TRADE SECRETS – THE NEW RISKS TO TRADE SECRETS POSED BY COMPUTERIZATION

By Andrew Beckerman-Rodau*
Suffolk University Law School – Boston, MA
E-mail: arodau@suffolk.edu
Web page: www.law.suffolk.edu/arodau
Copyright 2002 by Professor Andrew Beckerman-Rodau
(Originally published in 28 Rutgers Comp. & Tech. L. J. 227)

INTRODUCTION

Business enterprises have always relied on intellectual property to further economic goals.[1] Well-known trademarks have been critical to the success of many consumer products companies that have spent years inculcating the public with an association between their products and a specific trademark.[2] Entire industries, such as publishing, music, and software, rely on intellectual property rights afforded by copyright law[3] to protect their investments. Patents[4] provide protection for much of the research and development activities conducted by commercial enterprises. Trade secret law[5]

---

* Professor of Law, Suffolk University Law School, Boston, Massachusetts. B.S., 1976, Hofstra University; J.D., 1981, Western New England College; LL.M., 1986, Temple University. Website: *www.law.suffolk.edu/arodau;* e-mail: arodau@suffolk.edu. This article is based on materials prepared for and distributed at a continuing legal education program on intellectual property law presented at Suffolk University Law School on November 16, 2001.

1. *See, e.g.*, Aimee A. Watterberg, *Perfecting a Security Interest in Computer Software Copyrights: Getting it Right*, 15 J. MARSHALL J. COMPUTER & INFO. L. 855, 858 (1997) (explaining that intellectual property has been used as collateral to raise money in the past by famous inventors such as Thomas Edison).

2. *See, e.g.*, *In re* Owens-Corning Fiberglass Corp., 774 F.2d 1116, 1127 (Fed. Cir. 1985) (noting evidence that advertising expenditures to develop recognition of trademark exceeded $42 million); *see also* Quality Inns Int'l, Inc. v. McDonald's Corp., 695 F. Supp. 198, 212 (D. Md. 1988) (noting that McDonald's spends almost a billion dollars a year on marketing and advertising.).

3. 17 U.S.C. §§ 101-1101 (1994) (giving the provisions for federal copyright law).

4. 35 U.S.C. §§ 1-376 (Supp. 1999) (giving the provisions for patent law).

5. *See* UNIF. TRADE SECRETS ACT § 1 (amended 1985), 14 U.L.A. 433, 438

is utilized both as an alternative to patent protection and to protect commercial information that is outside the scope of patent protection.

The modern development of technology significantly impacts intellectual property. The increasing reliance on modern technology has resulted in intellectual property comprising a substantial portion of the business assets of modern commercial enterprises.[6] This is in contrast to the past when most business assets consisted of tangible property.[7] As a result, enterprises are increasingly utilizing intellectual property laws to protect the value of their intellectual property.[8] Correspondingly, the domain of intellectual property law has expanded to cover more types of intellectual assets.[9] This protection increases the economic value of such assets. Nevertheless, the modern development of technology has adversely affected the value of some intellectual property. For example, the widespread availability of the Internet,[10] coupled with its global reach, allows rapid and inexpensive dissemination of

(1990).

6. The value of intellectual property accounts for two-thirds of the market valuation of U.S. corporations. Jenna Greene, *Patent Office at Center Stage*, THE NAT'L L.J., Jan. 15, 2001, at B8. *See* Lars S. Smith, *Trade Secrets in Commercial Transactions and Bankruptcy,* 40 IDEA 549 (2000) ("[M]ajor assets of many corporations exist in the form of patents, copyrights, trademarks, and trade secrets . . ."). *See also* Mark A. Lemley, *Reconceiving Patents in the Age of Venture Capital*, 4 J. SMALL & EMERGING BUS. L. 137, 138 (2000) (noting the significant increase in the number of patents being issued).

7. *See* Lee G. Meyer*, Intellectual Property in Today's Financing Market*, 2000 ABI J. LEXIS 34, at *20 (Mar. 2000) (noting that, historically, the value of an enterprise was based on the land it owned; during the industrial revolution the value of an enterprise was based on the capital goods it owned; today, intellectual property is increasingly important in determining the value of an enterprise).

8. U.S. universities are also increasingly relying on intellectual property protection. In 1999, they filed more than 7600 patent applications and entered more than 3000 licensing agreements. Antonio Regalado, *Research, Red Ink: An Academic Group Seeks Balance,* WALL ST. J., Jan. 14, 2002, at B4.

9. Broader legal protection has also been adopted for intellectual property. In addition to civil law protection, the criminal law has been extended to intellectual property. *See, e.g.*, 18 U.S.C. § 1832 (2000) (criminal sanctions for theft of trade secret); *id*. at § 2320 (providing criminal sanctions for trademark counterfeiting); *id.* at § 2319 (criminal infringement of copyright).

10. *See generally* Michael A. Geist, *The Reality of Bytes: Regulating Economic Activity in the Age of the Internet*, 73 WASH. L. REV. 521, 525-30 (1998) (discussing operation and history of Internet).

data.[11] As a result, intellectual property that can be converted into digital data, such as music, software, and movies, can be distributed almost immediately, via the Internet, to literally millions of individuals for negligible cost.[12] This rapid dissemination reduces the ability to control access to intellectual property, which negatively affects its economic value. Additionally, the global reach of the Internet imposes significant jurisdictional limitations on the utilization of legal remedies to protect intellectual property, since legal redress under our system is generally based on the geographic location of the infringing party.[13] One response to this procedural problem has been enactment of at least some federal statutes that reach beyond the geography of the United States.[14] Another response has been the advent of intellectual property protection as an important trade issue that is addressed in trade discussions among the various nations of the world. This has resulted in the creation and adoption of international agreements to ensure worldwide protection of intellectual property.[15]

This article will specifically address the impact of modern technology on trade secret law. Part I will provide an overview of United States trade secret law; Part II will discuss specific threats

11. *See* Blumenthal v. Drudge, 992 F. Supp. 44, 49 (D.D.C. 1998) (noting that the Internet enables people to communicate with one another with unprecedented speed and efficiency); Florida v. Cohen, 696 So. 2d 435, 439 (Fla. Dist. Ct. App. 1997) (noting that the Internet allows virtually instantaneous worldwide distribution of images).

12. *See* Bruce W. Sanford & Michael J. Lorenger, *Teaching an Old Dog New Tricks: The First Amendment in an Online World*, 28 CONN. L. REV. 1137, 1159 (1996) (explaining how the Internet facilitates unauthorized copying and dissemination of intellectual property).

13. *See generally In re* Microsoft Corp. Antitrust Litigation, 127 F. Supp. 2d 702, 716-17 (D. Md. 2001) (asserting that drawing jurisdictional distinctions on the basis of geographic boundaries is archaic in light of the Internet).

14. *See, e.g.,* 18 U.S.C. § 1837 (2000) (extending penalties for trade secret theft to certain acts occurring outside the United States).

15. *See, e.g.,* Agreement on Trade Related Aspects of Intellectual Property Rights, Including Trade in Counterfeit Goods of the General Agreement on Tariffs and Trade (commonly referred to as the "TRIPS Agreement") (reprinted in PAUL GOLDSTEIN, EDMUND W. KITCH & HARVEY S. PERLMAN, SELECTED STATUTES AND INTERNATIONAL AGREEMENTS ON UNFAIR COMPETITION, TRADEMARK, COPYRIGHT AND PATENT 539-74 (2001). The TRIPS Agreement is also available at http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm (last visited Jan. 15, 2002)).

to trade secrets posed by the ubiquitous use of computer technology in the modern commercial environment.

I. TRADE SECRETS LAW – AN OVERVIEW

At its most basic level, trade secret law is a body of predominantly state law[16] that provides protection for valuable commercial information that is maintained in secrecy.[17] Typically, it allows legal redress against anyone who acquires or discloses such secret information in breach of a contractual agreement, in breach of a duty to maintain secrecy, or through improper actions.[18]

A. *Sources of Trade Secret Law*

(1) Common Law

Actions for misappropriation of trade secrets have their origins either in property law, contract law, or tort law depending upon the court and the particular facts of the case.[19] The Restatement (First) of Torts accurately summarizes the basic concepts embodied in common law trade secret law.[20] Typically, an action for misappropriation of a trade secret involves a party improperly disclosing or using a trade secret in violation of a contractual

16. Lars S. Smith, *Trade Secrets in Commercial Transactions and Bankruptcy*, 40 IDEA 549, 550 (2000).

17. *See* Smith v. Dravo Corp., 203 F.2d 369, 373 (7th Cir. 1953) (concluding that almost any secret knowledge or information used to conduct business can be a trade secret).

18. *See* UNIF. TRADE SECRETS ACT § 1, 14 U.L.A. 433, 438.

19. The Prefatory Note to the Uniform Trade Secrets Act notes that common law trade secret law has been based on a variety of theories including property, quasi-contract and breach of fiduciary relationships. *See* UNIF. TRADE SECRETS ACT, 14 U.L.A. 434, 435. *See also* ROBERT P. MERGES, PETER S. MENELL & MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 36 (2d ed. 2000) (noting both property and tort theories have been used to justify trade secret law).

20. *See* RESTATEMENT (FIRST) OF TORTS § 757, cmt. b (1939). It should be noted that trade secret law was omitted from the Restatement (Second) of Torts. However, trade secret law was included in the Restatement of Unfair Competition. *See* ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 1.01[1] at 1.20 (2001). *See also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 39-45 (1995).

agreement entered into between that party and the trade secret owner.[21] Alternatively, even in the absence of an agreement, acquiring a trade secret via improper means is actionable.[22] Typically, improper means includes illegal conduct and legal conduct deemed to be commercially unacceptable.[23] Despite the common law origins of trade secret law, a high degree of consistency existed among jurisdictions, at least with regard to the definition of a trade secret and the basic underlying concepts of trade secret law.[24] Nevertheless, some differences existed among states, for example with regard to statute of limitations and remedies. This prompted a movement to create a uniform body of law.[25]

2. Uniform Trade Secrets Act

The Uniform Trade Secrets Act (UTSA)[26] was promulgated by the National Conference of Commissioners on Uniform State Laws[27] in an attempt to create a uniform body of state trade secret law.[28] Arguably, creation of such a consistent body of law is critical in light of the importance of intellectual property assets to

21. *See generally* G. PETER ALBERT, JR., INTELLECTUAL PROPERTY LAW IN CYBERSPACE at 333 (1999).

22. *See id*. at 334; *see also* E.I. Dupont deNemours & Co. v. Christopher, 431 F.2d 1012, 1014-15 (5th Cir. 1970).

23. *See Christopher*, supra note 22, at 1015-17.

24. Prior to adoption of the Uniform Trade Secrets Act (*see infra* note 26), the Restatement (First) of Torts provided the uniformly recognized definition of a trade secret. *See* MILGRIM, *supra* note 21, § 1.01[1] at 1-4. However, other commentators have opined that prior to adoption of the UTSA common law trade secret law developed unevenly. *See* UNIF. TRADE SECRETS ACT, 14 U.L.A. 433.

25. *See* UNIF. TRADE SECRETS ACT , 14 U.L.A. 433. The prefatory notes to the UTSA note that it enunciates a single statute of limitations and codifies the results of some of the better reasoned cases with regard to remedies for misappropriation of a trade secret. *Id.* at 435.

