NOTES

WWW.MISAPPROPRIATION.COM: PROTECTING TRADE SECRETS AFTER MASS DISSEMINATION ON THE INTERNET

INTRODUCTION

The dilemma of where communication on the Internet fits a body of law designed to handle more traditional forms of communication has consumed pages in both case reporters and law journals.[1] The law's lack of a uniform approach for regulating various media forms has complicated the debate whether communication on the Internet should be treated the same as or different from traditional media.[2] Many analysts argue to keep the Internet as free from regulation as possible in order to foster a zone of free speech similar to the protections governing the written media.[3] However, the rate at which users can disseminate information via new multimedia technologies provides one important difference between the Internet and the more traditional print media and suggests at least the

1. A Westlaw search in the "Journals and Law Reviews (JLR)" database revealed at least 2,900 articles related to the Internet published in the last two years. Likewise, a search in the "Federal and State Cases (ALLCASES)" database resulted in 715 cases involving the Internet.

2. When it comes to regulating access and content in the mass media, the law generally has taken one of two approaches. The law has applied the first approach, characterized by its high premium on the First Amendment's protection of free speech and little reliance on regulation, to traditional written media like books, newspapers, and magazines. The law has applied the second approach, identified by a higher level of regulation, to the more technologically advanced broadcast media such as radio and television. However, "[u]nlike the rise of broadcast television and other media over the decades, in which new technologies have generated new bodies of law and extensive government regulation, the Internet is being treated much like newspapers or books, with judges emphasizing the primacy of the First Amendment." Joan Biskupic, *In Shaping of Internet Law, First Amendment is Winning*, WASH. POST, Sept. 12, 1999, at A2.

3. For example, advocates routinely advance this argument in order to protect political speech on the Internet. In a recent congressional debate over potential regulation of the Internet by the Federal Elections Commission, one Senator argued:

> The Internet uniquely provides the ability for any individual to express his political beliefs, and we think that should not be infringed upon. To limit free speech of individuals in the very country that created the Internet is as dangerous as it is misguided. As chairman of the Senate Communications Subcommittee, and cochairman of the Internet Caucus, I have been convinced time and time again of the folly of trying to regulate the Internet.
>
> Government should not impose burdensome regulations on political speech on the Internet, or any other medium. Instead, the Government should act to keep the Internet and those medium outlets a free speech zone.

145 CONG. REC. § 512,660, 667 (daily ed. Oct. 15, 1999) (statement of Sen. Burns).

possibility that the Internet warrants a unique approach.[4] This difference has caused at least one journalist to comment that "[m]onks spend years hunched over parchment to copy great works. Early presses took days. Xerox machines take hours. Now on the Internet, duplication is instantaneous."[5]

The rise of new media, especially the Internet, has brought with it a host of new legal and ethical issues. Although these issues are variations on traditional legal themes, they require fundamentally new approaches.[6] The popularity of the Internet as a forum for communication has placed a spotlight on the need to protect original ideas from improper use.

In the corporate arena especially, the issue of misappropriation[7] of

---

4. By one account, 125 million people worldwide use the Internet. Seventy million of them are in the United States alone. Some analysts estimate that this number will increase to 120 million in the United States and 250 million worldwide by 2001. 4 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 17.02 (1999). Although these numbers are very impressive, it is the ease with which one person has access to the other millions of Internet users that magnifies both the Internet's power and its dangers.

5. Lisa Carricaburu, *Cyber-Thieves; Internet's Speed Increases Pace of Broken Copyrights*, SALT LAKE TRIB., Feb. 11, 1998, at A1.

6. For an interesting discussion of current controversies in Internet law, see Jonathan D. Bick, *Why Should the Internet Be Any Different*, 19 PACE L. REV. 41 (1998).

7. Currently, legislation on the state level provides the most trade secret protection. Because a majority of the states have patterned their legislation on the Uniform Trade Secrets Act ("UTSA"), the Act itself provides the most relevant definition of "misappropriation":

> (2) "Misappropration" means:
>
> (i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or
>
> (ii) disclosure or use of a trade secret of another without express or implied consent by a person who
>
> (A) used improper means to acquire knowledge of the trade secret; or
>
> (B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was
>
> (I) derived from or through a person who had utilized improper means to acquire it;
>
> (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
>
> (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
>
> (C) before a material change of his [or her] position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

U.T.S.A. § 1-2 (1985). To date 43 states have adopted some form of the Uniform Trade Secrets Act ("UTSA"). *See* ALA. CODE §§ 8-27-1 to 6 (1993); ALASKA STAT. §§ 45.50.910-.945 (Michie 1996); ARIZ. REV. STAT. ANN. §§ 44-401 to 407 (West 1994); ARK. CODE ANN. §§ 4-75-601 to 607 (Michie 1991); CAL. CIV. CODE §§ 3426.1-.11 (West 1997); COLO. REV. STAT. §§ 7-74-101 to 110 (1997); CONN. GEN. STAT. ANN. §§ 35-50 to 58 (West 1997); DEL. CODE ANN. tit. 6, §§ 2001-2009 (1993); D.C. CODE ANN. §§ 48-501 to 510 (1997); FLA. STAT. ANN. §§ 688.001-.009 (West 1990 & Supp. 1997); GA. CODE ANN. §§ 10-1-760 to 767 (1994); HAW. REV. STAT. §§ 482B-1 to 9 (1992); IDAHO

trade secrets[8] poses unique problems in the context of an Internet-oriented culture.[9] The recent battle between the auto giant Ford Motor Company and a Web site publisher, Robert Lane, provides a telling example. In Detroit, Ford granted Lane's request to cover the company's vehicle development program, issuing him a media pass and allowing him access to the company's designers.[10] Lane compiled the information that he gained from this access and launched a Web site[11] devoted to providing automobile enthusiasts with information about Ford's products and company news.[12] As Lane's site grew in size and popularity, anonymous sources within Ford began providing him with corporate documents.[13] Ford refused Lane's request to sponsor his site, and their relationship

