their systems. *See also* Ian C. Ballon, *Pinning the Blame in Cyberspace: Towards a Coherent Theory For Imposing Vicarious Copyright, Trademark and Tort Liability for Conduct Occurring Over the Internet*, 18 HASTINGS COMM. & ENT. L. J. 729, 766 (1996).

162. Bulletin Board Systems (BBS) are computerized services that permit subscribers to "post" electronic messages. BBS are typically used for newsgroups, discussion groups conversing on every imaginable subject. BBS messages, once posted, are automatically cop-

The law is only beginning to consider whether BBS administrators, Internet access providers, and employers can or should be responsible for policing the communications that take place over their systems. This question becomes even more difficult when the abilities of intermediaries to read potentially defamatory e-mail messages or to examine posted computer files for the presence of protected trade secrets are considered.[163] Moreover, the international scope of the Internet makes playing the role of gatekeeper particularly difficult, and presents new questions concerning where the harm occurs and who should be responsible for it.

2. Adapting Trade Secret Law To New Technologies

In some respects, cyberspace represents a medium that defies the traditional methods of preventing and punishing misappropriation. In others ways, existing trade secret precedent can continue to provide an effective legal framework for the protection of valuable information and encouragement of innovation notwithstanding the emergence of new legal questions that the Internet age presents to trade secret laws. Authors[164] and practicing attorneys[165] have begun to grapple with new possibilities for protecting trade secrets from discovery.

While a computer is a physical object and can be protected through many of the same means as other forms of trade secrets embodied in tangible objects, the data it contains is far more difficult to control. The ease with which digital information can be transmitted to and among millions of different recipients, and the speed with which this can be done, has raised the stakes of wrongful acquisition of a trade secret.[166]

---

ied and distributed to all other members of that particular newsgroup. Members may then read them or post their own messages in response.

163. *See* Hardy, *supra* note 154, at 1003.

164. *See, e.g.*, Bruce T. Atkins, *Trading Secrets in the Information Age: Can Trade Secret Law Survive the Internet?*, 1996 U. ILL. L. REV. 1151.

165. *See, e.g.*, Victoria A. Cundiff, *Keeping the Information Highwaymen from Your IP, in* 16th ANNUAL INSTITUTE ON COMPUTER LAW, at 87 (PLI Patents, Copyrights, Trademarks, and Literary Prop. Course Handbook Series No. 444 (1996)).

166. It is essential to remember that what separates the Internet from other media historically considered in trade secrets cases is that computer data can be manipulated, stored, and transferred, consummating or creating a complex transaction without ever leaving a paper trail of what has occurred. Businesses and the legal world must adapt to this reality, in part by monitoring and restricting the use or transfer of trade secrets using computer technologies specifically designed to counteract this fluid environment. *See generally* Patrick F. McGowan, *The Internet and Intellectual Property Issues*, (455 PLI Patents, Copyrights, Trademarks, and Literary Prop. Course Handbook Series No. 303 (1996)) (noting that the absence of tangible evidence of Internet communications presents significant evidentiary and proof problems in litigating trade secrets cases).

Given the grave consequences of a breach of confidential relationship, trade secret holders should carefully consider the circumstances under which disclosures of their secrets are made.

Trade secret law must adjust to the new realities of the Internet age in two central respects. First, efforts that are reasonable under the circumstances to maintain the secrecy of proprietary information should be reconsidered in light of a business's growing reliance on computers. An effective security regime designed to protect sensitive information should include both physical and procedural measures. Additionally, confidential relationships, which have evolved as legal mechanisms for controlling the use and disclosure of trade secrets, can be extended to end users of consumer products through shrinkwrap licensing. The use of shrinkwrap licenses, although still in their legal infancy, may become a new tool in exerting reasonable efforts designed to maintain secrecy. Second, courts should reconsider the circumstances in which trade secret status is denied to sensitive information because the trade secret has become generally known. The recent case of *Religious Technology Center v. Netcom*[167] is an example of the challenges that courts must address in making the determination of when a trade secret has become part of the public domain.

a. *The Age Of The Internet Requires A Reevaluation Of "Efforts Which Are Reasonable Under The Circumstances To Maintain Secrecy"*

As discussed earlier,[168] all trade secret cases hold that in order to qualify for protection from the law, the owner of proprietary information must undertake "reasonable" measures to keep the information secret.[169] While trade secret cases have long considered this concept in connection with the theft of proprietary information,[170] the unique na-

167. 923 F. Supp. 1231 (N.D. Cal. 1995).

168. *See supra* notes 119-150 and accompanying text.

169. The significance of these efforts is twofold. Under the tort based view of trade secret law, the existence of measures which are reasonable under the circumstances include circumstantial evidence that the defendant had to resort to improper means to acquire the secret. Under the property based view of trade secret law, time, money, and effort spent by the owner in keeping the information a secret is circumstantial evidence of the secret's value.

170. *See, e.g.,* Data Gen. Corp. v. Digital Computer Controls, Inc., 357 A.2d 105, 108-10, 188 U.S.P.Q. (BNA) 276, 280-81 (Del. 1975) (reasonable efforts to protect a design for a minicomputer included drawings containing the plaintiff's trade secrets bore confidentiality legends, serving to put any recipient of the drawings on notice that they contained protected information, a copyrighted maintenance manual provided with the computer expressly prohibited use of the design information contained therein for any purpose except maintenance of the new machine).

ture of the Internet will require a close reevaluation of what constitutes "reasonable" measures. Given the ease with which a secret can be destroyed through instantaneous disclosure, trade secret owners must educate themselves in the most effective technologies for keeping digitized information secret. On the other hand, courts must be careful not to require businesses to undertake unduly burdensome security measures that would undermine cost-effective innovation and discovery.[171] A digitized world requires trade secret owners to undertake both physical and procedural security measures specifically designed to minimize the risk of trade secret misappropriation in light of new technologies.

The four legal guidelines that a trade secret holder should consider in developing a security regime are: (1) that security measures need not be so burdensome or expensive so as to prevent *improper* means of discovering the secret; (2) the trade secret holder's security measures must actually be implemented rather than merely intended; (3) the trade secret must be treated as a trade secret; and (4) these efforts must be specifically directed at the alleged trade secret.[172] Because trade secret law grants the secret holder certain legal rights only against certain forms of wrongful commercial conduct, undertaking reasonable measures to protect one's secrets has only evidentiary significance.[173] As described in the analysis of the *Rockwell* decision,[174] a trade secret holder need only produce sufficient evidence to demonstrate that the law's protection is justified, such as a showing that reasonable efforts were undertaken given the nature of the trade secret,[175] the nature of the industry,[176] and the nature of the company or individual claiming protection.[177]

---

171. Protecting industries' ability to protect their intellectual property in a reasonably cost effective manner is at the core of trade secret law. *See* Kewanee Oil v. Bicron Corp., 416 U.S. 470, 481 181 U.S.P.Q. (BNA) 673, 678 (1974) (illustrating the encouragement of invention as a fundamental policy of trade secret laws).

172. *See* David W. Slaby et al., *Trade Secret Protection: An Analysis of the Concept "Efforts Reasonable Under The Circumstances To Maintain Secrecy,"* 5 SANTA CLARA COMPUTER & HIGH TECH. L.J. 321, 326 (1989) (setting forth an analytical framework for the requirement under UTSA that the trade secret holder undertake reasonable security measures to protect trade secrets).

173. *But see* Rockwell Graphic Sys., Inc., v. DEV Indus., Inc., 925 F.2d 174, 178-79, 17 U.S.P.Q.2d (BNA) 1780, 1784. The *Rockwell* court, as discussed above, also considered the *remedial* significance of the reasonable efforts inquiry. However, even under the *Rockwell* court's rationale, a trade secret holder's reasonable efforts to protect the information is merely evidence that the defendant had engaged in wrongful conduct to acquire the secret, thereby entitling the owner to a remedy. Simply stated, that the owner of proprietary information undertakes reasonable efforts to protect it is but one part of the analysis in determining whether the information is in fact a protectible trade secret.