26. UNIF. TRADE SECRETS ACT §§ 1-11, 14 U.L.A. 433; *see also* http://www.law.upenn.edu/bll/ulc/fnact99./1980s/utsa85.htm (last visited Feb. 28, 2002).

27. *See* Uniform Law Commissioners, *at* http: www.nccusl.org/nccusl/default.asp (last modified Feb. 19, 2002) (official web site for National Conference of Commissioners of Uniform State Laws).

28. *See* UNIF. TRADE SECRETS ACT § 8, 14 U.L.A. 433, 465. The UTSA codifies the basics concepts embodied in common law protection; additionally, like the common law it includes general concepts to be judicially applied. *See id*. at 434-35.

businesses that operate throughout the United States.[29] Inconsistencies in state intellectual property law increase state-to-state compliance costs. Additionally, they may threaten the continued existence of a trade secret that is utilized nationwide by a business enterprise. Unlike other types of intellectual property, all rights in a trade secret cease to exist once the trade secret is released to the public, since absent secrecy a trade secret does not exist.[30] In the area of patent and copyright law, for example, federal statutes preempt state law, thereby eliminating the possibility of inconsistent state laws in these areas.[31] Nevertheless, in the past, a patent could be treated differently in different federal circuits. For example, the Court of Appeals for the Fifth Circuit could find a patent valid, while the Eighth Circuit could find the same patent invalid.[32] Unless the Supreme Court agreed to hear an appeal, the inconsistent results would stand. Despite the obvious problems, patent rights would continue to be valid and enforceable in the

29. As businesses increasingly operate globally the need for consistent trade secret law worldwide has become important. The recent Agreement on Trade Related Aspects of Intellectual Property Rights (including Trade in Counterfeit Goods of the General Agreement on Tariffs and Trade) (commonly called the TRIPS Agreement) requires member countries to enact trade secret law that closely resembles United States trade secret law. *See* TRIPS Agreement (REPRINTED IN GOLDSTEIN, *supra* note 16, at 539-74) (The Agreement, which became effective on January 1, 1995, also covers copyrights, trademarks, geographical indications, industrial designs, patents and integrated circuits designs. *See* Sue Ann Mota, *Trips – Five Years of Disputes at the WTO*, 17 ARIZ. J. INT'L & COMP. LAW 533, 533 (2000). *See also* http://www.wto.org/english/tratop_e/trips_e/intel2_e.htm (last visited Mar. 1, 2001) (providing an overview of the TRIPS Agreement). *See* http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm (last visited Mar. 1, 2001) (providing the actual text of the agreement). The TRIPS Agreement, which is administered by the World Trade Organization, has been agreed to by 117 countries. *See* John A. Harrelson, *TRIPS, Pharmaceutical Patents, and the HIV/AIDS Crisis: Finding the Proper Balance between Intellectual Property Rights and Compassion*, 7 WIDENER L. SYM. J. 175, 176 (2001).

30. Metallurgical Indus., Inc. v. Fourtek, Inc., 790 F.2d 1195, 1199 (5th Cir. 1986).

31. 17 U.S.C. § 301 (2000) (federal copyright law preempts equivalent state laws); Sears, Roebuck & Co. v. Stiffel Co., 376 U.S. 225, 229 (1964) (federal patent law preempts state patent protection).

32. *See* Graham v. John Deere Co., 383 U.S. 1, 4 (1966) (appeal to Supreme Court to resolve disagreement between the Fifth Circuit, which held a patent valid, and the Eighth Circuit, which held the same patent invalid).

Fifth Circuit but not in the Eighth Circuit.[33] By contrast, failure to find something a trade secret in one jurisdiction creates the potential for public disclosure of the secret in that jurisdiction. Upon such disclosure the trade secret ceases to exist everywhere. Hence, the formulation of a uniform national trade secret law is imperative.[34]

To date, the UTSA has been adopted by forty-four jurisdictions.[35] Many jurisdictions, however, adopted the UTSA with some changes. Additionally, since the UTSA is state law, different states may interpret and apply the it differently.[36] Nevertheless, courts continue to rely on the Restatement (First) of Torts' definition of a trade secret as an interpretive guide, both in states that have adopted the UTSA and in the few states, such as Massachusetts, that have not adopted the UTSA.[37]

33. This problem was eliminated in the patent area when the Federal Courts Improvement Act of 1982 created the Court of Appeals for the Federal Circuit, which was vested with exclusive jurisdiction over all patent appeals from all district courts. PAUL GOLDSTEIN, COPYRIGHT, PATENT, TRADEMARK AND RELATED STATE DOCTRINES 383 (Rev. 4th ed. 1999).

34. Trade secrets law is one of the last areas of intellectual property that is not covered by a federal statute granting a private right of action to trade secret owners. Currently, federal statutes exist that provide private rights of action to protect patents (35 U.S.C. § 281), copyrights (17 U.S.C. §§ 101-22), and trademarks (15 U.S.C. §§ 1051-1129).

35. Nine jurisdictions adopted the original 1979 version of the UTSA. Those jurisdictions are Alaska, Arkansas, California, Connecticut, Illinois, Indiana, Louisiana, Rhode Island and Washington. Thirty-five other jurisdictions adopted the UTSA with the 1985 amendments. Those jurisdictions are Alabama, Arizona, Colorado, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Iowa, Kansas, Kentucky, Maine, Maryland, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Mexico, North Dakota, Ohio, Oklahoma, Oregon, South Carolina, South Dakota, Tennessee, Utah, Vermont, Virginia, West Virginia and Wisconsin. *See* Uniform Law Commissioners, *A Few Facts About . . . The Uniform Trade Secrets Act*, *at* http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-utsa.asp (last visited Mar. 1, 2002). *See also* UNIF. TRADE SECRETS ACT, 14 U.L.A. 177 (West Supp. 2001-2002).

36. *See generally* TRADE SECRETS: A STATE-BY-STATE SURVEY (Arnold H. Pedowitz & Robert W. Sikkel, eds. 1997) & Cum. Supp. (2000) (reviewing trade secret law on a state-by-state basis).

37. *See* MILGRIM, *supra* note 21, § 1.01[2] at 1-23. *See also* JERRY COHEN & ALAN S. GUTTERMAN, TRADE SECRETS PROTECTION AND EXPLOITATION 71-96 (1998) (discussing the differences in the trade secret definition under the

3. Federal Law

The Economic Espionage Act (the EEA) of 1996[38] creates a federal crime for theft of trade secrets.[39] The EEA provides for exclusive original jurisdiction in U.S. District Courts for civil actions brought under this act,[40] and expressly states that it does not preempt other remedies available under state or other federal statutes for misappropriation of a trade secret. [41] Therefore, although the EEA does not create a private cause of action, an injured party can still bring an action under state law without regard to whether a federal prosecution is undertaken by the government.

Unlike both state trade secret law and other federal intellectual property law, such as copyright and patent law, the EEA states that it has extraterritorial effect.[42] Conduct in a foreign country is within the domain of the Act if the offender is a citizen or permanent resident alien of the United States. [43] Additionally, foreign actions of organizations created under state, federal or local United States laws are subject to the Act.[44] Finally, the EEA encompasses foreign actions if any act in furtherance of the foreign action was

Restatement and the UTSA).

38. *See* Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488-90 (codified as amended at 18 U.S.C. §§ 1831-39 (2000)

39. The EEA also allows the federal government to bring a civil action under the Act seeking appropriate injunctive relief. *See id.* § 1836(a).

40. *See id.* § 1836(b).

41. *See id.* § 1838. *See generally* COHEN & GUTTERMAN, *supra* note 38, App. C at 483-85 (listing of other federal statutes relevant to protection of trade secrets).

42. *See* 18 U.S.C. § 1837. *See generally* Rochelle Cooper Dreyfuss, *Trade Secrets: How Well Should We Be Allowed to Hide Them? The Economic Espionage Act of 1996*, 9 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1, 26-29 (1998) (discussing briefly the potential issues that can arise from extraterritorial application of the EEA). *Cf.* Rotec Indus. v. Mitsubishi Corp., 215 F.3d 1246, 1258 (Fed. Cir. 2000) (Newman, J., concurring) (citing Deepsouth Packing Co. v. Laitram Corp., 406 U.S. 518, 531 n.16 (1972) for the proposition that U.S. patent law has no extraterritorial effect); Los Angeles News Serv. v. Reuters Television Int'l, 149 F.3d 987, 990 (9th Cir. 1998) (citing Subafilms, Ltd. v. MGM-Pathe Communications Co., 24 F.3d 1088, 1094 (9th Cir. 1994) (en banc) for support of the propostion that U.S. copyright law has no extraterritorial effect).

43. *See* 18 U.S.C. § 1837(1).

44. *Id.*

committed in the United States.[45]

To date, only a limited number of actions have been brought under this Act.[46] Nevertheless, the EEA appears to be aimed at providing greater protection from theft and subsequent use of proprietary information utilized in modern industry.[47] It reflects recognition that industrial espionage is a serious problem[48] that is engaged in both by competitors and foreign countries.[49] In light of this, the Act contains a specific section that prohibits certain actions that will benefit foreign governments, their instrumentalities, or their agents.[50] This section is aimed at intelligence efforts carried out by foreign governments.[51] Another section of the Act prohibits trade secret misappropriation by any party if that misappropriation will injure or economically benefit someone other than the owner.[52] The EEA defines "trade secret" in a manner similar to how it is defined under both the common law and the UTSA.[53] The EEA prohibits attempting to misappropriate[54]

45. *See id.* § 1837(2).

46. *See* James M. Fischer, *An Analysis of the Economic Espionage Act of 1996*, 25 SETON HALL LEGIS. J. 239, 266-70 (2001) (discussing cases prosecuted under Act).

47. *See* Fischer, *supra* note 46, at 240.

48. *See generally* George J. Moscarino & Michael R. Shumaker, *Changing Times, Changing Crimes: The Criminal's Newest Weapon and the U.S.'s Response,* 16 DICK. J. INT'L L. 597, 599-600 (1998) (noting that surveys indicate U.S. businesses lose billions of dollars annually due to trade secret theft and that such theft is on the rise).

49. *See* Fischer, *supra* note 46, at 245-47. Fischer notes that, in 1996, the FBI was involved in 800 investigations involving twenty-three countries that allegedly sponsored the misappropriation of proprietary information. *See id.* He also includes the comments of Dan Whiteman, corporate security officer for General Motors, whose statement "the number one way you lose [a company's proprietary information] is employees going over to another company" lends support to Fischer's statement that a source of competitor theft includes "instances in which high-ranking company executives leave a particular company for a competitor and take with them valuable proprietary information." *Id.* at 247-48 (citing Economic Espionage Act of 1996: Hearing on H.R. 3723 before the Subcommittee on Crime of the Committee on the Judiciary, 104th Cong. 46 (1996) (statement of Dan Whiteman, Corporate Information Security Officer, General Motors).

50. *See* 18 U.S.C. § 1831.

51. *See* Fischer, *supra* note 46, at 258.

52. *See id.* § 1832.