---

CODE §§ 48-801 to 807 (Michie 1997); 765 ILL. COMP. STAT. ANN. 1065/1-/9 (West 1993); IND. CODE ANN. §§ 24-2-3-1 to 8 (Michie 1995); IOWA CODE ANN. §§ 550.1-.8 (West Supp. 1994); KAN. STAT. ANN. §§ 60-3320 to 3330 (1994); KY. REV. STAT. ANN. §§ 365.880-.900 (Michie 1996); LA. REV. STAT. ANN. §§ 51:1431-:1439 (West 1987 & Supp. 1995); ME. REV. STAT. ANN. tit. 10, §§ 1541-1548 (West 1997); MD. CODE ANN., COM. LAW. II §§ 11-1201 to 1209 (1990); MICH. COMP. LAWS §§ 445.1901- .1910 (1998); MINN. STAT. ANN. §§ 325c.01-.08 (West 1995); MISS. CODE ANN. §§ 75-26-1 to 19 (1991); MO. ANN. STAT. §§ 417.450-.467 (West 1995); MONT. CODE ANN. §§ 30-14-401 to 409 (1997); NEB. REV. STAT. §§ 87-501 to 507 (1994); NEV. REV. STAT. §§ 600A.010-.100 (1991); N.H. REV. STAT. ANN. §§ 350- B:1-:9 (1995); N.M. STAT. ANN. §§ 57-3A-1 to 7 (Michie 1998); N.C. GEN. STAT. §§ 66-152 to 157 (1997); N.D. CENT. CODE §§ 47-25.1-01 to 08 (1993); OHIO REV. CODE ANN. §§ 1333.61-.69 (West 1994); OKLA. STAT. tit. 78, §§ 85-94 (1991); OR. REV. STAT. §§ 646.461-.475 (1993); R.I. GEN. LAWS §§ 6-41-1 to 11 (1992); S.C. CODE ANN. §§ 39-8-10 to 130 (Law. Co-op. 1997); S.D. CODIFIED LAWS §§ 37-29-1 to 11 (Michie 1994); UTAH CODE ANN. §§ 13-24-1 to 9 (1996); VT. STAT. ANN. tit. 12, § 523 (1996); VA. CODE ANN. §§ 59.1-336 to 343 (Michie 1992); WASH. REV. CODE ANN. §§ 19.108.010-.940 (West 1989); W. VA. CODE §§ 47-22-1 to 10 (1996); WIS. STAT. ANN. § 134.90 (West 1989).

8. In its simplest terms, "a trade secret is legally anything that gives a competitor an advantage or head start." ROBERT C. DORR & CHRISTOPHER H. MUNCH, PROTECTING TRADE SECRETS, PATENTS, COPYRIGHTS, AND TRADEMARKS §§ 2.01[C](2000). When information rises to the level of a trade secret, the company or individual owner of the trade secret has exclusive rights to its use or control provided that the information remains protected from general disclosure. *Id.* For a more detailed discussion about trade secret misappropriation, see *infra* Part I.A.

9. Now that many employees have computers on their desktops, employers battle a variety of evils caused by the Internet. Some of these evils fit into the category of innocent distractions: personal e-mails, trading stocks on-line, or playing Internet-based games at work. Other evils, however, such as lewd e-mails and the viewing of on-line pornography, threaten the nature of the office work environment and can lead to sexual harassment lawsuits. In addition, this new personal technology poses external threats to the stability of the company when employees use workplace computers to intentionally disseminate the company's trade secrets. All of these problems, taken together, have prompted companies to initiate steps to monitor their employees' use of the Internet while at work. *See* Michael Stroh, *Firms Turn to Snoop Software Big Browser on Patrol in Computer Work Places*, BALTIMORE SUN, Oct. 19, 1999, at 1C.

10. Fara Warner et al., *Holes in the Net: Can the Big Guys Rule the Web? Ask Ford or Dunkin' Donuts*, WALL ST. J., Aug. 30, 1999, at A1.

11. Robert Lane, *BlueOvalNews.com, at* http://www.blueovalnews.com (last visited Nov. 13, 1999).

12. *See* Warner et al., *supra* note 10.

13. *Id.*

eventually soured.[14] Soon after, Lane began posting on his Web site some of the corporate documents he had received from his anonymous sources at Ford.[15] In an attempt to protect its ownership rights in the documents, Ford sought to enjoin Lane from continuing to show the documents on his site; however, the federal district court refused to grant the injunction on the grounds that Lane's First Amendment protections outweighed Ford's proprietary interest in the documents.[16]

The battle between Lane and Ford is, to date, the most publicized in a series of disputes over the misappropriation of trade secrets on the Internet.[17] However, new media poses other problems involving trade secrets in the workplace as well.[18] For instance, advances in technology have made it much easier for employees to take proprietary information with them when they change jobs.[19]

In light of cases like *Ford Motor Co. v. Lane*, this Note will examine the history of trade secret protection on the Internet, chart out how courts have approached this issue over time, and offer a proposal for addressing this problem in the future. Part I will provide a fundamental background in trade secret analysis. Part II will examine the traditional ways in which businesses and legal scholars have approached the problem of trade secret misappropriation and the Internet. Finally, Part III will propose the need for new federal legislation to help combat the dangers of mass dissemination of trade secrets on the Internet.