174. *Id.* at 177-78, 17 U.S.P.Q.2d (BNA) at 1783-84.

175. *Id.* Generally, the more valuable the secret is to the company and the more easily

Absolute secrecy, therefore, is not required to demonstrate the existence of a protectible trade secret.[178] The trade secret holder need not create an impenetrable fortress to guard the information, but must undertake precautions that would make it difficult for a would-be misappropriator to acquire the information other than by improper means.[179] Requiring a trade secret holder to guard against unanticipated, undetectable, or unpreventable methods of discovery would preclude smaller businesses from enjoying the law's protections for failing to implement often costly security systems.[180] Nevertheless, a trade secret holder must be eternally vigilant in protecting the trade secret from wrongful acquisition, disclosure, or use.[181] A reasonable security regime in the Internet age should therefore incorporate two dimensions, physical and procedural efforts, to maintain secrecy.

i. Physical Security Measures

A trade secret holder must constantly guard the physical objects which contain or embody the trade secret. In *Defiance Button Machine Co. v. C&C Metal Products Corp.*,[182] for example, the court considered

---

the trade secret can be identified and misappropriated, the stronger the showing a trade secrets plaintiff must make in order to demonstrate that a reasonable effort has been put forth in maintaining secrecy. *See* Slaby, *supra* note 172, at 331-32; *see also* Electro-Craft v Controlled Motion, Inc., 332 N.W.2d 890, 902-03, 220 U.S.P.Q. (BNA) 811, 820-21 (Minn. 1983) (a trade secret must be more closely guarded where its secret nature is intuitive, that is, where a reasonable observer familiar with the industry would conclude upon examination that a particular object or information that it is valuable and proprietary).

176. *See Electro-Craft*, 332 N.W.2d at 902, 220 U.S.P.Q. (BNA) at 820 (considering the question of reasonable measures within the servo motor industry, one in which, according to the court, industrial espionage was not a significant problem); Atlantic Wool Combing Co. v. Norfolk Mills, Inc., 357 F.2d 866, 869, 148 U.S.P.Q. (BNA) 571, 572 (1st Cir. 1966) (noting that the highly competitive and secretive nature of the wool combing industry).

177. A court is less likely to require small businesses to spend a substantial portion of their capital on security precautions, especially given that small firms tend to have fewer employees, reducing the risk of unauthorized disclosures by current or former employees. In any event, equitable considerations will guide the fact-specific determination of whether particular efforts are reasonable.

178. *See* K-2 Ski Co. v. Head Ski Co., Inc., 506 F.2d 471, 183 U.S.P.Q. (BNA) 724 (9th Cir. 1974) (applying the "relative secrecy" standard under represented in Maryland law and the law of the majority of other jurisdictions); *see also supra* notes 120-121 (for a discussion of relative secrecy).

179. *See* E.I. DuPont de Nemours & Co. v. Christopher, 431 F.2d 1012, 1017, 166 U.S.P.Q. (BNA) 421, 424-25 (5th Cir. 1970).

180. *See* Aries Info. Sys. v. Pacific Mgmt. Sys. Corp., 336 N.W.2d 366, 368 (N.D. 1983) (requiring only that the plaintiff had taken efforts to prevent against foreseeable misappropriation); E.I. DuPont de Nemours & Co. v. Christopher, 431 F.2d at 1016, 166 U.S.P.Q. (BNA) at 424.

181. *See* Slaby, *supra* note 172, at 325.

182. 759 F.2d 1053, 225 U.S.P.Q. (BNA) 797 (2d Cir. 1985).

what constituted reasonable efforts in the context of secret customer lists stored in a computer's memory and on floppy discs. The plaintiff, a manufacturer of metal buttons, left computer discs containing customer information within reach of the defendant's general manager during the course of an auction sale of the plaintiff company to the defendant. The customer lists were also left in the memory of a computer sold to the defendant. The defendant was able to retrieve the customer list using file names and passwords contained in source books that were readily accessible at the plaintiff's former plant. Significantly, the defendant was ultimately successful in retrieving the information only with the aid of one of the plaintiff's former employees, who was hired by the defendant to "demonstrate" the computer during the course of the sale. Nevertheless, the court ultimately held that defendant could not be liable for trade secret misappropriation where the plaintiff had failed to direct efforts towards keeping the customer information a secret, *notwithstanding the improper means* that the defendant used to retrieve the customer lists from the computer's memory.[183]

UTSA finds that reasonable physical security measures[184] may include employing guards to monitor access to proprietary machines, sites, or information,[185] keeping confidential information under lock and key,[186] segregating secrets in a different building or section of a facility,[187] and destroying, rather than merely discarding, hard copies of confidential data.[188] In short, reasonable physical security measures demonstrate that the owner of the secret has selected particular tangible objects or places which embody (as in the case of a secret machine) or contain (as in the case of a computer terminal or discs) the confidential information, and has excluded access to these places or things to all but those who need access to the trade secret in order for the business to function.

ii. Security Procedures Which Constitute Reasonable Efforts

---

183. *Defiance Button*, 759 F.2d at 1063-64, 225 U.S.P.Q. (BNA) at 804.

184. *See* UTSA § 1(4)(ii) (amended 1985), 14 U.L.A. 433 (1990).

185. *See, e.g.*, Valco Cincinnati, Inc. v. N&D Machining Serv., Inc., 492 N.E.2d 814, 819 (Ohio 1986) (finding reasonable efforts had been undertaken to protect sensitive manufacturing processes where, among other measures, people seeking access to materials embodying trade secrets were screened by a receptionist prior to being admitted).

186. *See, e.g.*, Capsonic Group v. Plas-Met Corp., 361 N.E.2d 41, 44 (Ill. App. Ct. 1977) (holding that the trade secret holder failed to demonstrate the existence of a protectible trade secret where it failed to "treat [its] information as confidential or restricted," including its failure to keep engineering drawings under lock and key).

187. This is particularly appropriate for trade secrets that are embodied in large machinery. Such a measure would be less relevant to trade secrets consisting of discrete, computerized information, the type most easily misappropriated via the Internet.

188. *See* Slaby, *supra* note 172, at 327-28.

Reasonable efforts undertaken to keep a trade secret confidential must also include implementing security policies and procedures that complement the physical care with which the secret must be treated.[189] The growth of the Internet and the growing role of the computer in everyday commerce calls for security procedures specific to computerized information and the rapid transmission of data. These procedures have traditionally taken two principal forms: (1) the creation of confidential relationships between the trade secret holder and a licensee or employee who makes use of the secret;[190] and (2) the marking and labeling of proprietary information.[191]

b. *The Continuing Importance Of Confidential Relationships In The Internet Age*

A trade secret holder's greatest exposure to the misappropriation of confidential information is often through the unauthorized disclosure of a trade secret by current or former employees.[192] At issue in these cases are breaches by employees of the duty of confidentiality that arise either by virtue of contractual agreements, or that are implied in law by virtue of the existence of the employment relationship. The principal significance of contractual non-disclosure agreements is twofold: (1) executing a confidentiality agreement creates a confidential relationship between the parties within the meaning of both the Restatement of Torts[193] and UTSA,[194] thereby providing for a cause of action if the rela-

189. *Id.* at 328.