53. *See* Dreyfuss, *supra* note 43, at 9. Nevertheless, the definition is not

or conspiring to misappropriate[55] trade secrets. Additionally, anyone who knowingly receives, buys or possesses trade secrets with knowledge that they were obtained improperly violates the Act.
[56]

B. *Definition of a Trade Secret*

1. Common Law Definition

The most commonly accepted (and cited)[57] common law definition of a trade secret is contained in the Restatement (First) of Torts. It states, in pertinent part, that "[a] trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."[58]

2. Uniform Trade Secrets Act Definition

The UTSA defines "trade secret" as follows:

"Trade secret" means *information*, including a formula, pattern,

identical. *See* John R. Bauer & Joseph F. Savage, Jr.*, Criminalization of Trade Secret Theft: On the Second Anniversary of the Economic Espionage Act*, 8 CURRENTS: INT'L TRADE L.J. 59, 61 (1999) (discussing the differences between the definition of trade secret under the UTSA, the common law, and the EEA). *See also* 18 U.S.C. § 1839(3) (defining "trade" under the EEA); UNIF. TRADE SECRETS ACT § 1(4), 14 U.L.A. at 438 (defining "trade secret" under the UTSA); and RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939) (providing the common law definition of trade secret).

54. *See* 18 U.S.C. §§ 1831(a)(4), 1832(a)(4).

55. *See id.* §§ 1831(a)(5), 1832(a)(5).

56. *See id.* §§ 1831(a)(3), 1832(a)(3).

57. *See, e.g.*, Metallurgical Indus. Inc. v. Fourtek, Inc., 790 F.2d 1195, 1201 (5th Cir. 1986); Harvard Apparatus, Inc. v. Cowen, 130 F. Supp. 2d 161, 174 (D. Mass. 2001); Forest Labs., Inc. v. Formulations, Inc., 299 F. Supp. 202, 205 (E.D.Wis. 1969), *aff'd in part rev'd in part*, 452 F.2d 621 (7th Cir. 1971); Buckley v. Seymour, 679 So. 2d 220, 223 (Ala. 1996); Plastic & Metal Fabricators, Inc. v. Roy, 303 A.2d 725, 729 n.2 (Conn. 1972).

58. RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939). Coverage of trade secrets was subsequently removed from the Restatement (Second) of Torts. RESTATEMENT (SECOND) OF TORTS DIV. 9, CH. 36, GEN. MATLS (1979). It was then included in the Restatement (Third) of Unfair Competition, which defines a trade secret as follows: "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. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995).

compilation, program, device, method, technique, or process, that:

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

(ii) is the subject of efforts that are *reasonable* under the circumstances to maintain its *secrecy*.[59]

3. Federal Law Definition

The EEA defines "trade secret" as follows:

[T]he term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering *information*, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

(A) the owner thereof has taken *reasonable* measures to keep such information *secret*; and

(B) the information derives independent *economic value*, actual or potential, from not being generally known to, and not *being readily ascertainable through proper means* by, the public[.][60]

C. *Requirements for the Existence of a Trade Secret – Detailed Discussion*

1. Secrecy Requirement

As implied by the name of this body of law, "secrecy" is the most basic requirement that must be established before relying on trade secret law.[61] Absent secrecy a trade secret cannot exist.[62]

Even in the absence of trade secret law nothing would prevent

59. *See* UNIF. TRADE SECRETS ACT § 1(4), 14 U.L.A. at 438 (emphasis added).

60. *See* 18 U.S.C. § 1839(3) (emphasis added).

61. The subject matter of a trade secret must be secret. The RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

62. *See generally* COHEN & GUTTERMAN, *supra* note 37, at 14 (stating that secrecy is the most important factor in determining existence of trade secret).

someone from relying on absolute secrecy to maintain control over valuable technology or information. Such control, as a practical matter, gives the owner of the secret know-how or information the ability to reap economic rewards from its use. Nevertheless, it requires the trade secret owner to expend substantial money and effort to maintain secrecy. This is often problematic if the secret information must be shared with personnel in a business enterprise or a manufacturing facility who need access to and knowledge of the trade secret. Additionally, maximizing the value of a trade secret may require its transfer to third parties which increases the likelihood of destruction of the trade secret via public disclosure.

Arguably, contract law could, be used to maintain secrecy by requiring anyone with access to the trade secret to maintain it in confidence. These agreements, often called non-disclosure agreements, are commonly used to protect trade secrets and other confidential information. Nevertheless, under contract law the only damages typically available for a breach are monetary damages. In many cases, such "after the fact" damages may prove inadequate. Injunctive relief, especially preliminary injunctive relief, will often be the only desirable remedy. Injunctive relief, however, is generally considered an unusual remedy under contract law. Likewise, preliminary relief barring a subsequent breach of contract would also be a highly unusual contractual remedy. Finally, the use of contract law alone to protect secret information ignores the fact that trade secrets are important commercial assets that are essentially property utilized by a business enterprise for the purpose of achieving economic gain. Consequently, both common law and statutory trade secret actions typically reject an absolute secrecy requirement.[63]

A trade secret owner is required only to utilize reasonable efforts to maintain the secrecy of a trade secret.[64] This requirement, which

63. *See* Metallurgical Indus., Inc. v. Fourtek, Inc., 790 F.2d 1195, 1200 (5th Cir. 1986), *motion to reinstate appeals granted*, 771 F.2d 915 (5th Cir. 1985) (trade secret law does not require absolute secrecy).

64. *See* USM Corp. v. Marson Fastener Corp., 393 N.E.2d 895, 902 (Mass. 1979), *aff'd in part, vacated in part* 467 N.E.2d 1271 (Mass. 1984) (at common law only reasonable, rather than heroic, actions required to maintain secrecy of trade secret).

is part of the common law, is codified in the UTSA. It states that a trade secret must be "the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[65] Arguably, requiring only reasonable secrecy efforts may facilitate misappropriation of trade secrets by employees, competitors, or other third parties. In contrast, requiring absolute secrecy would minimize the likelihood of such misappropriation. Nevertheless, the mere possibility of pursuing a trade secret misappropriation action acts as a disincentive to misappropriation. Likewise, requiring only reasonable secrecy efforts reflects the view that trade secrets are property. Therefore, a trade secret can be disclosed to third parties, such as employees, customers, or potential investors, in order to maximize the revenue that can be generated from the trade secret.[66] This is consistent with the view that a trade secret is property since one of the basic rights that attaches to property is the right of the owner to transfer her property.

Reasonableness, a common legal test, is easy to state but often hard to establish.[67] As in other areas of the law, courts look to objective tests to determine reasonableness. The following are often relevant in determining if reasonable efforts to maintain secrecy were engaged in:

• *Did the trade secret owner have an adequate protection program to insure secrecy?* - Courts often focus on the totality of the program and how it relates to the know- how or information being protected. Therefore, it is important to adopt a combination

65. UNIF. TRADE SECRETS ACT § 1(4)(ii), 14 U.L.A. at 438. As a practical matter, a trade secret owner may still expend considerable effort and expense protecting her trade secret. Such actions will often exceed the reasonable secrecy requirement because the goal of a business enterprise is to avoid disclosure and subsequent loss of the trade secret rather than being concerned with the minimum actions needed to prevail in a trade secret misappropriation law suit after destruction of the trade secret due to disclosure.

66. Of course, such disclosures must be in confidence to prevent public disclosure of the trade secret which destroys it. *See, e.g., Metallurgical Indus*., 790 F.2d at 1200 (permitting limited confidential disclosure of trade secret to third parties to further economic gain from that secret).

67. *See In re* Innovative Constr. Sys., Inc., 793 F.2d 875, 884 (7th Cir. 1986) (determining reasonable efforts to maintain secrecy of trade secret depends upon the surrounding facts and circumstances in a specific business).

of measures designed to maintain secrecy.

• *Did the trade secret owner comply with standard industry practice?* - Different security precautions are utilized in different industries. Therefore, whether such standard practices were followed or ignored may be relevant to a determination of whether a trade secret owner acted reasonably. This is analogous to determining reasonableness in a negligence action for product liability or medical malpractice where the actions involved are often measured against the customary standard or practice in the particular industry or field of endeavor.[68]

• *Did the trade secret owner invest adequate resources to insure secrecy*? - The amount of expenditures by the trade secret owner is relevant. This, however, cannot be analyzed in a vacuum. The relative value of the trade secret should also be considered. For example, it might be considered extraordinary to expect a company to invest a million dollars in a security program for a trade secret. If the trade secret, however, has a commercial value of hundreds of millions of dollars such an expenditure may be reasonable. In contrast, if the commercial value of the trade secret is $300,000, it would be an extraordinary amount to spend.

• *Did the trade secret owner advise employees and others that a trade secret existed?*

• *Did the trade secret owner limit knowledge of the trade secret on a need-to-know basis?* - Depending on the trade secret, disclosure to all employees may not be necessary. Additionally, only partial disclosure may be adequate in some cases. In contrast, disclosing to employees or third parties who do not have a need to know the information is potentially problematic. Therefore, only necessary disclosures should be made.

• *Did the trade secret owner limit access to any facility where the trade secret is used?* - Typically, some form of physical security measures should be utilized to protect a trade secret. Of course, these can vary from locking the information in a file cabinet to having the information in a locked room protected by armed

68. *See generally* Jacques v. First Nat'l Bank of Md., 515 A.2d 756,764 (Md. 1986) (noting that the industry standard may be evidence of the requisite standard of care in negligence action).

guards. What is necessary depends upon the value of the trade secret, among other things.

• *Did the trade secret owner use confidential legends or other labels on documents and other materials which contain information about a trade secret?*

• *Did the trade secret owner require employees and third parties to sign non-disclosure agreements prior to disclosing the trade secret to them?* - This is a common practice in most businesses that utilize trade secrets. Standardized agreements are commonly available, so this is an important, but relatively easy, matter to accomplish.

2. Readily Ascertainable Requirement

If something is generally known either by the public or by competitors it lacks the requisite secrecy to be a trade secret. Nevertheless, although some things may be secret, the amount of effort necessary to ascertain the secret information, via reverse engineering[69] or some other proper means, may be minimal. In such cases, the information will not qualify as a trade secret.[70] This requirement is embodied in the UTSA.[71] It states that a trade secret cannot exist if it is "readily ascertainable by proper means."[72] Determining whether information is readily ascertainable and therefore not a trade secret, or sufficiently difficult to obtain such that the information is a trade secret, is a difficult distinction to make. Some objective factors that can be considered in making this determination are:

• *Amount of time necessary to reverse engineer the secret*

69. For a discussion of reverse engineering, s*ee infra* note 87 & accompanying text.

70. *See generally* Wesley-Jessen Inc. v. Reynolds, 182 U.S.P.Q. 135, 144-47 (N.D. Ill. 1974) (under common law no right to claim trade secret exists if product embodying secret is freely sold to public so that it can be easily reverse engineered).

71. UNIF. TRADE SECRETS ACT § 1(4)(i), 14 U.L.A. at 438.

72. *Id. See also supra* note 59 & accompanying text (EEA trade secret definition includes readily ascertainable requirement). In evaluating whether a trade secret existed at common law, consideration of an analogous issue is a factor. *See infra* note 86 & accompanying text (sixth factor considered at common law with regard to existence of trade secret analogous to UTSA readily ascertainable requirement).

information.[73]

• *Amount of effort necessary to reverse engineer the secret information.*

• *Cost of reverse engineering the secret information.*[74]

• *Novelty of the secret information* - Although novelty is not a requirement for something to be a trade secret the fact that the information is novel or unique creates at least an inference that it is worthy of trade secret protection.

• *Secrecy precautions used to protect the secret information* - The existence of substantial secrecy precautions can provide at least inferential evidence that the trade secret must have been acquired by improper means.

• *Unsuccessful attempts by third parties to duplicate the secret information* - If others have experienced difficulty in duplicating the secret information, this suggests that the information is not readily ascertainable. Therefore, the more unsuccessful attempts to duplicate it the less likely it is readily ascertainable.