---

14. *Id*.

15. *Id*.

16. Ford Motor Co. v. Lane, 67 F. Supp. 2d 745, 754 (E.D. Mich. 1999).

17. For other examples of publicized disputes over trade secrets and the Internet, see *infra* Part I.C.

18. An example of such a situation is demonstrated by Wal-Mart's recent suit against the Internet retailer Amazon.com for allegedly luring several of Wal-Mart's employees to leave Wal-Mart with copies of sensitive corporate information. The material included consumer data, stocking schemes, and information about its distribution network. Emily Nelson, *Wal-Mart Accuses Amazon.com of Stealing Its Secrets in Lawsuit*, WALL ST. J., Oct. 19, 1998, at B12. The case has since settled and Amazon agreed to reassign one of the information-systems workers whom it hired away from Wal-Mart. Helen Jung, *Wal-Mart Settles with Amazon.com: Dispute over Hiring Away Retail Giant's Tech Workers*, SEATTLE TIMES, Apr. 5, 1999, at C1.

19. The high profile defection of General Motors' former purchasing chief, Jose Ignacio Lopez de Arriortua, to Volkswagen illustrates both the old and new methods of trade secret theft. When Lopez left GM in 1993, he and his top deputies removed sensitive and proprietary documents in both paper and electronic form. According to investigators, Lopez and his associates removed 20,000 documents consisting of millions of pages in cartons and suitcases as well as far more discrete computer diskettes. *See* Daniel Howes, *How GM Closed Its Chapter of the Lopez Affair*, DET. NEWS, Jan. 12, 1997, at F1; Micheline Maynard, *Rogue Warrior: Espionage and Intrigue in the Lopez Affair*, USA TODAY, Dec. 20, 1996, at B1-B2.

I. A HISTORICAL EXAMINATION OF TRADE SECRET PROTECTION

A. The Rise of Trade Secret Protection

Because the developing law regarding trade secret protection on the Internet is fundamentally rooted in traditional media law, any consideration of Internet protection must begin with a discussion of trade secrets in the media. Traditional definitions of "trade secrets" reflect the law's desire to provide protection to a significant body of proprietary information.[20] To justify such protection, courts[21] and legal scholars[22] contend that the protection of trade secrets advances public interest by

---

20. The *Restatement of Torts* defines a trade secret as "any formula, pattern, device or compilation of information which is used in one's business and which gives him an opportunity to obtain an advantage over competitors who do not know or use it." RESTATEMENT (FIRST) OF TORTS § 757 cmt.b (1939). *The Restatement of Unfair Competition* takes a similar view: "[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) UNFAIR COMPETITION § 39 (1995).

In the United States Code:

> the 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.

18 U.S.C. § 1839(3) (Supp. IV. 1998).

21. The United States Supreme Court in Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974), noted five basic reasons to protect trade secrets: 1) to allow businesses to enter into good faith transactions; 2) to form stable relationships; 3) to share confidential information; 4) to assist in product development; and 5) to deny competitors an advantage that they have obtained by unfair means. *Id.* at 480-87. Other courts have indicated that "trade secret law is designed to protect against a breach of faith and reprehensible means of learning another's secrets." Cataphote Corp. v. Hudson, 444 F.2d 1313, 1314 (5th Cir. 1971).

22. Professors Robert Cooter and Thomas Ulen approach the public-good rationale for trade secret protection from a more economically-oriented point of view:

> the creator of an idea has difficulty appropriating its social value. Granting exclusive rights to the creator of an idea allows him or her to appropriate much of its social value. Consequently, the incentive to create ideas aligns closely with their social value, as required for efficient innovation. . . . In general, the broader the scope and the longer the duration of the creator's property rights, the stronger the incentive for creating ideas and the weaker the incentive for disseminating and applying them.

ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 119 (2d ed. 1997). However, for a contrary view see Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241 (1998).

fostering innovation and new ideas.[23] The problem with trade secrets and the Internet, however, is that once someone posts information on the Web, the information becomes available for the entire world to see,[24] and it ceases to be a secret.[25] Courts have generally adopted this view.[26]

---

23. The *Restatement of Unfair Competition* provides a traditional public-good rationale for the protection of trade secrets:

> The development of rules protecting trade secrets formed part of a more general attempt to articulate standards of fair competition. More recently, the protection of trade secrets has been justified as a means to encourage investment in research by providing an opportunity to capture the returns from successful innovations. The rules protecting trade secrets also promote the efficient exploitation of knowledge by discouraging the unproductive hoarding of useful information and facilitating disclosure to employees, agents, and others who can assist in its productive use. Finally, the protection afforded under the law of trade secrets against breaches of confidence and improper physical intrusions furthers the interest in personal privacy.

RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. a (1995).

24. One commentator has noted five different ways in which trade secrets can find their way into cyberspace. First, companies, without realizing the consequences, may post information deliberately as a means of showing potential clients, investors, or other outsiders the strength of the company. Second, employees may e-mail secrets to individuals outside of the company without adequately securing the information from retransmission. Third, employees may send the information to third parties for malicious reasons. Fourth, an employee or someone else may post the information on a Web page or bulletin board. Fifth, hackers may break into the company's computer to steal the information and post it on the Web. Victoria A. Cundiff, *Trade Secrets and the Internet: A Practical Perspective*, 14 No. 8 COMPUTER LAW., August, 1997, at 6.