190. The significance of these agreements is that they give rise to a duty of nondisclosure by the recipient of the information. *See* UTSA § 1(2) (amended 1985), 14 U.L.A. 433 (1990). Most often, confidential disclosures occur either as part of the employer-employee relationship, or during the course of subcontracting between companies. These disclosures are usually necessary in order for the secret holder to enjoy the competitive advantage of using the information in commerce. Whether a confidential relationship actually exists between the parties at the time of the disclosure is a question of fact. *See* RTE Corp. v. Coatings, 267 N.W.2d 226 (Wis. 1978) (holding that no confidential relationship exists where the parties are dealing at arm's length and the recipient has not been put on notice of the confidential nature of the disclosure of a trade secret).

191. This practice becomes especially important for businesses that subcontract or otherwise rely upon outside entities for effective use of the trade secret because it may be harder to establish a confidential relationship on the basis of sporadic transactions. *See, e.g.*, Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 177-78 , 17 U.S.P.Q. (BNA) 1780, 1782-84 (7th Cir. 1991). In any event, labeling proprietary information as confidential is a relatively inexpensive and effective means of putting the recipient of the information on notice of its nature, and demonstrates that the trade secret owner in fact treated the information as a secret.

192. *See* Phillip G. Alden et al., *Technical Employees Raises Intellectual Property Stakes*, (visited May 1, 1997) <http://www.hg.org/1333.txt>.

193. *See* Ferranti Elec. Inc. v. Harwood, 251 N.Y.S.2d 612 (1964).

tionship is breached via use or disclosure of the trade secret, and (2) executing such an agreement constitutes evidence of reasonable efforts undertaken by a trade secret holder to protect the other information.[195] The significant amount of litigation that centers around breaches of these agreements. However, this fact only demonstrates that confidentiality agreements alone may be inadequate to prevent the damage that can occur when a computerized trade secret is misappropriated via the Internet.

For example, in *Aries Information Systems, Inc. v. Pacific Management Systems Corp.*,[196] the court considered a claim for the misappropriation of trade secrets through the breach by employees of "confidential information agreements."[197] The plaintiff, a computer software developer, had spent a significant amount of time, money, and effort to create an accounting program. The defendants had each executed a confidentiality agreement with the plaintiff, providing that all of plaintiff's proprietary software was confidential and could not be disclosed to anyone. In upholding the lower court's finding of misappropriation, the court noted that the confidentiality agreements gave rise to the defendants' duty not to use or disclose the trade secrets embodied in the computer software.[198] Additionally, the agreements put the defendants on notice of the confidential nature of the information.[199]

While a contractual agreement can have evidentiary significance to both the existence of a duty not to use or disclose a trade secret and the existence of a confidential relationship between the parties, courts will sometimes find that a "confidential relationship" exists even in the absence of such an agreement. For example, in *Anaconda v. Metric Tool & Die Co.*,[200] the court expressly held that the disclosure of a trade se-

194. *See, e.g.*, MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 26 U.S.P.Q.2d (BNA) 1458 (9th Cir. 1993) (finding liability for the misappropriation of trade secrets where defendants violated contractual duties of confidentiality).

195. *See, e.g.*, Valco Cincinnati, Inc. v. N&D Machining Serv., Inc., 492 N.E.2d 814, 819 (Ohio 1986).

196. 366 N.W.2d 366, 226 U.S.P.Q. (BNA) 440 (Minn. Ct. App. 1985).

197. *Id.* at 367, 226 U.S.P.Q. (BNA) at 441.

198. *Id.* at 369, 226 U.S.P.Q. (BNA) at 443. The court in *Aries* also noted that the appellants bore a common law duty of nondisclosure based upon the respondents notice of confidentiality.

199. *See supra* notes 193-195 and accompanying text; UTSA, § 1(2)(ii)(A)-(C) (amended 1985), 14 U.L.A. 433 (1990).

200. 485 F. Supp. 410, 205 U.S.P.Q. (BNA) 723 (E.D. Pa. 1980); *see also* Campbell Soup Co. v. Giles, 47 F.3d 467, 33 U.S.P.Q.2d (BNA) 1916 (1st Cir. 1995) (confidential relationship existed between a corporate executive with knowledge of sensitive company information and his former employer where executive signed an express written agreement prohibiting use or disclosure of trade secrets); W.R. Grace & Co. v. Hargadine, 392 F.2d 9, 13

cret is wrongful if the nature of the relationship between a trade secret holder and an alleged misappropriator had given rise to an implied duty of nondisclosure.[201] The plaintiff, a manufacturer of metal tubing, sued for the defendant's misappropriation of its trade secrets through the hiring of plaintiff's former employees. These employees had intimate knowledge of the unique machinery and manufacturing processes which constituted the trade secrets.

While the plaintiff had never *specifically* instructed these employees as to the proprietary nature of its machinery, other measures that the plaintiff had taken to protect the machinery from inspection effectively put these employees on notice of its proprietary nature. Specifically, the plaintiff restricted outside visitors to the plant and had erected barriers and screens around the secret machinery to shield it from view.[202] *Notwithstanding* the absence of a specific written confidentiality agreement between the plaintiff and its former employees, these efforts to protect the machinery from misappropriation gave rise to the employees' duty not to divulge this information to defendant.

While still important tools in protecting proprietary information, the ease with which confidentiality agreements and other security procedures can be compromised by an insider, that is, a person who *acquired* the trade secret legitimately, may require a reconsideration of what measures constitute reasonable efforts at keeping information secret. The ease with which a computerized secret can be compromised with the click of a button has raised the stakes of misappropriation considerably. Once a secret has been introduced into the public domain it can never be recalled. Nevertheless, protecting confidential relationships that arise either out of contractual agreements or which are implied in law by virtue of the parties' relationship, will continue to be a central concern of trade secret law.[203]

c. *Shrinkwrap Licenses As A Reasonable Effort*

(6th Cir. 1968) (duty not to disclose customer information arose where high-level corporate officers formed a new venture in competition with their former company); Jet Spray Cooler, Inc. v. Crampton, 282 N.E.2d 921, 924, 174 U.S.P.Q. (BNA) 272, 274 (Mass. 1972) (employer-employee relationship may give rise to an implied duty of nondisclosure).

201. *Anaconda*, 485 F. Supp at 423, 205 U.S.P.Q. (BNA) at 734.

202. *Id.* at 415, 205 U.S.P.Q. (BNA) at 727.

203. The court in *Bendix Corp. v. Balax, Inc.*, 421 F.2d 809, 821, 164 U.S.P.Q. (BNA) 485, 495 (7th Cir. 1970), held that the existence of a confidential relationship was a condition precedent to a cause of action for misappropriation in cases where a defendant acquires the trade secret from its owner legitimately (for example, no wrongful acquisition), but subject to an obligation not to use or disclose it.

One possible approach to better protecting trade secrets from wrongful use or disclosure is to expand the scope of what constitutes a confidential relationship between the trade secret holder and one who ultimately receives or uses the information. A highly mobile workforce threatens to undermine the formation and duration of the types of confidential relationships which are at the heart of trade secret cases of years past. Today employees change jobs frequently in competitive and fast-paced industries. Moreover, courts have historically protected the rights of employees to change jobs and use their skills and knowledge for the benefit of different employers.[204]

In addition to protecting trade secrets at their source by forbidding the unauthorized use or disclosure, trade secret holders could also consider the potential for protecting trade secrets at their final destination. The use of shrinkwrap licenses presents one possibility for extending the protection of trade secrets contained in mass marketed consumer products. A shrinkwrap license is a printed warning or seal that the user of proprietary information (often a computer program available to the general public) must break in order to use the software. The license typically states that the information contained in the program is not truly being sold to the user, but is merely licensed to the buyer subject to certain terms and conditions.[205] The recent decision rendered by the Seventh Circuit Court of Appeals in *ProCD, Inc. v. Zeidenberg* held that such licenses are enforceable against the buyers of software programs, and may form the legal basis for the greater protection of trade secrets contained in, or acquired through, the use of information-based products.[206]

In *Zeidenberg*, the court concluded that the defendant purchaser of a telephone directory computer program was bound by the plaintiff software developer's terms and conditions of use, which were printed

---

204. *See, e.g.*, Valco Cincinnati v. N&D Mach. Serv., Inc., 492 N.E.2d 814, 818 (Ohio 1986) (quoting GTI Corp. v. Calhoun, 309 F. Supp. 762, 768, 165 U.S.P.Q. (BNA) 621, 625 (S.D. Ohio 1969)) ("Underlying almost every case in which a former employee is accused of the unauthorized disclosure or use of trade secrets is the matter of balancing ... the conflicting rights of an employer to enjoy the use of secret processes ... and the right of employees to earn a livelihood by utilizing their personal skill, knowledge and experience.").