• *Willingness of third parties to pay for a license to use the secret information* - Third parties willing to pay for a license to use the secret information suggests that it is not readily ascertainable since it is unlikely someone would pay for something he or she could easily obtain for free. Additionally, the more a licensee is willing to pay the less likely the information can be considered readily ascertainable.

3. Business Use Requirement

The Restatement (First) of Torts definition of a trade secret expressly states that a trade secret must be "used in one's business."[75] Additionally, it states that "[a] trade secret is a process

73. *See generally* Technicon Data Systems Corp. v. Curtis 1000, Inc., 224 U.S.P.Q. 286, 289-90 (Del. Ch. 1984) (finding that considerable time spent on reverse engineering indicates secret information not readily ascertainable).

74. *See, e.g.,* Unistar Corp. v. Child, 415 So. 2d 733, 734 (Fla. Dist. App. Ct. 1982) (finding that a list of dealers is a trade secret due in part to the fact that $800,000 was spent to compile the list).

75. RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939). *See supra* text accompanying note 57. *Contra* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995) (stating that "[a] trade secret is any information that *can be used* in the operation of a business" rather than stating it must be used) (emphasis added).

or device for continuous use in the operation of the business."[76] This requirement prevents certain things, such as negative information, from being a trade secret.[77] For example, a researcher might have learned from her experiments that the general avenue of research being pursued in the field is a dead-end. This knowledge is very valuable to the researcher because it allows her to avoid wasting her time and energy by pursuing a dead-end unlike her competitors who are unaware of the futility of their research. Additionally, a trade secret owner may not be making any use of her secret knowledge because she lacks adequate capital to manufacture or market any resulting product based on the trade secret. The Restatement definition would bar this secret information from qualifying as a trade secret.

At common law, some judicial decisions followed this "business use" requirement; however, other decisions rejected it.[78] The UTSA clearly rejects this requirement by omitting any reference to the requirement that a trade secret be used in one's business.[79] Likewise, the EEA is consistent with the UTSA by not requiring any actual use to qualify as a trade secret.[80]

4. Economic Value Requirement

At common law, a trade secret must provide the trade secret owner with a competitive advantage[81] because it is that competitive

76. RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

77. *See* COHEN & GUTTERMAN, *supra* note 37, at 72. At common law, unlike under the UTSA, the case law is unsettled with regard to whether negative information is a trade secret. *See id.* at n.12. *Contra* UNIF. TRADE SECRETS ACT § 1 official cmt., 14 U.L.A. at 439 (noting that negative information can be trade secret).

78. *See* Syntex Ophthalmics, Inc. v. Tsuetaki, 701 F.2d 677, 682-83 (7th Cir. 1983) (noting some early cases required use under common law but current common law focuses on whether trade secret has value to the owner rather than whether it was actually used); *see also* COHEN & GUTTERMAN, *supra* note 37, at 94.

79. *See supra* note 59 & accompanying text for UTSA definition of a trade secret. *See* UNIF. TRADE SECRETS ACT § 1 official cmt., 14 U.L.A. at 439. *See also* COHEN & GUTTERMAN, *supra* note 37, at 72.

80. *See supra* note 59 & accompanying text for the EEA definition of a trade secret.

81. Cherne Indus., Inc. v. Grounds & Assocs., Inc., 278 N.W.2d 81, 90 (Minn. 1979).

advantage that makes the trade secret valuable.[82] In contrast, the UTSA requires that a trade secret have "independent economic value."[83] Nevertheless, this UTSA requirement has been interpreted to codify the common law competitive advantage requirement.[84] Additionally, the UTSA expressly states that the economic value can be either "actual or potential."[85] The elimination of the business use requirement (discussed above) coupled with retention of the economic value requirement means that, under the UTSA, the determination of whether information can qualify as a trade secret focuses on the value of the secret information rather than on whether it is actually being used or on how it is being used.

5. Objective Factors Used to Determine Existence of a Trade Secret

The Restatement (First) of Torts contains six factors to be evaluated for determining whether information or know-how is a trade secret.[86] These factors, listed below, are frequently quoted and relied on by judicial decisions that determine the existence of a trade secret under both the common law[87] and under the UTSA:[88]

[T]he extent to which the information is known outside of [the] business;

[T]he extent to which it is known by employees and others involved in the business;

[T]he extent of measures taken . . . to guard the secrecy of the information;

[T]he value of the information to the business and to . . .

82. Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1011 n.15, 104 S. Ct. 2862, (1984).

83. *See* UNIF. TRADE SECRETS ACT § 1(4)(i), 14 U.L.A. at 438. The EEA also incorporates the requirement that a trade secret must have independent economic value. *See* 18 U.S.C. § 1839(3). *See also supra* note 60 and accompanying text..

84. *See* COHEN & GUTTERMAN, *supra* note 37, at 95.

85. *See* UNIF. TRADE SECRETS ACT § 1(4)(i), 14 U.L.A. at 438.

86. RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

87. *See, e.g.*, Jet Spray Cooler, Inc. v. Crampton, 282 N.E.2d 921, 925 (Mass. 1972) (quoting and applying the six Restatement factors to evaluate existence of trade secret under common law).

88. *See, e.g.,* Basic Am., Inc. v. Shatila, 992 P.2d 175, 184 (Idaho 1999) (quoting and applying the six Restatement factors to evaluate existence of trade secret under UTSA).

competitors;

[T]he amount of effort or money expended . . . in developing the information;

[T]he ease or difficulty with which the information could be properly acquired or duplicated by others.[89]

D. *Limitations on Trade Secret Rights*

1. Reverse Engineering

"Reverse engineering is the process of starting with a finished product and working backwards to analyze how the product operates or how it was made."[90] The possessor of the product, by virtue of being the owner of the product, is free to do what she wants with the product. This can include reverse engineering it. Trade secret law, in this regard, is different than copyright or patent law.[91] An item that contains copyrighted or patented aspects consists of two distinct property interests.[92] For example, if a person buys a book protected by copyright, that person becomes the owner of the book. The owner of the book is free to sell or destroy the book.[93] However, the book also contains intangible property rights protected by copyright law. These property rights were not conveyed to the book owner when she purchased the book. Therefore, she is not free to makes copies of the book, for example, because that would infringe the copyright rights in the book. The right to copy a copyrighted work is one of the rights embodied in the intangible property interest created by

89. RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

90. Secure Serv. Tech., Inc. v. Time and Space Processing, Inc., 722 F. Supp. 1354, 1361 n.16 (E.D. Va. 1989). The U.S. Supreme Court has defined reverse engineering as "starting with the known product and working backward to divine the process which aided in its development or manufacture." Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974). *See also* Andrew Johnson-Laird, *Software Reverse Engineering in the Real World*, 19 U. DAYTON L. REV. 843, 846 (1994) (discussing reverse engineering of software).

91. *See* Junker v. Plummer, 67 N.E. 2d 667, 670 (Mass. 1946) (stating that trade secret owner cannot exclude third parties who acquired trade secret via legitimate means from using it unlike patent owner who has exclusive right to bar all third party use).

92. *See* 17 U.S.C. § 202 (2000).

93. *See id.* § 109(a) (commonly called the first sale doctrine).

copyright law.[94] Additionally, a person that buys a patented machine, as the owner, is free to utilize the machine for its intended purpose. That same owner, however, is not free to duplicate the machine because that would infringe the property interests of the patent owner, which includes the exclusive right to reproduce the patented machine.[95] In contrast, trade secret law only protects a trade secret so long as it remains a secret. Therefore, once a third party is allowed to acquire a copy of a product embodying the trade secret, that party is free to engage in reverse engineering.

Two restrictions, however, do exist on the right of a third party to engage in reverse engineering. First, if the product to be reverse engineered was acquired improperly, the mere acquisition of the product may be misappropriation of a trade secret.[96] Therefore, no right to engage in reverse engineering would exist. Second, the extent of the interest conveyed in the product to be reverse engineered must be ascertained. If the trade secret owner merely licensed[97] a third party to use the product for a specific purpose, the third party may have only a very limited property interest in the product.[98] Additionally, the trade secret owner and the third party may have contractually agreed that the third party may not engage in any reverse engineering of the product. In such a case, reverse engineering by the third party may amount to misappropriation of the trade secret.

2. Independent Development

A trade secret owner cannot bring a misappropriation action against another party who uses or discloses the trade secret if that

94. *See id.* § 106(1).

95. *See* 35 U.S.C. § 271(a) (1994).

96. *See* COHEN & GUTTERMAN, *supra* note 37, at 205.

97. "A license is a contract in which the owner of the trade secret or other intellectual property permits another party (the 'licensee') to use the intellectual property without liability, generally in return for payment." MARGRETH BARRETT, INTELLECTUAL PROPERTY 45 (1995). *See generally* COHEN & GUTTERMAN, *supra* note 37, at 253 – 311 (giving a detailed examination of trade secret licensing).

98. For example, software is often licensed rather than sold, so that the owner of the copyright interest in the software can restrict what the software purchaser can do with the software. Often such licenses prohibit the buyer from duplicating, reverse engineering, decompiling or modifying the software, or installing it on more than one computer. *See generally* BARRETT, *supra* note 97.

other party independently developed the trade secret information.[99] This is logical under a property theory because the other party did not take the property from the trade secret owner. Rather, her independent development makes the trade secret her property since it was the result of her personal intellectual activity. Likewise, this result is justifiable under a tort theory because the other party has not engaged in commercially unacceptable conduct with regard to acquiring the trade secret. Rather, the other party has engaged in socially desirable conduct by independently developing useful technology. The law encourages such development activities because it facilitates competition, which is desirable in a free market economic system.

3. The Effect of Reverse Engineering and Independent Development on a Trade Secret

Reverse engineering or independent development by a third party, although not actionable by a trade secret owner, does not automatically destroy the trade secret.[100] The effect on the trade secret depends upon what the third party does once they have discovered the trade secret.[101] If they publicly disclose the trade secret, it ceases to exist since a trade secret cannot exist in the absence of secrecy. In contrast, if the third party maintains the secrecy of the information acquired via reverse engineering or independent development, it will continue to be a trade secret.[102] In such a situation, it is possible for multiple parties to independently possess a trade secret provided they all maintain it as a secret and it continues to be unknown generally to others in the same business or industry.[103]

4. First Amendment Restrictions

Any litigation involving a trade secret is inherently risky because the very nature of a trade secret requires secrecy to prevent

99. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974) (stating that trade secret law does not protect against independent invention or reverse engineering).

100. COHEN & GUTTERMAN, *supra* note 37, at 207.

101. *Id.*

102. *Id.*

103. *See generally* UNIF. TRADE SECRETS ACT § 1 cmt., 14 U.L.A. at 438-39.

destruction of the trade secret.[104] Nevertheless, judicial proceedings are typically open to the public and the media to ensure fairness and to protect the rights of the litigants. To avoid the obvious public disclosure of a trade secret in such proceedings, courts will often hold *in camera* proceedings and seal court documents.[105] This issue is specifically addressed by the UTSA, which permits a court to utilize "reasonable means" to preserve secrecy.[106] Nevertheless, an alleged trade secret misappropriator may wish to publicly reveal the trade secret prior to trial. Such action may destroy the trade secret in the event a determination is made after a trial on the merits that the trade secret had been taken improperly. However, prior to the trial on the merits, it is unknown if the know-how or information involved is a trade secret. Additionally, even if it is a trade secret, it is unknown prior to the trial if it was taken or used improperly. Numerous factual determinations, which can only be resolved by an adjudication on the merits, must be ascertained before a determination can be made that misappropriation has occurred. To deal with this problem, the trade secret owner can seek a preliminary injunction barring disclosure of the trade secret.[107] Upon a proper showing, injunctive relief is typically allowed since without such relief public disclosure causes the trade secret to cease to exist.[108] In such a case, the only remedy available would be for damages, but such damages

104. FMC Corp. v. Taiwan Tainan Giant Indus. Co., 730 F.2d 61, 63 (2d Cir. 1984) ("A trade secret once lost is, of course, lost forever.").