25. *See* State *ex rel*. Rea v. Ohio Dept. of Educ., 692 N.E. 2d 596, 601 (Ohio 1998) (noting that "once material is publicly disclosed, it loses any status it ever had as a trade secret.")

26. The United States Supreme Court originally took the position that trade secret law "does not offer protection against discovery by fair and honest means, such as by independent invention, accidental disclosure or by so-called reverse engineering, that is by 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). However, over time some courts have used this proposition to support the notion that once a trade secret has been placed in the public domain by any means, it is no longer a trade secret:

> The nature of a trade secret is such that, so long as it remains a secret, it is valuable property to its possessor who can exploit it commercially to his own advantage. Once the secret is published to the "whole world," however, it loses its protected status and becomes available to others for use and copying without fear of legal reprisal from the original possessor.

Underwater Storage, Inc. v. United States Rubber Co., 371 F.2d 950, 954 (D.C. Cir. 1966).

Despite this apparent high bar to obtaining trade secret status announced by the court in *Underwater Storage*, the court provided support for the continuing protection of companies from the use of the trade secret by those acting in concert with the original misappropriator. For example, the court would not allow Company *A* to utilize the trade secrets of Company *B* if Company *A* hired a thief to steal Company *B*'s trade secrets and then post the information on the Internet for the benefit of both Company *A* and the rest of the world. *Id*. at 955. To this scenario the court responded: "We do not believe that a misappropriator or his privies can 'baptize' their wrongful actions by general publication of the secret." *Id*. Put another way, two commentators have noted that "[t]his is something like a situation where a wife murders her husband and then pleads for mercy at sentencing time on the ground she is a widow." EARL W. KINTNER AND JACK L. LAHR, AN INTELLECTUAL PROPERTY LAW PRIMER 221 (1975). However, the small amount of protection provided by the court in *Underwater Storage* would do little to protect Company *B* if Company *A* was not a party to the initial theft, but rather innocently stumbled onto the materials on the Internet after a misappropriator posted them there.

Trade secret protection began as a loose series of common law decisions, eventually synthesized in the *Restatement (First) of Torts*.[27] The Supreme Court first recognized the common law tort of "misappropriation" in *International News Service v. Associated Press*.[28] In defining this new tort, the Court distinguished it from previously recognized tortious conduct in that the "defendant's conduct differs from the ordinary case of unfair competition in trade principally in this that, instead of selling its own goods as those of complainant, it substitutes misappropriation in the place of misrepresentation, and sells complainant's goods as its own."[29] Protection of trade secrets at the state level received a boost in 1979 when the National Conference of Commissioners on Uniform State Laws approved the Uniform Trade Secrets Act ("UTSA").[30] However, despite the theoretical benefit of such a "uniform" act, UTSA's inconsistent use by the states provided less than adequate protection for individuals and companies needing its coverage.[31] Only recently has Congress enacted federal legislation to provide criminal sanctions for trade secret misappropriation,[32] and some experts have suggested that this congressional response fails to go far enough.[33] In fact, some scholars have even endorsed the enactment of UTSA-based legislation on the national level as a means to replace patchwork state laws with a statutory scheme that federal courts could apply consistently across the country.[34]

See infra notes 85-96 and accompanying text for a further discussion of this scenario.

27. Marina Lao, *Federalizing Trade Secrets Law in an Information Economy*, 59 OHIO ST. L.J. 1633, 1649 (1998).

28. 248 U.S. 215 (1918).

29. *Id.* at 242. Despite the significance of *International News Service*, the Restatement (Third) of Unfair Competition points out that even though "the decision has been frequently cited, it has been sparingly applied. Notwithstanding its longevity, the decision has had little enduring effect." RESTATEMENT (THIRD) UNFAIR COMPETITION § 38 cmt.b (1995).

30. U.T.S.A. Prefatory Note (1990).

31. In her article on the need for a federal civil trade secrets statute, Professor Lao notes that "unlike the Uniform Commercial Code, the UTSA never won the support of all of the states, and even the states that did adopt the UTSA modified it, sometimes substantially, before enactment. Consequently, despite UTSA, the law on trade secret misappropriation continues to vary from jurisdiction to jurisdiction." Lao, *supra* note 27, at 1649-50.

32. *See, e.g.*, the Economic Espionage Act, 18 U.S.C. § 1831 (Supp. IV 1998), and the Federal Trade Secrets Act, 18 U.S.C. § 1832 (Supp. IV 1998).

33. For a thorough review of federal activity in trade secrets laws and a call for further congressional action, see Lao, *supra* note 27.

34. *Id.* at 1694-95. Professor Lao suggests that any national trade secrets legislation could easily use the UTSA as a pattern because it preserves "the balance between protection on the one hand and disclosure and competition on the other hand . . . ." *Id.* at 1694. Lao asserts that in addition to remaining consistent with our international treaty obligations, the model act has carefully avoided infringing on the domains of the patent and copyright laws:

> For example, recognizing that society does not exact anything tangible from the owner of a

B. The Prior Restraint Problem[35]

Throughout much of the last century, even before the advent of the Internet, the Supreme Court has been reluctant to endorse prior restraints (such as injunctions or temporary restraining orders) when dealing with free speech issues. In the first case to establish boundaries for the doctrine, the Court faced a suit by local officials who attempted to force a newspaper out of business.[36] The paper had reported allegations that a local organized crime figure supported gambling, bootlegging, and racketeering under the noses of Minneapolis's law enforcement community.[37] In an attempt to silence the paper, the local county attorney brought suit under a Minnesota statute[38] to enjoin *The Saturday Press* from continuing to publish.[39] In what would form the basis of free speech protection in later cases dealing with the Internet,[40] the Supreme Court in *Near v. State of Minnesota*[41] ruled in favor of the newspaper, stating: "In determining the extent of the constitutional protection, it has been generally, if not universally, considered that it is the chief purpose of the

---

> trade secret in return for protection, such as disclosure of the secret for the public's future use, the UTSA does not grant exclusivity to the owner; it only protects the owner against another's taking of her information in a morally reprehensible manner (improper means), and only if the information or knowledge was in fact secret, which means not already in the public domain.