205. ProCD, Inc. v. Zeidenberg, 908 F.Supp 640, 644-45, 650, 38 U.S.P.Q.2d (BNA) 1513, 1515, 1520 (W.D. Wis. 1996), *rev'd*, 86 F.3 1447, 39 U.S.P.Q.2d 1161 (7th Cir. 1996).

206. 86 F.3d 1447, 39 U.S.P.Q.2d (BNA) 1161 (7th Cir. 1996). The *Zeidenberg* decision was not the first to consider the operation of limitations on the usage of a computer-related product post sale. In *Data General Corp. v. Digital Computer Controls, Inc.*, 357 A.2d 105 (Del. Ch. 1975), the court gave effect to conditions of use contained in a standard form contract which came with a computer system, holding that the defendant was on notice of these restrictions prior to his wrongful use of the confidential information.

on both the inside and outside of the box in which the product was packaged.[207] The license terms prohibited a buyer from redistributing the telephone listings contained in the software. The defendant formed a corporation for the purpose of posting the information contained in the program on an Internet bulletin board, charging a fee to the public for access to the information.[208] The dissemination of these listings to commercial buyers undermined the plaintiff's pricing system, under which it sold the software to individual users at a lower rate than it did to commercial users.[209] In considering the enforceability of these licenses, the court cited other commercial transactions which are subject to licenses, restrictions, or other terms. These terms can become effective as against the buyer after the initial sale provided that: (1) the buyer was on notice of the terms and conditions, even if the specifics are not known at the point of sale; (2) the terms were available to the buyer for inspection; and (3) the buyer had the right to return the product is the terms are unacceptable.[210]

The court ruled that the Uniform Commercial Code permitted the parties to a commercial transaction to set the terms and conditions of the transaction by contract.[211] The plaintiff offered the use of the computer software to the buyer subject to its terms,[212] and the defendant accepted the product by using it.[213] The defendant had the opportunity to read plaintiff's terms and conditions, and was continually reminded of them when the program displayed the terms of the license each time it was booted into use.[214] The *Zeidenberg* court analyzed the plaintiff's claim of copyright infringement under contract law, concluding that the

---

207. *Zeidenberg*, 86 F.3d at 1450-53, 39 U.S.P.Q. (BNA) at 1163-65.

208. *Id.* at 1450, 39 U.S.P.Q. (BNA) at 1163.

209. *Id.* at 1449-50, 39 U.S.P.Q. (BNA) at 1162-63.

210. *See generally id.* at 1452-53, 39 U.S.P.Q. (BNA) at 1165. In this case, the court found that the defendant's purchase of the plaintiff's product fulfilled all three of these conditions. *See id.*

211. *Id.* at 1452, 39 U.S.P.Q. (BNA) at 1164-65.

212. *Zeidenberg*, 86 F.3d at 1452, 39 U.S.P.Q. (BNA) at 1164; UCC § 2-204(1) ("A contract for the sale of goods may be made in any matter sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract."). At issue was Wisconsin's state equivalent of the UCC, which did not "differ ... in any material respect" from the UCC. *See id.* at 1452.

213. *See* UCC § 2-606 (1995) (defining circumstances under which a buyer accepts the goods); UCC § 2-602 (1) (1995) (stating that the failure of the buyer to make a rejection within a reasonable time indicates acceptance subject to the terms and conditions of the contract).

214. *Zeidenberg*, 86 F.3d at 1452, 39 U.S.P.Q. (BNA) at 1164-65. The defendant was thus on notice of the restrictions contained in the shrinkwrap license.

defendant had used the product subject to the express terms of the shrinkwrap license, had violated those terms, and was therefore liable to the plaintiff for damages.[215]

Even though decided in the context of copyright infringement, the *Zeidenberg* decision represents a significant advance in the possibilities for trade secret owners to protect their information in the computer medium.[216] A shrinkwrap license could be attached or encoded into all proprietary information to put the recipient of information on notice of its confidential nature.[217] As in *Zeidenberg*, these terms and conditions should precede use, or, in the case of trade secrets, discovery of the protected information through such means as requiring the user's express assent to them. Having been made an "offer" by a trade secret owner for the limited use of a trade secret, an "accepting" recipient would then be bound by the terms and conditions of the license, and a confidential relationship would have been created contractually.[218]

---

215. The court expressly reserved a definitive determination on whether there are any differences between a contract and a license, which may have relevance under the first dale doctrine of copyright law. *See id.* at 1450, 39 U.S.P.Q. (BNA) at 1163; *see also* Copyright Act of 1976 (as amended), 17 U.S.C. § 109(b)(1)(A) (1994); Microsoft Corp. v. Harmony Computers & Elecs., Inc., 846 F. Supp. 208, 31 U.S.P.Q.2d (BNA) 1135 (E.D.N.Y. 1994). However, even if the first sale doctrine applies to shrink wrap licenses, the doctrine would not necessarily permit the purchaser of a computer program to use the trade secrets contained therein (usually in the object code of the program), for any use other than disposing of the product. Such a transfer does not bind the secondary purchaser, however, just as the secondary recipient of a trade secret is not bound by any duty to the (former) trade secret owner when the information is acquired from the public domain.

216. *But see* Peterson, *supra* note 46, at 449-450 ("Trade secret protection for mass-distribution software, at least as the result of a contractual obligation of confidentiality is . . . doubtful."); Judith A. Szepesi, *Maximizing Protection For Computer Software*, 12 SANTA CLARA COMPUTER & HIGH TECH L.J. 173, 176 (1996) ("Although used almost universally among software distributors, the enforceability of shrink-wrap agreements is questionable."); *see also* Step-Saver Data Sys. Inc. v. Wyse Tech., 939 F.2d 91 (3d Cir. 1991) (refusing to enforce a boxtop license disclaiming warranties); Arizona Retail Sys. v. Software Link, 831 F. Supp. 759 (D. Ariz. 1993). The policies underlying these cases, that warranties which guarantee minimum standards of product performance, cannot be disclaimed and are not a basis of the parties' bargain, would actually be *served* by giving effect to shrinkwrap terms which limit the unauthorized disclosure or use of trade secrets. *See, e.g.*, Kewanee Oil Co. v. Bicrom Corp., 416 U.S. 470, 481, 181 U.S.P.Q. (BNA) 673, 678 (1974) (explaining that preservation of minimum standards of commercial morality is a fundamental concern of trade secret law).

217. Trade secrets that are contained within computer programs can be concealed within the object code of a particular program, copy-protected, or otherwise obscured electronically from an inquiring user seeking access to the protected trade secret.