105. UNIF. TRADE SECRETS ACT § 5 (1985), 14 U.L.A. at 461.

106. *Id.* at 438.

107. Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147, 229 (1998) (stating that preliminary injunctive relief is a common remedy to protect trade secrets). In some cases, an ex parte temporary restraining order is initially sought to prevent destruction of the trade secret due to disclosure.

108. The four factor test for a preliminary injunction requires plaintiff to establish: (1) likelihood of success on the merits; (2) irreparable harm or injury will result if injunction denied; (3) balance of hardships favors plaintiff; and (4) public interest favors granting injunction. Nalco Chemical Co. v. Hydro Techs., Inc., 984 F.2d 801, 802 (7th Cir. 1993). *See generally* COHEN & GUTTERMAN, *supra* note 37 at 215-18 (discussing preliminary injunctive relief in trade secret cases).

will often be hard to ascertain.[109] Therefore, injunctive relief to preserve the trade secret may often be preferred to obtaining damages.[110] Some commentators have asserted that such preliminary injunctive relief amounts to a prior restraint in violation of the First Amendment right to freedom of speech.[111] Most courts have rejected this argument.[112] Nevertheless, a recent federal court decision accepted this argument.[113] In this decision, the court refused to grant a preliminary injunction prohibiting the defendant from releasing plaintiff's trade secrets on the Internet.[114] The court found that the plaintiff had "presented substantial evidence to support its claim that [the defendant] violated the

109. COHEN & GUTTERMAN, supra note 37, at 214-15.

110. *Id.* at 214.

111. Lemley & Volokh, *supra* note 107, at 230-32.

112. Preliminary relief is usually granted to protect trade secrets from disclosure. *See, e.g.*, Pepsico, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995) (granting preliminary injunction prohibiting former PepsiCo employee from working for competitor for a fixed time period in order to prevent inevitable disclosure of PepsiCo trade secrets to competitor). *See also* Standard & Poor's Corp., Inc. v. Commodity Exch., Inc., 541 F. Supp. 1273, 1275 (S.D.N.Y. 1982) ("[I]nterference with access to business confidences and trade secrets is not an abridgement of the freedom of speech and of the press protected by the First Amendment"). *See generally* 3 MILGRIM, *supra* note 21, § 14.01[2][a], at 14-26 n.15 ("[T]here is a long line of authority upholding content neutral injunctions to protect intellectual property and that such injunctive relief is *not* an impermissible prior restraint.").

113. *See* Ford Motor Co. v. Lane, 67 F. Supp. 2d 745 (E.D. Mich. 1999).

114. The defendant in *Ford Motor Co. v. Lane*, Robert Lane, operates a web site on the Internet, called *Blue Oval News - The Independent Voice of the Ford Community Since 1998* (*see* http://www.blueovalnews.com (last visited October 15, 2001)), where he posts information about the Ford Motor Company. This web site also contains a review of the lawsuit by Mr. Lane and newspaper and other articles about the lawsuit. *See* http://www.bonforums.com/legal/ford_lawsuitmain.htm (last visited Mar. 26, 2002). In State *ex rel.* Sports Mgmt. News, Inc. v. Nachtigal, 921 P.2d 1304 (Or. 1996), where the Oregon Supreme Court held that a newsletter publisher could not be barred from publishing trade secrets it lawfully obtained prior to a trial on the merits. Any preliminary relief was held to be a prior restraint in violation of the state constitution because it was based on the content of the speech involved. *Id.* at 1307-09. The court noted that the appropriate remedy was injunctive relief or damages after a trial on the merits. *Id.* at 1309. Nevertheless, the court noted that it was not deciding if the First Amendment would require the same result. *Id.* at 1307 n.6.

Michigan Uniform Trade Secrets Act."[115] Despite such findings, the court refused to grant a preliminary injunction because it concluded it would be an invalid prior restraint of speech in violation of the First Amendment.[116]

5. Governmental Action

In light of the fact that trade secrets are generally treated as property, the government, arguably, has the right to take such property for public use. The only limitation is found in the Fifth Amendment, which would require the government to pay the value of the trade secret to its former owner.

Nevertheless, a recent federal decision held that a Massachusetts law which required cigarette makers to disclose the various additives—which arguably were trade secrets—used in each brand of cigarettes was not a taking under the Fifth Amendment.[117] The information was required by the state for public health purposes, and would become public information unless the cigarette makers opted not to do business in Massachusetts.[118]

E. *Trade Secret Misappropriation Actions*

Trade secrets are important commercial assets that are essentially property utilized by a business enterprise for the purpose of achieving economic gain. Consequently, as with other types of property, there must be legal protection which allows the trade secret owner to control access to, and use of, her trade secret. However, unlike real property and tangible personal property, trade secrets, like other intellectual property, can be possessed and used by multiple parties simultaneously. Such use may even occur without each user being aware of or directly affected by other users. Additionally, independent development and reverse

115. *Ford Motor Co.*, 67 F. Supp. 2d at 746.

116. *Id.* at 750. *But see* Bartnicki v. Vopper, 532 U.S. 514, 535 (2001). In *Bartnicki*, the Court suggests, in dicta, that trade secrets are private matters that are less likely to trigger First Amendment concerns than information of general interest to the public. *Id.* at 533. *See also* 3 MILGRIM, *supra* note 2, § 14.01[2][a], at 14-26.1 n.15 (criticizing the result in *Ford Motor Co.*).

117. *See* Philip Morris, Inc. v. Reilly, 267 F.3d 45 (1st Cir. 2001), *withdrawn*, *available at* 2001 U.S. App. LEXIS 22348 (1st Cir. Oct. 16, 2001).

118. *Id.*

engineering, discussed above, are defenses to a trade secret misappropriation action. In light of this, trade secret misappropriation actions focus on how a third party learned of or came into possession of the trade secret at issue. An action for misappropriation of a trade secret is essentially a tort action for the unauthorized or improper taking of property (in the form of a trade secret) from the trade secret owner.

A trade secret misappropriation action typically consists of two elements:

(a) The existence of a trade secret must be established; *and*

(b) The conduct engaged in by a third party who acquire the trade secret must be objectionable conduct that is either a breach of an agreement or other obligation to maintain the confidentiality of the trade secret; *or* the trade secret was obtained by conduct deemed to be improper.[119]

1. Conduct Requirement - Contractually Based Actions

Although trade secret misappropriation is a tort action, the obligation of a third party to maintain the secrecy of the trade secret can arise from a contract.[120] Typically, this occurs in one of two situations. First, an employee is bound by a non-disclosure agreement under which the employee contractually agrees to maintain the secrecy of the employer's confidential information. Disclosure of the information by the employee in breach of the agreement makes the employee liable in a trade secret misappropriation action. Such non-disclosure agreements normally must be express agreements but, in appropriate situations, a contractual agreement can be implied.

The second situation involves disclosure of a trade secret by the owner to a licensee. For example, a trade secret owner may generate revenue from licensing third parties to use the trade secret in their businesses. Such disclosures must be made pursuant to a non-disclosure agreement which provides that the licensee will

119. North Atlantic Instruments, Inc. v. Haber, 188 F.3d 38, 43-44 (2d Cir. 1999) (*citing* Hudson Hotels Corp. v. Choice Hotels Int'l, 995 F.2d 1173, 1175 (2nd. Cir. 1993); *see also* UNIF. TRADE SECRETS ACT § 1, 14 U.L.A. at 438.

120. This is codified in the UTSA. It prohibits disclosure of trade secrets via improper means, which are defined to include, among other things, breach of a duty to maintain secrecy. *See* UNIF. TRADE SECRETS ACT § 1(1), 14 U.L.A. at 437.

maintain secrecy. If the third party breaches the agreement by allowing an unauthorized party to have access to the trade secret, the licensee is liable for trade secret misappropriation.

2. Conduct Requirement—Improper Conduct

A third party can be liable for misappropriation of a trade secret even in the absence of any contractual or other relationship with the trade secret owner. Such actions focus on the conduct of the third party. Conduct that results in trade secret misappropriation is typically referred to as *improper conduct.*[121] Clearly, improper conduct includes illegal conduct, such as trespass, theft or bribery, with the intent to acquire a trade secret.[122] Additionally, otherwise legal conduct used to acquire a trade secret may be considered actionable improper conduct if it was used to acquire a competitor's trade secret, provided the trade secret owner utilized reasonable measures to maintain its secrecy.[123] Arguably, this type of trade secret misappropriation action is grounded in tort because it prohibits otherwise legal conduct on the basis of the conduct exceeding the bounds of commercial reasonableness. In this regard, the trade secret law recognizes that some conduct, even if legal, may go beyond the bounds of acceptable competition and render a party liable for misappropriation of a trade secret.[124] The

121. The UTSA defines improper conduct to include "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means." *Id.*

122. *Id*.

123. *Id.* § 1, cmt., 14 U.L.A. at 438-39. *See, e.g.,* E.I. DuPont de Nemours & Co. v. Christopher, 431 F.2d 1012 (5th Cir. 1970), *cert. denied*, 400 U.S. 1024 (1970) (stating that under the common law aerial overflight of construction site to acquire layout of facility for reverse engineering of process is actionable improper conduct when trade secret owner had utilized reasonable measures to maintain secrecy). Under the UTSA, the result in *Christopher* would likely be the same because the conduct would be considered "espionage" which is defined as improper conduct by the Act. *See* UNIF. TRADE SECRETS ACT § 1 & cmt., 14 U.L.A. at 437-39. *See also* Tennant Co. v. Advance Mach. Co., 355 N.W.2d 720 (Minn. Ct. App. 1984) (finding the third party liable for $500,000 for trade secret misappropriation for obtaining trade secrets by rummaging through trade secret owner's garbage).

124. In *Christopher*, 431 F. 2d at 1016, the court states "our devotion to free wheeling industrial competition must not force us into accepting the law of the jungle as the standard of morality expected in our commercial relations". *See generally Kewanee Oil Co.*, 416 U.S. at 487. In addition to the increased costs for

UTSA broadly defines improper conduct: "'[i]mproper means' includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means."[125]

3. Actions Based on Special Relationships

The law commonly creates obligations that arise merely from the existence of certain relationships. For example, partners owe a fiduciary duty to one another based simply on the existence of the partnership relationship. Additionally, corporate directors owe a fiduciary obligation to the corporation based on their status as directors. Likewise, disclosure of a trade secret to employees, business partners, customers and licensees may create an obligation to maintain the information in confidence.[126] Depending on the

protection from burglary, wiretapping, bribery, and the other means used to misappropriate trade secrets, there is the inevitable cost to the basic decency of society when one firm steals from another. A most fundamental human right, that of privacy, is threatened when industrial espionage is condoned or is made profitable; the state interest in denying profit to such illegal ventures is unchallengeable.