Id. at 1695.

35. Other articles go into great detail on the process of injunction and the application of the prior restraint doctrine. Because courts have refused almost uniformly to employ prior restraints when trade secrets are released on the Internet, this Note will make only general references to injunctive relief. For a comprehensive examination of the prior restraint doctrine in the context of information on the Internet, see Ryan Lambrecht, Note, *Trade Secrets and the Internet: What Remedies Exist for Disclosure in the Information Age*, 18 REV. LITIG. 317 (1999).

36. Near v. State of Minnesota, 283 U.S. 697 (1931).

37. *Id.* at 703-4.

38. As quoted by the Court, the relevant portion of the statute is as follows:

> Section 1. Any person who, as an individual, or as a member or employee of a firm, or association or organization, or as an officer, director, member or employee of a corporation, shall be engaged in the business of regularly or customarily producing, publishing or circulating, having in possession, selling or giving away . . .
>
> (b) a malicious, scandalous and defamatory newspaper, magazine or other periodical, is guilty of a nuisance, and all persons guilty of such nuisance may be enjoined, as hereinafter provided.

Id. at 702.

39. *Id.* at 703.

40. *See, e.g.*, Ford Motor Co. v. Lane, 67 F. Supp. 2d 745 (E.D. Mich. 1999); Taucher v. Born, 53 F. Supp. 2d 464 (D.D.C. 1999); SNA, Inc. v. Array, 51 F. Supp. 2d 542 (E.D. Pa. 1999); Junger v. Daley, 8 F. Supp. 2d 708 (N.D. Ohio 1998); N.W. Enter. v. City of Houston, 27 F. Supp. 2d 754 (S.D. Tex. 1998); Religious Tech. Ctr. v. Lerma, 897 F. Supp. 260 (E.D. Va. 1995).

41. 283 U.S. 697 (1931).

guaranty [of freedom of the press] to prevent previous restraints on publication."[42] The Court further noted that only in the most extreme cases would it allow a prior restraint on publication.[43]

Although the Court in *Near* left the door open for restraints on free speech in cases that involve national security,[44] the Court later refused to expand that exception when it considered the national security question directly in *New York Times Co. v. United States*.[45] In what became known as the *Pentagon Papers Case*, a former Department of Defense official, Daniel Ellsberg, leaked a top secret defense department study entitled "History of U.S. Decision Making Process on Vietnam Policy" and a report labeled "Command and Control Study of the Tonkin Gulf Incident" to various news sources.[46] The federal government then filed suit to block the publication of these reports by the *New York Times* and the *Washington Post*.[47] The Supreme Court, in a per curium opinion,[48] refused to grant the Justice Department's request to enjoin the *New York Times* and the *Washington Post* from publishing any additional excerpts from the top secret reports.[49] Despite the national security implications of

---

42. *Id.* at 713.

43. *Id.* at 716. Chief Justice Hughes limited this exception to the general prohibition against prior restraints to a few "exceptional cases." *Id.* The Chief Justice listed as exceptional cases: 1) during times of war when such speech would interfere with recruitment efforts or would compromise strategic plans; 2) when the "requirements of decency" require a prohibition against obscene material; 3) incitements to acts of violence; and 4) to prevent the overthrow of the government. *Id.*

44. *Id.*

45. 403 U.S. 713 (1971).

46. For a history of the facts of the *Pentagon Papers Case*, see Whitney North Seymore, Jr., *At Last, the Truth is Out*, 19 CARDOZO L. REV. 1359 (1998).

47. New York Times Co., 403 U.S. at 714.

48. Scholars have doubted the actual significance of the *Pentagon Papers Case*. Some argue that it was not a great victory for the freedom of the press, but rather opened the door to censorship in situations where the government can build a compelling case that the necessity of secrecy outweighs the public's right to know. *See, e.g.*, Stanley Godofsky & Howard M. Rogatnick, *Prior Restraints: The Pentagon Papers Case Revisited*, 18 CUMB. L. REV. 527 (1988). Others argue that the *Pentagon Papers Case* was a significant case for the freedom of the press. The Court has since ruled both ways on the issue:

> Following the *Pentagon Papers* ruling, the Court further expanded freedom of the press by striking down an injunction against publication of news which allegedly would have prejudiced the jury in a murder prosecution. The Court extended free speech claims to the new territories of commercial speech and political campaign spending, and it granted the press a broad right of access to criminal trials. On the other hand, the Court restricted press access to prisons and pretrial suppression hearings, it limited speech occurring on public and private property, it reduced the protection accorded to defamatory speech, and it resorted to virtually incoherent doctrine to censor speech found to be "obscene."

Norman Dorsen, *The United States Supreme Court: Trends and Prospects*, 21 HARV. C.R.-C.L. L. REV. 1, 9-10 (1986).