218. Such licenses would then, however, be subject to contract law defenses to their enforceability such as unconscionability and lack of assent to the license's terms. *See generally* E. ALAN FARNSWORTH, et al., FARNSWORTH ON CONTRACTS § 4.28 (1990) (explaining contemporary controls on the creation, modification and enforcement of contracts).

d. Marking And Labeling Of Trade Secrets In The Computer Environment

Marking and labeling of confidential information is another important procedure for putting the recipient of a trade secret on notice of its proprietary nature. This practice is especially relevant to the licensing of trade secrets to non-employee third parties who must receive some tangible representation of the trade secret, such as engineering or other drawings, in order for it to be put to productive use.[219] While marking or labeling information as confidential will not confer trade secret status on that item per se, it constitutes important evidence that the trade secret owner actually treated the information as secret.[220]

Such labeling can also be accomplished in a computer environment. Access to computerized trade secrets should be controlled in part through "warning" screens designed to put the computer user on notice of the nature of the information which is being accessed.[221] Typically, these "I agree to conditions" screens require the user to affirmatively assent to the terms of use before accessing confidential information by clicking "OK" with the mouse or keyboard.[222] These screens also indicate that accepting the owner's terms and conditions presumes that the user has actually read and assented to those conditions, whether the user has in fact done so or not. Such warnings constitute evidence of

---

219. *See, e.g.,* Rockwell Graphic Sys., Inc. v. DEV Indus., 925 F.2d 174, 179-180, 17 U.S.P.Q. (BNA) 1780, 1784-85 (7th Cir. 1991); Data General Corp. v. Digital Computer Controls, 357 A.2d 105, 109 (Del. Ch. 1975) (holding drawings which bore proprietary notices, in conjunction with the standard form contracts which came with a computer system, as evidence of reasonable efforts at protecting trade secrets from unauthorized use); *see also* CVD, Inc. v. Raytheon Co., 769 F.2d 842, 853, 227 U.S.P.Q. (BNA) 7, 12-13 (1st Cir. 1985) (failure of trade secret owner to follow its own procedures for stamping and marking of confidential drawings weighs against a finding that owner treated the information as "secret").

220. The trade secret holder must be careful not to "cry wolf" unnecessarily. Marking everything as confidential, whether proprietary or not, may indicate a lack of specificity as to what actually constituted the trade secret. A trade secret holder, in order to prove a protectible interest in his or her information, must be able to identify, with some degree of particularity, precisely what information is claimed as a trade secret. *See* MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 522-23, 26 U.S.P.Q. (BNA) 1458, 1466-68 (9th Cir. 1993) (computer software cannot claim the existence of trade secrets generally in programs, but must specifically identify which elements of its programs are secret); Universal Analytics Inc. v. MacNeal-Schwendler Corp., 707 F. Supp 1170, 1177 (C.D. Cal. 1989) (requiring plaintiff to establish precisely which trade secrets were misappropriated). Conversely, overclaiming trade secret protection through such means as marking drawings which may or may not be confidential is not in itself fatal to a claim for misappropriation. *See* Rockwell Graphics, 925 F.2d at 176-77, 17 U.S.P.Q.2d (BNA) at 1782.

221. Many software programs display this type of information screen, essentially putting the user on notice of any information contained in these screens.

222. *See* Cundiff, *supra* note 165.

reasonable efforts undertaken by the trade secret owner to protect trade secrets in a computer environment.

e. *Other Technological Means For Implementing Reasonable Efforts At Protecting Secret Information*

Technological responses specific to the computer environment are also an essential part of both the physical and the procedural security regime. Building digital "firewalls" between confidential and non-confidential information is one way to accomplish this. "Firewall" software prevents access to the information stored in one area of a computer network from beings accessed from an "unauthorized" terminal.[223] However, because the Internet permits joint access from different computer terminals to "common" areas of cyberspace, such as through computerized BBS's which "exist" apart from any particular terminal but which can be accessed by both, firewalls are not always effective.[224] Passwords that restrict access to sensitive information are also an important means for protecting private information, as the court recognized in the *Peoplesoft* decision.

Specialized document management systems can keep a trade secret owner informed as to who is accessing, modifying, or copying confidential information.[225] Likewise, services that are readily available on the Internet, often for free, can guide trade secret holders toward programs and procedures designed to protect the privacy of electronic mail ("e-mail") and other Internet-related communications.[226] First and foremost, trade secrets should never be e-mailed because e-mail messages are not entirely secure from access by computer hackers. Additionally, e-mail messages can easily be sent to the wrong address at the touch of a key and messages can easily be forwarded to other e-mail accounts without the consent of the original sender.[227]

---

223. This can be accomplished by simply excluding certain files from computers to which unauthorized personnel have access, by requiring passwords for access to particular files, and so forth. *See* Robert C. Scheinfeld & Parker H. Bagley, *Protection Issues on the Internet*, N.Y. L.J., Jan. 24, 1996, at 3. (defining Internet-related terms such as "firewalls" and "encryption").

224. *See* Victoria Cundiff, *The New York Law of Trade Secrets: A Practical Guide*, N.Y. State B.J. May-June 1995, at 32.

225. *Id.*

226. A cursory search of the keyword "privacy" produces thousands of Internet based services centered around the discussion of privacy issues on the Internet, as well as potential digital solutions to keeping confidential information private.

227. In addition to a trade secret holder's concerns about the security of computerized communications, the widespread use of electronic mail has spawned a host of new legal dilemmas concerning workplace privacy. *See* Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa.

Once the province of spy stories, encryption or coding of everyday Internet-based communication is rapidly becoming a crucial part of secure financial transactions and communications conducted over the Internet.[228] Encrypted messages prevent all but the designated recipient of the confidential information, who has a digital key to decode the message, from accessing it. The adoption of an international standard technology for the encryption of private Internet communications could rapidly advance the security of the Internet as a commercial environment.[229] The effectiveness of encryption technology in permitting private and instantaneous communication worldwide has also attracted the attention of law enforcement officials, who fear that such secure communication could serve as a vehicle for crimes other than the misappropriation of trade secrets.[230] While none of these measures guarantee secrecy, all can constitute evidence that the secret holder has undertaken reasonable efforts to protect the information, an essential element in demonstrating the existence of a protectible trade secret.

III. THE INTERNET AND THE PUBLIC DOMAIN—*RELIGIOUS TECHNOLOGY CENTER V. NETCOM*; THE CONTOURS OF THE "PUBLIC DOMAIN" AND KEEPING YOUR TRADE SECRETS FROM BECOMING "GENERALLY KNOWN"

1996) (considering an employee's expectation of privacy in workplace electronic mail messages); Jill L. Rosenberg, *Legal Issues Surrounding Employee Hiring, Privacy and Investigations*, in 25th ANNUAL INSTITUTE ON EMPLOYMENT LAW, at 569 (PLI Litig. & Admin. Practice Handbook Series No. 547, 1996); Hardy, *supra* note 154, at 1008 (discussing the legal issues surrounding e-mail in the workplace).

228. *See* Scheinfeld & Bagley, *supra* note 223; Security and Freedom through Encryption (SAFE) Act: Hearings on H.R. 3011 before the House Comm. On the Judiciary, 104th Cong. 64 (1996) Statement of Roberta R. Katz, Senior Vice President, General Counsel & Secretary, Netscape Communications Corp [hereinafter Katz].

229. *See* Katz, *supra* note 228. Ms. Katz outlined the importance of encryption technology in Internet-based commercial activity. In short, encryption would permit the already explosive growth of commerce on the Internet to continue, while simultaneously protecting companies' ability to communicate confidential information securely. Ms. Katz addressed concerns that the export of cutting edge U.S. encryption technologies would become a weapon in the hands of terrorists, arguing that wrongdoers already have access to less powerful encryption technology and that the national security interest would in fact be better served through the marketing and open export of American encryption technology. One way this interest could be served is through establishing a mandatory key escrow (i.e., depositing a key to privately encrypted communications) that would permit government access to encrypted communications under controlled circumstances.

230. Sandra Ann Harris, *Reno Warns of Encryption in Cyberspace*, BC Cycle, June 14, 1996 (available in LEXIS *curnews* file) (discussing the possibility for use of encryption technology by terrorists, identifying the balance which must be struck between serving legitimate, private business interests and protecting public safety).