125. UNIF. TRADE SECRETS ACT § 1(1). Comment f of section 757 of the Restatement (First) of Torts states the following with regard to improper conduct under the common law:

"The discovery of another's trade secret by improper means subjects the actor to liability independently of the harm to the interest in the secret. Thus, if one uses physical force to take a secret formula from another's pocket, or breaks into another's office to steal the formula, his conduct is wrongful and subjects him to liability apart from the rule stated in this Section. Such conduct is also an improper means of procuring the secret under this rule. But means may be improper under this rule even though they do not cause any other harm than that to the interest in the trade secret. Examples of such means are fraudulent misrepresentations to induce disclosure, tapping of telephone wires, eavesdropping or other espionage. A complete catalogue of improper means is not possible. In general they are means which fall below the generally accepted standards of commercial morality and reasonable conduct."

Christopher, 431 F.2d at 1017 (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. f (1939)). Section 43 of the Restatement (Third) of Unfair Competition states that improper means "includes 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." RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 (1995).

126. *See* Barrett, *supra* note 97, at 44 (1995). *See generally* Maxwell Alarm Screen Mfg. Co. v. Protective Serv. Corp., 218 U.S.P.Q. 580 (C.D.Ca. 1982) (confidential relationship requiring protection of trade secret can exist even in the

facts, this obligation may arise out of an implied contract.[127] Or, the existence of fiduciary obligations based on the relationship of the parties may require the confidentiality of the trade secret to be protected without regard to whether a non-disclosure agreement exits.[128] In either case, the recipient of the trade secret typically must have notice that the information disclosed by the trade secret owner is, in fact, a trade secret.[129]

4. Equity Based Actions Against Third Parties

The previous sections dealt with culpable parties who either disclosed a trade secret in breach of a non-disclosure obligation, or who utilized improper means to acquire a trade secret. It is also possible for an innocent third party to learn of a trade secret either inadvertently or accidentally. Additionally, an individual who misappropriates a trade secret may pass it on to an innocent third party. Under certain circumstances, the innocent third party may be able to use the trade secret without liability; but under other circumstances, such use is legally impermissible. The rules governing such situations embody some basic equity doctrines found in the law. For example, innocent use, or the use of a trade secret without knowledge that the information is a trade secret, is typically not actionable. The third party would be liable once she is notice that she has a trade secret. The common law governing such situations is codified in the Restatement (First) of Torts, as discussed below. Likewise, the UTSA also codifies rules for such situations.

a. Common Law

At common law, the Restatement (First) of Torts states the following with regard to third party liability:

One who learns another's trade secret from a third party

absence of express agreement to preserve secrecy). *See also* Ruesch v. Ruesch Int'l Monetary Serv., Inc., 479 A.2d 295, 296-97 (D.C. App. Ct. 1984) (finding that agent has duty to keep principal's trade secrets confidential based on agency law).

127. *See* Barrett*, supra* note 97.

128. *See id*. *See also* Affiliated Hosp. Prods., Inc. v. Baldwin, 373 N.E.2d 1000, 1006 (Ill. App. 1978) (concluding that obligation to maintain trade secret in confidence can arise from fiduciary relationship absent express contract).

129. *See* Barrett, *supra* note 97.

without notice that it is secret and that the third person's disclosure is a breach of his duty to the other, or who learns the secret through a mistake without notice of the secrecy and the mistake,

is not liable to the other for a disclosure or use of the secret prior to receipt of such notice, and

is liable to the other for a disclosure or use of the secret after the receipt of such notice, unless prior thereto he has in good faith paid value for the secret or has so changed his position that to subject him to liability would be inequitable. [130]

This Restatement section establishes the basic equitable idea that a third party who comes into possession of a trade secret without any knowledge that it is a trade secret may not be liable for using it.[131] Liability can only arise once the third party is aware she is using a trade secret.[132] However, such knowledge alone does not automatically make the third party liable; she must also be aware that the disclosure of the trade secret was in breach of a contractual or other obligation barring such disclosure. Arguably, both of these requirements make sense from an equitable viewpoint. If a third party learns some particular information, she should be free to utilize it without liability if she does not know it is a trade secret. This is consistent with the common law view that ideas and information are generally considered to be in the public domain absent some specific legal restrictions that arise due to statutory laws such as patent or copyright laws.[133]

Additionally, even if a third party knows she has received a trade secret, she may reasonably believe the party providing the trade secret had the right to transfer it. This is consistent with the idea that trade secrets are property, and, therefore, can be transferred

130. RESTATEMENT (FIRST) OF TORTS § 758 (1939). *See generally* Forest Labs, Inc. v. Pillsbury Co., 452 F.2d 621, 626 (7th Cir. 1971) (applying § 758 to find a corporation liable for trade secret misappropriation once the corporation received actual knowledge that it had acquired trade secret belonging to another party).

131. *See generally Forest Labs*. at 623 n.1 (7th Cir. 1971) (dismissing defendant from trade secret misappropriation case because it did not have notice that the method it utilized was a trade secret).

132. *See* RESTATEMENT (FIRST) OF TORTS § 758(a).

133. *See* Sears, Roebuck & Co. v. Stiffel Co., 376 U.S. 225 (1964); *see also* Compco Corp. v. Day-Brite Lighting, Inc., 376 U.S. 234 (1964).

just like other commercial assets.[134] Consequently, liability will typically only arise if the third party acquires information she knows is a trade secret that has been disclosed in violation of some obligation not to reveal it or was acquired via improper means.

The Restatement also embodies two exceptions that may allow a third party to use a trade secret without liability despite its being improperly obtained. First, if an innocent third party has paid value in good faith for a secret prior to learning it was acquired improperly, she may be entitled to continue using it without liability.[135] Arguably, this is merely application of the familiar bona fide purchaser doctrine, which is commonly utilized in property law.

Second, if the innocent third party changes her position, prior to learning that she has obtained a trade secret that was improperly disclosed, it may be inequitable to subject her to liability.[136] Arguably, this is merely an application of a detrimental reliance or estoppel theory, which is widely applied in a variety of legal fields to facilitate equitable results.

b. UTSA

Consistent with the common law, the UTSA makes a third party liable for trade secret misappropriation if she acquires a trade secret with knowledge that the trade secret was obtained in breach of an obligation to maintain its secrecy or via improper means.[137] Additionally, an innocent third party who acquires a trade secret may escape liability for misappropriation if she materially changes her position prior to learning that she has acquired a trade secret by accident or mistake.[138] Arguably, this exception to liability is analogous to the similar exception, discussed above, under the

134. This should make it clear that a trade secret owner must engage in some policing or oversight of the activities of her trade secret licensees. The absence of such policing could result in a licensee disclosing the trade secret to a third party who does not know such secret was transferred improperly. Such third party could innocently disclose the trade secret to the public, thereby destroying its economic value.

135. RESTATEMENT (FIRST) OF TORTS § 758(b).

136. *See* RESTATEMENT (FIRST) OF TORTS § 758 (b); *see also* BP Chems. Ltd. v. Formosa Chem. & Fibre Corp., 229 F.3d 254, 264 n.3 (3rd Cir. 2000).

137. *See* UNIF. TRADE SECRETS ACT § 1(2)(i), 14 U.L.A. 438.

138. *Id.* § 1(2)(ii)(C).

Restatement.

F. *Remedies*

Unlike many assets, the value of a trade secret is difficult to determine. Its value depends upon many factors, including how long it will retain economic value. This depends on predicting many things, including how long the owner can maintain it as a secret[139] and whether other innovations will nullify any economic advantage flowing from the trade secret. Such a valuation is inherently difficult and often speculative. Additionally, a trade secret, unlike other property, is volatile in nature. Once it is publicly disclosed, the property interest ceases to exist. Consequently, in some cases, injunctive relief may be preferable to monetary damages.

1. Preliminary Relief

A trade secret owner will often seek an ex parte temporary restraining order or a preliminary injunction when she learns that a third party is engaged in improper use of her trade secret.[140] This is often viewed as a necessity to prevent public disclosure of the trade secret, which would destroy the trade secret, and to further prevent the resulting competitive advantage that flows from it. This remedy is typically permitted both at common law and under the UTSA.[141]

Such preliminary relief is often essential to limit the potential loss of trade secrets resulting from departing employees. This is a major concern in light of the mobility of the United States workforce. Typically, workers, especially highly trained technical workers, will often be employed by competitors of a former employer. This may enable the former employee to disclose her former employer's trade secrets to her new employer. Former employers in such cases often seek an injunction barring the former

139. National Starch & Chem. Corp. v. Parker Chem. Corp., 530 A.2d 31, 33 (N.J. Super. Ct. App. Div. 1987) (damages may be inadequate once trade secret disclosed).

140. *See* COHEN & GUTTERMAN, *supra* note 37, at 217 (regarding requirements to obtain a preliminary injunction).

141. *See* UNIF. TRADE SECRETS ACT § 2(A), 14 U.L.A. at 449 (allowing threatened misappropriation to be enjoined).

employee from working for the new employer on the theory that it is inevitable that the former employee will disclose the former employer's trade secrets. This theory, known as the *inevitable disclosure* doctrine, has been recognized by some courts.[142] Nevertheless, it has some limitations because it impacts the ability of an employee to choose where she desires to work. This necessitates balancing the employer's interest in protecting trade secrets against an employee's freedom to choose her place of employment.[143] Nevertheless, courts, in some cases, have preliminarily enjoined employees from working for a competitor for a limited period of time.[144]

2. Permanent Injunctive Relief

Upon a finding that a trade secret has been misappropriated, following adjudication on the merits, the trade secret owner can seek permanent injunctive relief against the party who acquired the trade secret via misappropriation. Typically, three different approaches or theories have been utilized by courts with regard to the issuance of injunctions following a trial on the merits.[145] Each of these theories is discussed below.

Shellmar Rule

Under the Shellmar rule, the party liable for misappropriation is permanently enjoined from ever using the trade secret.[146] This prohibition applies even if the trade secret, due to

142. *See* Pepsico, Inc. v. Redmond, 54 F.3d 1261 (7th Cir. 1995) (following the doctrine and finding that "a plaintiff may prove a claim of trade secret misappropriation by demonstrating that defendant's new employment will inevitably lead him to rely on the plaintiff's trade secrets."). *But see* Seagate Tech. v. IBM Corp., 962 F.2d 12 (8th Cir. 1992) (doctrine not followed). *See also* MASS. ANN. LAWS ch. 93, § 42A (allowing preliminary injunction against former employee working for competitor, but only after former employee has used trade secret).

143. Standard Brands, Inc. v. Zumpe, 264 F. Supp. 254, 259 (E.D. La. 1967).

144. *Pepsico*, 54 F.3d at 1261 (affirming a preliminary injunction temporarily restricting employee from working for competitor).

145. A longstanding conflict has existed among different jurisdictions with regard to the proper theory to utilize to determine the duration of an injunction. *See, e.g.*, American Can Co. v. Mansukhani, 742 F.2d 314, 334 n.24 (7th Cir. 1984).