49. *New York Times Co.*, 403 U.S. at 714.

publication, the Court found that the government simply had not demonstrated a sufficient justification for imposing a prior restraint.[50] This decision thus raised the bar for challenges to free speech and later provided a key component in First Amendment claims brought by Web site operators.[51]

C. Free Speech Applied to the Internet

In 1997 the United States Supreme Court had the opportunity to examine the issue of constraints on free speech as it applied to communication on the Internet in a landmark case in Internet law.[52] In *Reno v. American Civil Liberties Union*[53] the ACLU challenged the constitutionality of provisions of the Communications Decency Act (CDA).[54] Specifically, the advocates for free speech on the Internet objected to two provisions[55] designed to "protect minors from 'indecent'

---

50. *Id.*

51. *See, e.g.*, Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211 (S.D.N.Y. 2000); Ford Motor Co. v. Lane, 67 F. Supp. 2d 745 (E.D. Mich. 1999); Cyberspace Communications, Inc. v. Engler, 55 F. Supp. 737 (E.D. Mich. 1999); Taucher v. Born, 53 F. Supp. 2d 464 (D.D.C. 1999); Junger v. Daley, 8 F. Supp. 2d 708 (N.D. Ohio 1998); Am. Civil Liberties Union v. Johnson, 4 F. Supp. 2d 1029 (D.N.M. 1998); United States v. Matthews, 11 F. Supp. 2d 656 (D. Md. 1998); Religious Tech. Ctr. v. Lerma, 897 F. Supp. 260 (E.D. Va. 1995).

52. As one article noted:

> Reno v. ACLU is significant for two basic but noteworthy reasons. First, it represents the first time the Supreme Court has issued a ruling that goes to the very heart of the Internet, which the court itself described as a "unique and wholly new medium of worldwide human communication."
>
> Second, the court clearly and unequivocally decided that this new medium warrants full First Amendment protection.

Michael J. Wagner, *While the Courts in 1997 Grappled with Novel Internet Issues, New Questions Concerning Business and Attorney-Client Confidences are Likely to Arise in 1998*, NAT'L L.J., Jan. 19, 1998, at B7.

53. 521 U.S. 844 (1997).

54. 47 U.S.C. § 223 (Supp. 1997).

55. The first provision, 47 U.S.C. § 223(a), makes illegal the knowing transmission of obscene or indecent messages to any recipient under 18 years of age by providing that:

> (a)Whoever—
>
> (1) in interstate or foreign communications--
>
> . . . .
>
> (B) by means of a telecommunications device knowingly—
>
> (i) makes, creates, or solicits, and
>
> (ii) initiates the transmission of, any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication;

and 'patently offensive' communications on the Internet."[56] In striking down the statute, the Court took note of the unique nature of the Internet compared to other forms of broadcast media.[57] The Court found two factors particularly persuasive in distinguishing the Internet from more traditional broadcast media. First, that the Internet has not faced the same level of regulation as the broadcast industry.[58] Second, that the Internet was not as "invasive" as the broadcast media and thus warranted different treatment.[59] Based in significant part on these distinctions, the Court announced a broad holding that protected not only potentially offensive

---

. . . .

. . . or

(2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity,

shall be fined under title 18, or imprisoned not more than two years, or both.

47 U.S.C. § 223(a) (Supp. 1997).

The second provision, § 223(d), prohibits knowingly sending or displaying patently offensive messages by any means that are available to a person under 18 years of age:

(d)Whoever—

(1) in interstate or foreign communications knowingly—

(A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or

(B) uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or

(2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity, shall be fined under Title 18, or imprisoned not more than two years, or both.

47 U.S.C. § 223(d) (Supp. 1997).

Under § 223(e)(5), the Act created two affirmative defenses to the proscribed conduct. The first defense protects those who take "good faith, reasonable, effective, and appropriate actions" to restrict access to the prohibited communications by minors. 47 U.S.C. § 223(e)(5)(A) (Supp. 1997). The second provision provides a defense to those who restrict viewers' access to covered material by requiring forms that prove age, such as a verified credit card or an adult identification number or code. 47 U.S.C. § 223(e)(5)(B) (Supp. 1997).

56. 521 U.S. at 849.

57. *Id*. at 885.

58. *Id*. at 870. The Court explained the difference in the level of regulation of the Internet and broadcast media by stating that "unlike conditions that prevailed when Congress first authorized regulation of the broadcast spectrum, the Internet can hardly be considered a 'scarce' expressive commodity." *Id*.

59. *Id*. at 869. The Supreme Court relied on the District Court's findings of fact in this respect, noting that "[t]he District Court specifically found that '[c]ommunications over the Internet do not "invade" an individual's home or appear on one's computer screen unbidden. Users seldom encounter content "by accident."'" *Id*.

materials on the Internet, but in later cases would apply to a wide range of communication in cyberspace as well.[60]

D. Misappropriation of Trade Secrets and the Internet

Two years before the United States Supreme Court conclusively applied the protections of free speech to the Internet,[61] a series of cases testing the delicate balance between the new mass communications medium of the Internet and an individual's or company's proprietary interest in a potential trade secret reached the federal courts. The *Scientology Cases* have formed the basis of most of the scholarly writing and thought on this subject to date.[62]

As in each of the *Scientology Cases*, the earliest case, *Religious Technology Center v. Lerma*,[63] involved a suit by a branch of the Church, the Religious Technology Center.[64] The Church of Scientology filed suit in federal court to enjoin one of its former members, Arnaldo Lerma, from posting writings[65] by the Church's founder, L. Ron Hubbard, on the

---

60. Requiring those seeking a restraint on free speech to meet a high standard, the Court insisted that:

> [a]s a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship.

Id. at 885.

61. See *supra* notes 52-60 and accompanying text for a discussion of *Reno v. Am. Civil Liberties Union*, 521 U.S. 844 (1997).