A. *A Foreshadowing of Litigation to Come:* Religious Technology Center v. Netcom

Arguably the most pressing challenge posed by the Internet to trade secret law is the ease and speed that information can go from being secret to being part of the public domain. The availability of bulletin board systems, the prevalence of newsgroups and e-mail that permit instantaneous exchange of ideas, and the sheer size of the audience that a disclosed trade secret could be published has changed the question of when a trade secret has become generally known. Similarly, the ease in which a vast body of individual users can access such information using ordinary term searches on an Internet browser[231] may alter the inquiry as to whether, and when, information disclosed in this respect is readily ascertainable.

The question of when an Internet posting has become generally known dovetails logically with other interrelated concepts that define the protection of trade secrets, including what constitutes reasonable measures to keep the information secret and how valuable the information is, given the relative ease of access. While cases dealing with these questions are sparse, *Religious Technology Center v. Netcom*[232] represents one court's attempt to decipher the question of when a trade secret, which has been placed on an Internet bulletin board becomes generally known.

In *Netcom*, plaintiff Religious Technology Center ("Center"), a Church of Scientology,[233] sought a preliminary injunction against defendants Netcom On-line Communication Services, an Internet service provider, Dennis Erlich, a former Center minister, and Tom Klemsrud, the operator of a computerized bulletin board system, for the misappropriation of trade secrets.[234] The suit arose when Erlich, having become a critic of the Scientology's theories and methods, acquired parts of the Center's Advanced Technology ("AT") documents. These spiritual teachings of the late L. Ron Hubbard, the Center's founder, were

---

231. A browser is a computer program that permits the user to access the information on the Internet in a user-friendly fashion. Popular browsers include Netscape and Microsoft Explorer.

232. Religious Tech. Ctr. v. Netcom On-Line Communication Servs., 923 F. Supp. 1231 (N.D. Cal. 1995).

233. The Church of Scientology is considered by the Internal Revenue Service to be a not-for-profit religious institution. *All Things Considered* (National Public Radio broadcast, Mar. 12, 1997).

234. *Netcom*, 923 F. Supp. at 1234-40. The defendants were also accused of copyright infringement.

used by the Center during the course of spiritual auditing,[235] and were heavily guarded from disclosure to unauthorized persons and non-members.

Erlich allegedly posted the AT excerpts on Klemsrud's bulletin board under the newsgroup "alt.religion.scientology" for the purpose of criticizing the Center's methods and ideology.[236] Two groups of AT documents were at issue in the case. The first group consisted of materials, Erlich alleged, had already become part of the public domain, including materials which had become part of the public record in a related case,[237] materials which had already been posted on the Internet when the *Netcom* suit was commenced,[238] and materials which Erlich allegedly received anonymously through the mail (the "Exhibit A" works).[239] The second group of documents was unpublished Center documents that had not been disclosed or made public prior to Erlich's posting of them on the Internet bulletin board (the "Exhibit B" works).[240]

The alleged secrecy of the AT works was central to the plaintiff's claim that irreversible economic and spiritual damage was suffered when these materials were posted and automatically distributed to all members of Erlich's discussion group.[241] In evaluating this claim, the

---

235. *Id.* at 1238 n.4. This process uses the Center's religious texts for the purpose of gradually moving its members towards a "higher spiritual existence."

236. *Id.* at 1243. The court accepted that Klemsrud's purpose for the postings was "criticism or Article" in passing upon the Center's claim of copyright infringement stemming from the defendants' allegedly unauthorized duplication of the AT works.

237. *See* Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 37 U.S.P.Q.2d (BNA) 1258 (E.D. Va. 1995). The court granted summary judgment to defendant The Washington Post for misappropriation of the Center's trade secrets when the Post published a story about the Center's ongoing litigation battles. The Post ultimately acquired the AT materials, which it quoted from in parts of its story, from an affidavit filed by Steven Fishman, who, like Erlich, was a disgruntled former Center member being sued for misappropriation. The affidavit contained 69 pages of the Center's AT works. *See* Church of Scientology v. Fishman, 1994 WL 467999, (9th Cir. 1994) (unpublished opinion available only on WESTLAW).

238. *See Lerma*, 908 F. Supp. at 1364, 37 U.S.P.Q.2d (BNA) at 1259. The defendant, Arnaldo Lerma, obtained a copy of the Fishman affidavit and posted portions of the AT works on the Internet via Digital Gateway Systems, an Internet services provider.

239. *Netcom*, 923 F. Supp. at 1256.

240. *Id.* at 1239-40.

241. *Id.* at 1239. According to the plaintiff, the AT works would not only spread the Center's proprietary information to splinter religious groups and other competitors, but would also damage its members spiritually. The Center provides spiritual guidance to its members, who proceed through ascending levels of auditing. Each level must be studied, using the relevant texts and materials, before the next spiritual level can be achieved. Disclosing the information prematurely would expose the listener to spiritual concepts for which he or she was not ready, thereby endangering the plaintiff's very mission.

court first considered whether the information posted by Erlich constituted a protectible trade secret.[242] The court required a showing that the information was of sufficient value in the owner's operation of its enterprise such that it provided an actual or potential advantage over others who did not know or use the information.[243] The plaintiff only needed to demonstrate that the information would have been potentially valuable to a competitor, and not whether it was actually valuable to the particular defendant in the case.[244] The court rejected the defendant's argument that the AT works were devoid of value because the Center depended upon the donations and fees paid by its parishioners for its existence, part of which were paid to use or explore the AT works.[245]

Second, the court focused upon the secrecy of the information at issue.[246] It reviewed other judicial constructions of efforts that are reasonable under the circumstances, including warnings to employees regarding the secret nature of the proprietary information, limiting access to sensitive information to a "need to know" basis, and the use of confidentiality agreements.[247] The safekeeping system employed by the plaintiff, which included an elaborate system of locked cabinets, safes, and logging and identification of materials, plus the limited availability of the AT materials at only a handful of sites worldwide, was the basis for the court's conclusion that the Center's efforts fell within UTSA's definition of "efforts which are reasonable under the circumstances."[248]

The Center, however, ultimately failed to demonstrate the existence of a protectible trade secret in the AT works, however, for two reasons: (1) the Exhibit A materials had become part of the public domain prior

242. *Id.* at 1250-51. Recognizing the existence of a protectible trade secret is characteristic of the property-first approach to trade secret litigation which is typically used in cases decided under UTSA.

243. *Id.* at 1252.

244. *Netcom*, 923 F. Supp. at 1256.

245. *Id.* at 1251. The court also held that the Center's status as a religion does not itself preclude it from holding a trade secret. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. d (1995) ("[N]onprofit entities such as ... religious organizations can also claim trade secret protection for economically valuable information ....").

246. *Netcom*, 923 F. Supp. at 1231.

247. *Id.* at 1253.

248. *Id.* at 1253-54. The Center's efforts included use of locked cabinets, safes, logging and identification of the materials, availability of the materials at only a handful of sites worldwide, electronic sensors attached to the documents, locked briefcases for transporting works, alarms, security personnel, and confidentiality agreements for all of those who had access to the works. The Center's procedures convinced the court to draw the inference that these materials were secret on the basis of their efforts alone.

to the Center's suit,[249] and (2) the plaintiff failed to identify precisely which of the Exhibit B works (those that had *not* become generally known) had been misappropriated by Erlich.[250] The court concluded that the Exhibit A materials had become part of the public domain, and hence both generally known and readily ascertainable, in part because of their prior publication by posting on the Internet. This defeated the possibility that the Center could continue to claim these materials as protectible trade secrets.[251]

The court, however, was clearly troubled by its conclusion; that the posting of information to an Internet bulletin board, at which time it became accessible to millions of potential Internet users, defeated the possibility for the information to continue to receive protection as a trade secret.[252] The court reasoned that while the Internet had not yet reached the status where a temporary posting on a newsgroup was akin to publication in a major newspaper or broadcast on a television network, those with an interest in using the Center's trade secrets to compete with the Center were likely to look at the posted AT works, as were other interested members of the scientology newsgroup.[253] Notwithstanding these reservations, the court found no authority to negate the finding that the information's secret character could not be recaptured once it had been released into the public domain.[254]

The *Netcom* decision reiterated the rule that trade secret protection can be claimed only for information that fits within the statutory definition of a trade secret, and that this status is defeated when the secret is posted to the Internet, making it generally known.[255] The decision also

---

249. *Id.* at 1257.