146. *See generally* Shellmar Prods. Co. v. Allen-Qualley Co., 87 F.2d 104 (7th Cir. 1936).

public disclosure, has entered the public domain and consequently is free for anyone to use.[147] Such a remedy ensures that the party who engaged in misappropriation does not benefit from her wrongful conduct.[148] Nevertheless, it can be argued that such an injunction is punitive in nature if the trade secret at issue has entered the public domain. Additionally, from a public policy perspective, such an injunction may be unreasonable because it has an anticompetitive effect with regard to a trade secret that has been publicly disclosed. Namely, it essentially eliminates the misappropriator from being a competitor because she cannot use the trade secret even though everyone else can utilize it.[149]

Conmar Rule

According to the Conmar rule, injunctive relief will be allowed only until the trade secret enters the public domain.[150] Once it enters the public domain the only remedy is an award of damages.[151] Arguably, this result ensures that the remedy is more closely related to the injuries suffered by the trade secret owner.[152]

Head Start Rule

Consistent with the Head Start rule, injunctive relief will continue until the trade secret enters the public domain, plus an additional amount of time equal to the time it would take a competitor to be able to utilize the secret following public disclosure.[153] Arguably, this rule prevents the wrongdoer from gaining any competitive advantage in the marketplace. It puts the wrongdoer on an equal footing with other third parties who are free to use the trade secret once it is disclosed to the public.

Although judicial disagreement continues to exist with regard to the above rules, according to some commentators, the trend seems

147. *See id.* at 109-10.

148. *See id.* at 110.

149. *See* Kubik, Inc. v. Hull, 224 N.W.2d 80, 93-94 (Mich. Ct. App. 1974).

150. *See* Conmar Prods. Corp. v. Universal Slide Fastener Co., 172 F.2d 150, 156 (2d Cir. 1949).

151. *See id.* at 155-57.

152. *See Kubik*, 224 N.W.2d at 93.

153. *See* Winston Research Corp. v. Minnesota Mining & Mfg. Co., 350 F.2d 134, 141-43, (9th Cir. 1965).

to favor the Head Start Rule.[154] Additionally, the language of the UTSA seems consistent with the underlying theory of the Head Start rule.[155]

3. Damages

Preliminary and permanent injunctive relief are vitally important if the trade secret has not been publicly disclosed. Absent such relief, the trade secret can be disclosed and consequently destroyed. Therefore, injunctive relief is primarily aimed at preserving the existence of the trade secret. Once it is established that a trade secret has been misappropriated, damages may be available in addition to or instead of injunctive relief.[156] Damages are aimed at compensating the trade secret owner for actual monetary loss suffered due to trade secret misappropriation. Typically, such damages would be measured by the actual loss suffered by the trade secret owner. A variety of theories, discussed below, have been developed for determining the appropriate damages.

Actual Loss Theory

The actual loss to the trade secret owner represents the traditional common law theory of damages.[157] Typically, courts may consider the following in ascertaining actual damages:

- *Lost profits*[158]
- *Decline in the value of the business enterprise*[159]
- *Costs to develop the trade secret*[160]

154. *See, e.g.,* COHEN & GUTTERMAN, *supra* note 37 at 218.

155. *See* UNIF. TRADE SECRETS ACT § 2(a), 14 U.L.A. at 449..

156. *See id.* § 2 (injunctive relief) and § 3 (damages). *See also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 44 (injunctive relief) and § 45 (damages).

157. The Uniform Trade Secrets Act also expressly allows for damages based on the actual loss to the trade secret owner. *See* UNIF. TRADE SECRETS ACT § 3(A), 14 U.L.A. at 455. However, the Act provides that "[e]xcept to the extent that a material and prejudicial change of position prior to acquiring knowledge or reason to know of misappropriation renders a monetary recovery inequitable, a complainant is entitled to recover damages for misappropriation" of a trade secret. *Id.*

158. *See* Sperry Rand Corp. v. A-T-O, Inc., 447 F.2d 1387, 1394 n.4 (4th Cir. 1971).

159. *See generally* Smith v. Dravo Corp., 203 F.2d 369, 378 (7th Cir. 1953).

160. *See Kubik*, 224 N.W.2d at 95.

Costs to remedy the effects of misappropriation of the trade secret[161]

Often, it may be difficult to ascertain damages based on the above considerations. Additionally, damages based on mere speculation are not allowable.[162] Therefore, the trade secret owner typically must demonstrate that the asserted damages flow directly from the misappropriation of her trade secret.[163] This may involve providing evidence of:

• *Profit projections*

• *Sales projections*

•*Market trends suggesting sales increases but for the misappropriation*

•*Decreased sales/profits of trade secret owner following misappropriation*

•*Use of the misappropriated trade secret to sell competing goods*

The difficulty of proving actual losses coupled with the difficulty, in some cases, of overcoming the argument that the damages are merely speculative in nature has resulted in the development of additional damage theories.

Unjust Enrichment

Allowing a party to keep profits earned as a result of misappropriating a trade secret amounts to allowing someone to benefit from legally impermissible conduct. Therefore, on equitable grounds, a trade secret owner is entitled to recover the profits earned by the misappropriator based on her use of the trade secret plus the cost savings due to not having to develop the trade secret via independent development, reverse engineering or some other legitimate method.[164] Typically, the unjust enrichment theory of damages is used in lieu of the actual loss theory, discussed above, when actual damages are too difficult to establish. These theories can be viewed as alternate theories. Recovery is generally only allowed under one theory, in order to avoid double

161. *Id.*

162. *See* Julius Hyman & Co. v. Velsicol Corp., 233 P.2d 977, 1008 (Colo. 1951), *cert. denied*, 342 U.S. 870 (1951).

163. *See id.*

164. *See generally* Telex Corp. v. IBM, 510 F.2d 894, 932 (10th Cir. 1975).

recovery.[165] Nevertheless, in appropriate cases, recovery may be allowed under both theories provided the amount recovered under the unjust enrichment theory is not already accounted for under the actual loss theory.[166]

Reasonable Royalty Theory

The reasonable royalty theory is difficult to apply, because it involves attempting to ascertain what a reasonable royalty would be in a competitive marketplace. Therefore, it is typically used only when neither of the above theories provides adequate recovery.[167] If the trade secret has not been publicly disclosed and it has been licensed to third parties, those third party licenses can provide a good basis for determining damages under this theory. However, if the trade secret has been disclosed to the public, this theory of damages may be more difficult to apply. In ascertaining damages under this theory courts consider, among other things, the following factors:

• *Changes in the competitive relationship between the trade secret owner and the party who engaged in misappropriation*

• *Research and development costs to create the trade secret*

• *How important the trade secret is to the trade secret owner's business enterprise*

• *Number of licensees of the trade secret*

• *Amount paid by licensees to utilize the trade secret*

• *Current use of the trade secret by its owner*

• *Projected future uses of the trade secret*

• *Availability of alternatives to the trade secret that could be utilized*

Punitive Damages

At common law, courts have permitted punitive damages in appropriate cases.[168] The UTSA allows the court discretion to

165. *See Sperry Rand Corp*., 447 F.2d at 1392-93. *See also* UNIF. TRADE SECRETS ACT § 3(A), 14 U.L.A. at 455.

166. *See* UNIF. TRADE SECRETS ACT § 3, 14 U.L.A. at 455.

167. *See* Vitro Corp. of America v. Hall Chem. Co., 292 F.2d 678, 682-83 (6th Cir. 1961) (discussing the reasonable royalty theory).

168. *See, e.g.,* Clark v. Bunker, 453 F.2d 1006, 1011-12 (9th Cir. 1972). Such damages typically will only be awarded if the misappropriator "acted wantonly, willfully, or in reckless disregard of the [trade secret owner's] rights." In Re

award such damages, but punitive damages cannot exceed double any other damage award.[169]

Attorney's Fees

Under the UTSA, a court has discretion to award reasonable attorney fees to the prevailing party in a case involving willful and malicious misappropriation.[170] Additionally, such fees can be awarded to the prevailing party if a misappropriation claim is made in bad faith or if a motion to terminate an injunction is made or resisted in bad faith.[171]

III. RISKS TO TRADE SECRETS POSED BY COMPUTERIZATION

The use of nondisclosure agreements, restricting access to trade secrets on a need to know basis, utilizing security mechanisms to limit unauthorized access to trade secrets, reminding employees on a regular and ongoing basis of the importance of maintaining trade secrets in confidence and marking appropriate documents with a legend indicating they are secrets are among the standard mechanisms utilized to protect trade secrets. Such methods remain important today to protect trade secrets and to establish that reasonable actions have been taken to maintain secrecy. Nevertheless, modern computer technology has become a ubiquitous tool used in business in the United States. For example, most cash registers in retail stores are computerized and are often part of a system that utilizes software to keep track of inventory. They also often include technology that allows the electronic transmission of credit or debit card data directly to the credit issuer. Likewise, personal computers have become almost as common as telephones in the workplace; it is rare today to see a desk or workstation without a computer. Increasingly, such computers are connected to the other computers in the same organization via an internal network called an Intranet. Often, that Intranet is connected to the Internet so each computer on the network has

Innovative Constr. Sys., Inc., 793 F.2d 875, 889 (7th Cir. 1986).

169. *See* UNIF. TRADE SECRETS ACT § 3(B), 14 U.L.A. at 456. The Uniform Trade Secrets Act also provides that punitive damages can only be awarded "[i]f willful and malicious misappropriation exists. . . ." *Id.*

170. *See* UNIF. TRADE SECRETS ACT § 4, 14 U.L.A. at 459.

171. *See id.*

access to everything on the Internet. The use of and reliance on computers has become so commonplace that the inherent danger they pose to business information is often overlooked. This is problematic with regard to trade secrets because it may lead to their disclosure and consequent loss. Below is an overview of some practical concerns that should be addressed to ensure the protection of trade secrets and other confidential business information in a computer environment.

A. *Computers*

In many work environments desktop computers have become the primary device for creating data and information with word processing programs such as WORD, with database programs such as ACCESS, and with presentation software such as POWERPOINT. Modern computers typically come equipped today with very large hard drives so most users rarely delete anything they have created or stored on their computer. The result is that a significant amount of company data and information is often stored on such computers. This can include confidential information, trade secrets and other data not meant for external use by nonemployees. Leaving such computers unsecured is akin to leaving important company data in an unlocked file cabinet.[172] This can be problematic for many businesses because third parties, such as cleaning personnel, have access to offices during the evening when such offices are vacant. Additionally, the majority of enterprises outsource such cleaning services to independent contractors. Therefore, the enterprise has neither any control nor even knowledge of the cleaning personnel working in the facility in the evening when no company employees are present.

Simple security measures can be implemented at virtually no cost. At a minimum, employees should be reminded that important information is often stored on their desktop computers. Second, all such computers should employ methods to limit unauthorized access to them. The simplest access limitation is installing a password that must be provided to the computer whenever it is

172. Portable storage media for computer data, such as floppies, tapes or zip disks, should be secured. Just like important documents, such media can be copied with ease by unauthorized parties if they are left accessible.

turned on. Software to activate such passwords, often called power-on passwords, is included in almost all computers today and can be activated in a matter of minutes simply with a few keystrokes on the computer keyboard. Nevertheless, computers in most work environments are left on all day so a power-on password alone will not restrict access.[173] Therefore, all computers should also use a screensaver password; software to activate such a password is a standard feature on virtually all desktop computers today. Moreover, it can be activated very quickly by the computer user. Once such a password is activated, computer access will be restricted when the computer automatically shifts into screensaver mode after being left unattended. The use of a power-on password is still critical even if a computer is never turned off. Absent a power-on password, anyone could bypass the screensaver password by simply rebooting the computer. This simple password bypass is avoided, however, with the use of a power-on password since the rebooting process will halt if this password is not supplied to the computer.