62. *See, e.g.*, Stephen Fraser, *The Conflict Between the First Amendment and Copyright Law and Its Impact on the Internet*, 16 CARDOZO ARTS & ENT. L.J. 1, 39 at n.277 (1998); Marilyn C. Maloney, *Intellectual Property in Cyberspace*, 53 BUS. LAW. 225, 235 (1997); James Boyle, *A Politics of Intellectual Property: Environmentalism for the Net?* 47 DUKE L.J. 87, 89 (1997).

63. 897 F. Supp. 260 (E.D. Va. 1995).

64. *See* Religious Tech. Ctr. v. F.A.C.T.Net, Inc., 901 F. Supp. 1519, 1521 (D. Colo. 1995).

65. The Church closely guards access to these documents, which are known as "Advanced Technology," through a procedure known as "auditing," which is believed to purge:

> impressions recorded by the unconscious mind in times of trauma in this life or previous lives . . . . Auditing uses the "technology" and "advanced technology" of the Church. . . . The adherent must proceed through a series of increasingly sophisticated technologies of closely structured questions and answers to reach a "higher level of spiritual existence." The Church asserts that the unsupervised, premature exposure of an adherent to these materials will produce a spiritually harmful effect.

Religious Tech. Ctr. v. Wollersheim, 796 F.2d 1076, 1077 (9th Cir. 1986). The auditing process involves supervision by senior members of the Church and is restricted to only those members who have "attained the proper level of enlightenment" as well as made sufficient pecuniary assistance to the Church. *F.A.C.T.Net*, 901 F. Supp. at 1521. As a testament to the level of protection that the Church afforded this information, prior to its unauthorized dissemination of some of these "Advanced Technology" documents on the Internet, the Church made the documents accessible from only seven

Internet.[66] The district court analyzed the problem by looking to *Near v. Minnesota*[67] and *New York Times v. United States*.[68] Using the analyses set forth in those two cases, the court rejected the Church's argument that dissemination of its materials would cause irreparable injury in the form of "copyright infringement and trade secret misappropriation."[69] Instead, the district court stated, "[i]f a threat to national security was insufficient to warrant a prior restraint in *New York Times Co. v. United States*, the threat to plaintiff's copyrights and trade secrets is woefully inadequate."[70] Further, the court looked to Virginia's definition of a trade secret.[71] The Virginia definition creates a two-part test for determining whether information rises to the level of a trade secret.[72] The first prong of this test requires that the information is not "generally known" to the public.[73] The second prong examines whether the holder of the purported trade secret has taken steps to protect the secrecy of the information.[74] In *Lerma*, the district court declared that a plaintiff must meet both prongs of the test.[75] Even though the Church satisfied the second prong by taking steps to prevent dissemination of the information, they were not entitled to an injunction without a showing that the Church satisfied the first prong as well.[76] The court noted that the plaintiff could not meet the first prong of the test because the Church's documents had "escaped into the public domain and onto the Internet . . . [and thus] it would seem that plaintiff

---

sites located around the world. *Id*. at 1521-22. The Scientologists are not the only religious group to claim a proprietary interest in their religious publications. On November 10, 1999, The Church of Jesus Christ of Latter Day Saints won a temporary restraining order from a federal district judge in Utah against the operators of a nonprofit ministry who posted excerpts from a Church handbook that is used by lay clergy. Steven Oberbeck, *Ministry's Restraint Order Expanded*, SALT LAKE TRIB., Nov. 11, 1999, at C2.

66. *Lerma*, 897 F. Supp. at 261-62.

67. 283 U.S. 697 (1931). For a discussion of *Near v. State of Minnesota*, see *supra* notes 37-43 and accompanying text.

68. 403 U.S. 713 (1971). For a discussion of *New York Times Co. v. United States*, see *supra* notes 45-51 and accompanying text.

69. *Lerma*, 897 F. Supp. at 262.

70. *Id.* at 263.

71. Virginia defines a "trade secret" as any information that

> [d]erives 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 . . . is the subject of efforts that are reasonable under the circumstance to maintain its secrecy.

VA. CODE ANN. § 59.1-336 (Michie 1992), *cited in Lerma*, 897 F. Supp. at 266.

72. 897 F. Supp. at 266.

73. *Id.*

74. *Id.*

75. *Id.*

76. *Id.*

cannot establish that the AT documents are not 'generally known.'"[77]

In the second *Scientology* case, *Religious Technology Center v. F.A.C.T.Net*,[78] the Church filed suit against various former members.[79] These individuals had developed a library and archive devoted to the collection of evidence regarding allegations that the Church participated in psychological coercion that caused both mental and physical injuries to a number of its members.[80] The defendants posted much of the information that they had collected on a computer bulletin board service.[81] The Church charged that some of the information posted on the Internet included the same type of Advanced Technology materials at issue in *Lerma*.[82] In *F.A.C.T.Net*, the court found that the documents were "widely known outside the Church through multiple sources," including the Internet.[83] Thus, the court concluded that the Colorado trade secret statute did not cover these materials.[84]

The third of the *Scientology Cases*, *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*,[85] involved a former member of the Church, Dennis Erlich, who, after his departure, became highly critical of the Church.[86] Erlich posted his criticisms to a "Usenet newsgroup"[87] devoted to the discussion of issues related to the Church of

---

77. *Id.*

78. 901 F. Supp. 1519 (D. Colo. 1995).

79. Although not named as an individual defendant in this case, Arnoldo Lerma was a director of F.A.C.T.Net and the Virginia suit, *Religious Tech. Ctr. v. Lerma*, 897 F. Supp. 260 (E.D. Vir. 1995), arose out of events related to the actions at issue in this case.