250. *Id.* at 1252, 1254. Because the *Netcom* court considered only whether to issue a preliminary injunction, it stated only that it was unable to determine whether the Exhibit B materials had been disclosed to the public. While this did not preclude the possibility of recovery for Erlich's posting of secret materials, the absence of an injunction meant that the materials could remain exposed to the public on the Internet, quickly destroying any possibility that they would remain secret.

251. *Netcom*, 923 F. Supp. at 1256 ("To the extent that someone uses or discloses any information taken from [the Exhibit "A" materials], there is clearly no trade secret claim.").

252. *Id.* (stating the court was "troubled by the notion that any Internet user, including those using 'anonymous remailers' to protect their identity, [can] destroy valuable intellectual property rights by posting them over the Internet.").

253. *Id.* at 1256.

254. *Id.* ("While the court is persuaded by the Center's evidence that those who made the original postings likely gained the information through improper means, as no one outside the Center or without a duty of confidence would have had access to the works, this does not negate the finding that, once posted, the works lost their secrecy.").

255. *See In re* Remington Arms Co., 952 F.2d. 1029, 22 U.S.P.Q.2d (BNA) 1063, 1066 (8th Cir. 1991); FMC Corp. v. Taiwan Tainan Giant Indus. Co., 730 F.2d 61, 63 (2d Cir. 1984)

reaffirmed the rule that one may not prosecute a claim for misappropriation against a person who uses information acquired without any wrongful conduct, such as through the use of the materials available on the Internet. While correctly decided as to these points of trade secret law, the *Netcom* decision failed to detail explicitly how, when, and under what circumstances, information becomes part of the public domain. A closer examination of the circumstances under which information is introduced into the public domain might present possibilities for protecting trade secrets *notwithstanding* their posting on the Internet.[256]

For example, in *Religious Technology Center v. Lerma*, the court considered whether materials attached to the Fishman affidavit had actually been viewed by the relevant public.[257] The court noted that the materials had been exposed as public documents for an extensive period of time, notwithstanding the Center's extraordinary efforts to prohibit access to the file.[258] The Center's application for a sealing order to prevent disclosure of the AT works had likewise failed.[259] Therefore, it was not the filing of the affidavit per se that destroyed the secrecy of the AT documents, but rather the fact that the AT had been available in the public record for a period of over two years. These works had also been publicized in a major newspaper, clearly making these materials generally known and a part of the public domain. The *Lerma* court implicitly rested its conclusion that the AT documents were not trade secrets on the ample evidence that the documents had *in fact* been viewed by the public.[260]

("A trade secret once lost is, of course, lost forever.").

256. *See* Architectronics, Inc. v. Control Sys., Inc., 935 F. Supp. 425 (S.D.N.Y. 1996) (holding that whether elements, or a combination of elements, in a computer software program were generally known is factual question appropriate for the jury).

257. *See* Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 1364, 37 U.S.P.Q.2d (BNA) 1258, 1259 (E.D.Va. 1995).

258. *Id.* The *Lerma* court noted that the AT documents had been available in the court's public records between April 14, 1993 and August 15, 1995, a total of twenty-eight months. The Post was able to acquire a copy of these documents, which it used to write its story. The court had little trouble, as an evidentiary matter, assuming that the documents had *in fact* become generally known.

259. *Netcom*, 923 F. Supp. at 1255.

260. The *Netcom* court may have implicitly relied on the *Lerma* court's factual finding that those portions of the Exhibit "A" works which had been posted on the Internet remained available for ten days and that scientology dissidents increasingly turned to the Internet to share information. *See Lerma*, 908 F. Supp. at 1365, 37 U.S.P.Q.2d (BNA) at 1368. A closer question may be presented where a trade secret is introduced into a less traveled area of the Internet.

B. A Careful Examination of the Divide Between "Known" and "Knowable": Actual vs. Potential Access to Trade Secrets that are Misappropriated Onto the Internet

An equally rigorous examination of the circumstances under which alleged computerized trade secrets are posted to the Internet may permit courts, in some instances, to uphold the secrecy of information which has been posted on the Internet.[261] Specifically, a line may be drawn between trade secrets that have actually been accessed by Internet users and trade secrets that merely became potentially accessible for a limited period of time.[262] Moreover, the possibility remains that an exposed trade secret can be cured through giving timely notice of the information's proprietary nature to those who would have had actual access to it. In short, courts must familiarize themselves with the technological possibilities for electronically tracking and erasing trade secrets that are misappropriated via the Internet, potentially reestablishing the element of secrecy notwithstanding a wrongful misappropriation.[263]

Authors have questioned whether a trade secret that is surreptitiously placed on the Internet can automatically be assumed to have become part of the public domain.[264] Three factors should guide the de-

---

261. *Cf.* McDonald, *supra* note 2. The authors note that merely sending e-mail, for example, probably does not eliminate the message's veil of secrecy. While e-mail is susceptible to being intercepted or republished, it is a criminal offense to intercept or read an e-mail message without the consent of its sender. "That a criminal act is necessary to lose secrecy will probably preclude a claim that using e-mail is a per se failure to take reasonable steps to maintain secrecy." *Id.* Similarly, mere use of e-mail alone should not give rise to an irrebuttable presumption that the information has become generally known merely because it could become so at the touch of a button.

262. In *Gates Rubber Co. v. Bando Chem. Indus., Ltd.*, 9 F.3d 823, 849, 28 U.S.P.Q. (BNA) 1503, 1521 (10th Cir. 1993), for example, the court found that the information retained its trade secret status despite being disclosed at a hearing, where plaintiff evidenced continuing intent to maintain its secrecy by acting to seal the record. While not decided in the Internet context, this case presents the possibility that trade secret status may be maintained where a plaintiff exercises due diligence to retain the element of secrecy. Permitting recovery under these circumstances is not at all unlike the mode of analysis used for determining whether a plaintiff has taken reasonable measures to protect the information, permitting recovery even where the information has not been kept absolutely secret. *See supra* notes 178-181 and accompanying text.

263. Internet use creates electronic footprints which permit skilled computer users to track data. Anonymous remailers are services which erase a computer user's identity in Internet communications. *See* Reno v. American Civil Liberties Union, ___ U.S. ___, 117 S. Ct. 2329, 2353-55 (1997) (discussing the progressive, though incomplete, process through which Internet users and providers are zoning cyberspace, that is controlling electronically who may view the contents of a particular web page of posting).

264. *See, e.g.*, James Pooley, *Is Nothing Secret? - The Newest Communications Medium*

termination of whether information has truly become generally known: (1) the size of the relevant "public" to which the trade secret is published, (2) the nature of the information misappropriated, and (3) the amount of time for which the secret was exposed. Taken together, these factors could sufficiently weigh in favor of a trade secrets plaintiff in a trade secret suit asserting that the information had remained a secret notwithstanding its posting on the Internet. This analysis should also take into consideration whether the trade secret owner had undertook reasonable measures to erase or to retrieve the trade secret, and whether there is evidence of actual use of the trade secret.