B. *Laptop Usage*

Laptop computers have become standard tools carried by business personnel when traveling. They can reduce wasted time by allowing an employee to work while traveling.[174] Often they contain important company information that an employee loaded onto the computer so that she can work while traveling, or they may contain confidential information that will be used at a meeting

173. Many desktop computers are left on all night so that backup software can automatically operate. This is important since computers still "crash" and lose data that can only be easily recovered if the data is backed up. Computers can also be set up to automatically run antivirus software and other utilities such as Defrag and Scandisk. Additionally, desktop computers with Internet access can be programmed to periodically connect to the Internet and retrieve updates for an antivirus program. Such automated actions are important because most employees fail to backup data or run any utilities on a regular basis. It is also important to safeguard backup media, such a floppies, zip disks or tapes, since these can be easily removed or copied. One solution is to use avoid using removable backup media. For example, if desktop computers are networked they can automatically backup data to a secure network server. Alternatively, a second internal hard drive can be installed and used as a backup storage medium.

174. As an example, I am writing what you are currently reading on a laptop computer while traveling on an Amtrak train to a conference.

with other employees. Some employees even use a laptop at work with a docking station in lieu of a desktop computer. When they travel, they remove the laptop from its docking station and take it with them. In this case, the laptop may contain many, if not all, of the files used by an employee.

In addition to the risks discussed above for computers, laptops pose an additional risk: they can be more easily lost or stolen, and therefore could provide a third party with substantial access to confidential company information. Additionally, laptops are often used in public locations where third parties may inadvertently view confidential data on the computer screen. Banning the use of laptops by employees eliminates any risk but it is obviously impractical. Nevertheless, it is important to educate employees about the risks inherent in traveling with a laptop. At a minimum, only necessary files should be on a laptop. Additionally, it may be appropriate to carry confidential files on a disk that is carried separately from the computer, and to encrypt the data on this disk.

C. *Remote Access via the Internet*

Many organizations allow employees to access computer files and other data remotely over the Internet. This increases employee efficiency because the employee has access to substantial company resources, via the Internet, regardless of where she is located or traveling. It also facilitates telecommuting which is an option being used increasingly in some industries. Additionally, some employees, such as salespersons, can transmit customer data from a remote location back to the home office. Typically, all an employee needs is a laptop computer and Internet access. Increasingly, computers are sold with modems and/or network cards so a laptop can be connected to the Internet via an ordinary phone line or via a broadband connection, which hotels are starting to offer. One concern is that this increased efficiency comes at a cost. The Internet is accessible worldwide. Therefore, in addition to employees, virtually anyone with Internet access can potentially gain access to your computer system. This potential risk must be balanced against the damage that could result from third party access to valuable company information including trade secrets. Even if security measures are implemented they can only reduce

potential third party access; they cannot eliminate it. The degree and extent of any security measures largely depends on balancing the costs and inconvenience of such security against the value of the data being protected.

D. *Chat Rooms*

Chat rooms[175] have become a popular pastime for many Americans. Often people will engage in anonymous discussions, via chat rooms, with unknown third parties. Sometimes employees can inadvertently reveal information about their employer that can be utilized by a competitor who may be monitoring a particular chat room.[176] Such action may assist a competitor in ascertaining your confidential information. [177]

E. *E-mail*

E-mail has become the ubiquitous method of communicating in the modern business world.[178] Such commonplace use has obscured inherent risks related to using e-mail. As a result, many employees may discuss or transfer information that should be maintained in confidence. Once an e-mail message is created and sent, it often becomes permanent. Most individual e-mail programs on desktop computers keep copies of incoming and outgoing messages. Additionally, many companies have shifted to web based e-mail to facilitate using the e-mail system from any location. However, such mail systems are usually server-based such that a user's e-mail is maintained on the server. Typically, servers are backed up on a regular basis so copies of both incoming and outgoing e-mail may

175. A chat room is "a virtual room on the Internet where a conversation session takes place between individuals who often use pseudonyms to maintain anonymity." America Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377, 379 n.3 (Va. 2001).

176. *See* Susan Warren, *I-Spy: Getting the Lowdown on Your Competition is just a Few Clicks Away*, WALL ST. J., Jan. 14, 2002, at R14.

177. *See generally* Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756, 759-60 (N.J. Super. Ct. App. Div. 2001) (ruling that such action may be the basis of trade secret misappropriation action).

178. Businesses in North America sent 40 billion e-mail messages in 1995; in 2001, it is estimated that they sent 1.4 trillion messages. *See* Elizabeth Weinstein, *Help! I'm Drowning in E-Mail!,* WALL ST. J., Jan. 10, 2002, at B1.

be kept on tape or some other backup medium. As a result, a company may have confidential data available from a variety of places without realizing it. Additionally, anyone who gains access to an individual computer or the network may be able to read an employee's e-mail. Often this is easy to do in light of the fact that many employees use such simple passwords they can often be determined by guessing.[179]

F. *Computer Networks*

1. Wired Networks

Most companies connect all individual computers via wired networks. This means anyone in the company can potentially access data and files network-wide. Typically, the information technology personnel responsible for maintaining the computer system can access everything on the network. This would suggest background checks of such personnel prior to employment. Additionally, many if not most networks are also connected to the Internet. This allows computer hackers located anyplace in the world the potential to gain unauthorized access to your network. In light of current technology, highly skilled and determined hackers can penetrate virtually any computer network. Such activities may also be engaged in by competitors, or by foreign governments engaged in economic espionage.[180] In some cases, such unauthorized access may not even be detected. Therefore, an enterprise should seriously balance the benefit of allowing certain data to be maintained on networked computers against the consequences of unauthorized access.

2. Wireless Networks

Increasingly, many companies are utilizing wireless networks today. Often, the cost of retrofitting an older building by running cabling for a network is very costly. Modern wireless networks provide an alternative that is less expensive and highly reliable. Nevertheless, in addition to the risks associated with

179. Even if the password cannot be guessed a variety of "hacker" programs can be obtained from the Internet which enable a user to engage in unauthorized access to passwords.

180. *See supra* notes 48 & 49 and accompanying text.

wired networks, wireless networks provide an extra risk.[181] These networks essentially transmit radio waves that cannot be retained inside a building. Consequently, a third party, in a public area outside the building, can utilize a laptop computer to receive data transmitted on the wireless network. Such data could include e-mail, among other things. Encryption software can minimize the ability of such data being intelligible to a third party, but, surprisingly, many companies do not utilize encryption technology for wireless networks.[182]

G. *Disposal of Old Computer Equipment*

The rapid pace of technological development means computer equipment, unlike a lot of other office equipment, such as telephones, must be continually replaced. Desktop computers and laptops often need replacement every few years. Older computers are often donated to non-profit organizations although increasingly they are simply discarded because the usefulness of used computers is very limited.[183] Disposal of such equipment can lead to unintended disclosure of company information that is stored on the hard drives of the discarded computers. Even if the files on the hard drives are deleted prior to disposal of the computers, it is relatively simple to recover many of the files with inexpensive off-the-shelf software due to the fact that deleted files remain on the hard drive even after erasure. At a minimum, special programs, which are inexpensive and readily available, can be used to make it very difficult to recover deleted files. Nevertheless, in many cases it is preferable to remove hard drives prior to disposal of computers. They can then be physically destroyed. This eliminates any possibility that files can be recovered.

181. *See* Don Clark, *Security Experts are on Alert Over Wireless Hacking Technique*, WALL ST. J., Oct. 15, 2001, at B7. S*ee also* Eric Janszen, *Wireless Area Networks Could Pose Security Risks*, 19 MASS. HIGH TECH 23, 40 (Oct. 1, 2001).

182. *See* Clark, *supra* note 167.

183. Old machines often have little value because each new generation of software requires increased computing power. Therefore, the latest software programs will often not run (or they will run too slow) on older machines. Additionally, the computer industry generally does not provide much legacy support so older machines have limited use.

Floppy disks, tape cartridges, zip disks and CDs are all common media used to store computer data. Often these media are used to provide backups of important information on a computer. Disposal of these media may allow important confidential company information to become available to third parties.[184] Consequently, it is imperative that such media be physically destroyed before disposal.

H. *Reasonable Measures to Protect Trade Secrets in an Electronic Environment*

Trade secret law, as previously discussed, only requires reasonable measures to preserve secrecy. This is important since absolute protection of data in our electronically interconnected world is virtually impossible. Therefore, the question is what measures should be taken to ensure that the reasonableness standard will be met. Below is a list of measures that should be considered:

• *Ongoing employee education programs* - It is important to have ongoing efforts to remind employees of the risks to company data posed by computers and of the activities that must be employed to minimize these risks. Such efforts make it clear to employees that the company takes computer security seriously. Failure to engage in such educational activities often sends the message that the company is not concerned about computer security issues. Company actions can be largely responsible for the type of environment or culture that exists in a workplace, which can affect the ability of a company to protect secret information.

• *Firewalls* - Firewalls are software programs that can help identify and repel unauthorized third party entry into a computer system.

• *Anti-virus software* - The biggest problem with anti-virus software is that it is not updated once installed. New viruses are continually created so it is critical to update this software on a regular basis. Typically, such updates should be conducted at least

184. *See generally* Tennant Co. v. Advance Machine Co., 355 N.W.2d 720 (Minn. Ct. App. 1984) (concerning a situation in which a third party rummaged through company garbage to find information about its trade secrets).

monthly.

• *Encryption* - Numerous programs are currently available to encrypt e-mail and other data; many are relatively inexpensive.

• *Proper passwords* - Incredibly, many computer users use their first name or some other obvious password. Employees need to be educated to develop passwords that are more difficult to determine, like combinations of numbers and letters in both upper and lower case.

• *Change passwords periodically* - Few employees will ever voluntarily change their passwords. One simple solution, available if company computers are networked, is to program the network servers to invalidate passwords periodically, such as every 30 days. Then once a month every user will be prompted to select a new password to gain access to the network.

• *Restrict storage of important company data on removable media such as disks, tapes or CDs.*

• *Secure network backup media* - This applies to both backup tapes commonly used to backup network servers and to media used by individual employees to backup their computers.

• *Isolate sensitive data on an in-house computer that is not connected to the Internet or any external network.*

• *Immediately eliminate all computer access, including network access, for departing employees.*

• *Maintain a regular program of updating software whenever patches are made available to fix security problems* - Most hardware and software producers continually identify bugs or glitches in their software that can allow a third party unauthorized access. Typically, they provide software patches or fixes that can usually be downloaded free of charge from a website maintained by the company. Of course, such patches do not work unless they are downloaded and installed.

• *Designate a person to be responsible for the above tasks.*

IV. CONCLUSION

Trade secret law provides a viable option for protecting inventions and other know-how or information that can provide a competitive advantage in the marketplace. However, unlike other bodies of law that protect intellectual property, trade secret law

mandates that the subject matter of the trade secret be kept confidential. This necessitates careful consideration of both legal and business factors when deciding whether to rely on trade secret law in lieu of another body of law, such as patent law. Nevertheless, the extremely broad scope of subject matter protectible via trade secret law encompasses many things that are not given protection by any other body of intellectual property law. Therefore, trade secret law can serve as a source of protection, or it can supplement other types of protection by protecting aspects of intellectual property that fall outside the domain of patent, copyright or trademark law.

Nevertheless, the rapid expansion of computer technology has increased the vulnerability of business enterprises to unauthorized outsiders. The increased utilization of computer technology to store information and data electronically combined with widespread transfer of data via e-mail and the Internet enhances the risk that trade secrets can be misappropriated. This makes it important for an enterprise to identify potential risks and take appropriate precautions to minimize those risks.