1. The Size of the Public

Unquestionably, the Internet represents a vast gathering of people interconnected by the web of Internet connected computers. The sheer size of the audience could potentially *support* a trade secret holder's claim to the continued secrecy of the information, as millions of postings circulating through cyberspace between all of the nations of the world might obscure the visibility of a single addition. Use of the Internet might therefore require a closer examination of when information is truly known.

The court in *Laird* noted that to define whether secret information is or is not readily ascertainable and therefore not generally known, it is necessary to consider whether the information at issue has been acquired, digested, and expressed in the form of journal articles and publications specific to the industry to which the information is relevant.[265]

Threatens Business Information, THE RECORDER, p.4 (Nov. 6, 1996) (available in LEXIS *curnews* file) (arguing that whether misappropriated information on the Internet has become "generally known" should depend on: (1) the amount of information that was exposed relative to the "entire" secret; (2) the time of exposure; (3) the extent to which Internet users actually accessed the information; (4) whether the disclosure was to a defined group; (5) the extent to which the information was disclosed to persons in a position to understand it; (6) whether the owner of the information took prompt action by giving notice and seeking to correct the situation by self-help and through the courts; and (7) the extent to which those who had actual access to the information relied upon or used it). *But see* Eduardo M. Carreras, *Intellectual Property: First Casualty on the Information Highway?*, ACCA Docket, Jan.-Feb. at 26, 30 (1995) (arguing that posting a secret onto the Internet irrevocably destroys the element of "secrecy"). Recent cases have begun to equate the Internet with the public domain. *See* Whirlpool Fin. Corp. v. GN Holdings, Inc., 873 F. Supp. 111 (N.D. Ill. 1995), *aff'd*, 67 F.3d 605 (7th Cir. 1995); Religious Tech. Ctr. v. F.A.C.T.NET, Inc., 901 F. Supp. 1519, 1527, 36 U.S.P.Q.2d (BNA) 1690, 1695-96 (D. Colo. 1995); Castano v. Am. Tobacco Co., 896 F. Supp. 590, 595 (E.D. La. 1995).

265. *See* Amoco Prod. Co. v. Laird, 622 N.E.2d 912, 917, 30 U.S.P.Q.2d (BNA) 1515,

Underlying this approach were certain assumptions about the medium in which information is published; specifically, that articles discussing the information claimed to be secret represent the end product of a thoughtful and somewhat time consuming process of analyzing and expressing the information claimed to be a secret.[266] Under these circumstances, it is logical to deny the information trade secret protection on the basis that anyone in the industry knows that the information is "old hat" by looking to the literature.

The sheer amount of information available in cyberspace defies this assumption however. It is less likely that one who is merely surfing the Internet will *necessarily* give the same degree of attention to proprietary information which has been posted on the Internet as would an author of a trade journal article published through conventional means. Discovery of a trade secret on the Internet, which would make the information generally known, is dependent upon two separate events: (1) that the Internet user had actual access to the trade secret, and (2) that the user gained some consequent understanding of its meaning or importance. Internet technology has made the occurrence of the first event more simple than it has ever been in the past. The second stage, however, requires a closer examination. Whether a trade secret has truly been known necessarily implies some understanding of its importance and some possibility that the trade secret could be used by the recipient.

The type of Internet service employed to disseminate the trade secret will play a factor in whether the information is received by people who are able to understand its importance. The *Netcom* court noted that the people most likely to have accessed the Center's AT documents were participants in the scientology newsgroup organized by Tom Klemsrud.[267] The court in this case did not have to reach the issue of whether a trade secret posted on an obscure web page, or one which is sent to a single competitor via electronic mail, has truly become generally known. Where actual evidence that a misappropriated trade secret has been both readily ascertainable in cyberspace, and that the material

---

1518 (Ind. 1993).

266. In the past, materials that had been published and available to an appreciable number of people, such as through a television network or in a major newspaper, usually implied that the information had gone through some process of editing, dissection or analysis. The Internet permits any user to potentially become an instant publisher to millions and defeats this assumption. A court might conclude that because the information appears in cyberspace, it does not necessarily mean that the information had undergone a similar process of understanding or analysis. This would change the definition of when something is generally known. *See generally* Hardy, *supra* note 154.

267. Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 923 F. Supp. 1231, 1254-55 (N.D. Cal. 1995).

had been "hit," or viewed, by people able to understand its importance, the secret has lost its protected character. In the absence of such evidence, courts should pause before concluding that a trade secret introduced in some way into cyberspace has become generally known.

2. The Nature of the Trade Secret

Another consideration underlying whether a trade secret has become generally known or readily ascertainable is the nature of the information itself. The *Electro-Craft* court noted the difference between intuitive, or obvious, trade secrets and those that are obscure or discoverable only through careful analysis or inspection.[268] A secret customer list that contains the names and needs of important buyers, for example, may be more readily ascertainable or understandable to one with access to this secret over the Internet than would be a complex chemical formula or a list of tolerances for specialized machinery. The complexity of the misappropriated secret will impact both the size of the relevant public by delineating the number of people who would seek access to this secret from the sea of information available over the Internet in the first place, as well as the degree to which the information could then be "known" by these onlookers.

3. The Time For Which the Secret Was Exposed

Obviously, the longer a trade secret remains in a medium in which it can be so easily accessed, the more likely that it will in fact be accessed by those who are interested in it. The *Netcom* court considered this exposure in holding that the documents that had been attached to the Fishman affidavit became public knowledge.[269] Similarly, courts considering claims for trade secret misappropriation over the Internet could consider whether the plaintiff had successfully traced and removed the stolen secret prior to its having become generally known. A court could then draw a distinction between a trade secret which had truly become generally known and one that had been merely knowable, but retrieved with no evidence of actual discovery by the relevant public.

A plaintiff could also exercise due diligence following the misappropriation of a trade secret by posting notice of the protected nature of the secret in the same areas of cyberspace in that a secret is most likely to be discovered. This would place the recipient of a secret squarely

268. Electro Craft Corp. v. Controlled Motion Inc., 332 N.W.2d 890, 899, 220 U.S.P.Q. (BNA) 811, 817 (Minn. 1983).

269. *See supra* notes 232-246 and accompanying text.

within the definitions of misappropriation which forbids disclosure or use by one who has acquired a trade secret with knowledge that it had been wrongfully acquired.[270] Even if the notice is ineffective to prevent a trade secret, widely accessed via the Internet, from becoming generally known, notice could potentially permit a trade secret owner to prosecute claims for misappropriation against users of the secret who can be proven to have received this notice. In these ways, the legal elements of trade secret claims can be adapted to the realities of the age of the Internet. The Internet, while it unquestionably presents a host of new challenges to the protection of proprietary information, need not spell the end of trade secret law protections.

CONCLUSION

Trade secret law must continue to evolve while addressing new technological realities. The age of the Internet presents significant challenges to the protection of proprietary information. Tortious conduct, such as industrial espionage, threatens the security of secret information vital to the operation of businesses worldwide. Similarly, the ease and speed with which information can be introduced into the public domain, destroying the element of secrecy, has increased dramatically in a world ever more dependent upon computer communications. Notwithstanding these challenges, trade secret holders, lawyers, and courts alike can educate themselves in the operation of this new technology in an effort to isolate and implement effective measures for protecting trade secrets. Similarly, a familiarity with this new medium will permit courts to separate information which has truly become part of the public domain from information that slips only briefly into the vast sea of information available on the Internet. Through these efforts, trade secrets and trade secret law may continue to peacefully exist in an Internet-connected world.

270. *Cf.* IMED Corp. v. Systems Eng'g Assocs. Corp., 602 So.2d 344 (Ala. 1992) (stating that an individual who knew, or should have known at the time the individual used or disclosed the trade secret, that the trade secret was acquired in breach of a confidential relationship by a third person is liable for misappropriation).