80. *F.A.C.T.Net*, 901 F. Supp. at 1522. A related area of inquiry for the defendants in this case was the legitimacy of the Church's status as a tax exempt religious organization. *Id.* at 1521.

81. *F.A.C.T.Net*, 901 F. Supp. at 1522. A "bulletin board service" is:

> A teleconferencing system often run on a dedicated computer for use by enthusiasts who can connect their personal computers by means of modems and telephone lines or network connections. The bulletin board allows its users to post notices that they wish seen by other users on a variety of topics, to read the notices left by previous users, and to download software and information for use on their own systems.

Dictionary of Computing 55 (4th ed. 1996).

82. *F.A.C.T.Net*, 901 F. Supp. at 1522.

83. *Id*. at 1527.

84. *Id.*

85. 923 F. Supp. 1231 (N.D. Cal. 1995).

86. *Id.* at 1239.

87. A "newsgroup" is:

> A forum on the Internet for threaded discussions on a specified range of subjects. A newsgroup consists of articles and follow-up posts--all of which are (supposed to be) related to the specific subject names in the original article's subject line--constitutes a thread. Each newsgroup has a name that consists of a series of words, separated by periods, indicating the newsgroup's subject in terms of increasingly narrow categories, such as rec.crafts.textiles.needlework.

MICROSOFT PRESS, COMPUTER DICTIONARY 329 (3rd ed. 1997). "Usenet" is "a set of thousands of

Scientology.[88] The Church alleged that some of Erlich's postings contained proprietary writings by the Church's founder.[89] Unlike the information posted by the defendants in *F.A.C.T.Net*, not all of the information had been posted on the Internet.[90] Like the courts in the two cases before it, the district court in *Netcom* found that the Church had taken reasonable steps to protect its information as trade secrets.[91] The court also noted that mere disclosure of the information on the Internet was not a sufficient test of whether the information was "generally known."[92] The court gave great weight to the fact that by posting the information on the Internet more than twenty-five million people could have viewed the documents,[93] causing them to lose their status as trade

---

newsgroups . . . distributed via the Internet [and distributed through its own network prior to the advent of the Internet]." DOUGLAS A. DOWNING, ET AL., DICTIONARY OF COMPUTER AND INTERNET TERMS 489 (6th ed. 1998).

88. *Netcom*, 923 F. Supp at 1239.

89. *Id.*

90. *Id.* at 1240. In fact, Erlich claimed that one of the documents he posted he received anonymously through the mail. *Id.*

91. *Id.* at 1253-54. Among the reasonable steps noted by the court were the 1) use of locked cabinets and safes; 2) logging and identification of the materials; 3) availability at only a limited number of sites; 4) electronic sensors attached to the documents; 5) locked briefcases during transportation; 6) alarms; 7) photo identification for personnel; and 8) confidentiality agreements for anyone given access to the information. *Id.* at 1254.

92. *Id.* at 1255. The court cited Gates Rubber Co. v. Bando Chem. Indus., 9 F.3d 823, 848-49 (10th Cir. 1993). In *Gates* the court found that information retained its trade secret status even though it had been disclosed at a hearing. *Id.* The *Gates* court noted the significance of the plaintiffs' continuing intent to maintain the information's secrecy by acting to seal the record of the hearing. *Id.* However, the court in *Netcom* appears to cite this passage merely for the proposition that there is sometimes a need in judicial proceedings to view documents filed both under seal and not under seal. The viewing of these documents in the context of a judicial proceeding should not destroy the trade secret status. The court does not make the important caveat that the trade secret status does not remain when the documents "were somehow made generally available to the public during the period they were unsealed, such as by publication." *Netcom*, 923 F. Supp. at 1255.

93. By so holding, the court implicitly rejects one argument which suggests that just because something has been made available to a large group of people via the Internet does not necessarily mean that a large group of people have actually seen or read the material on-line. According to this argument, therefore, injunction would seem the most viable alternative because the sooner the information is retrieved from the Web, the less likely others have retransmitted it, thereby causing the information to lose its status as a trade secret.

According to Milgrim, the court eventually reconsidered its holding with respect to the loss of trade secret status at the point the information is published on the Web. Milgrim found that:

> the *Netcom* court rejected its initial holding that a work loses its trade secret status once it is posted on the Internet as an "overly broad generalization." Instead, it favored more critical inquiry and discerned that "[t]he question of when a posting causes the loss of trade secret status requires a review of the circumstances surrounding the posting and considerations of the interests of the trade secret owner, the policies favoring competition and the interests, including first amendment rights, of *innocent* third parties who acquire information off the Internet." Nonetheless, the court expressed a view that in most cases Internet postings should be treated in the same manner as information published in traditional materials such as

secrets.[94] The court also addressed the problem of intentional release of trade secrets on the Internet for the specific purpose of destroying the trade secret protection and thus escaping liability.[95] The court stated that when an individual, such as the defendant in this case, is not a party to the initial misappropriation, public disclosure can be claimed as a defense to any trade secret violation suit brought against the individual.[96]

The most recent pronouncement on the issue of loss of trade secret protection through mass dissemination on the Internet came from a federal judge in the Eastern District of Michigan.[97] In *Ford Motor Company v. Lane*,[98] the automaker brought suit against the operator of an Internet site[99] for allegedly posting Ford's proprietary information on the Internet. Before any of Ford's potentially proprietary information appeared on Lane's site, Ford objected to the use of the trademarked word "Ford" in the Web site's[100] domain name,[101] and blocked Lane from having access to its press releases on the Web.[102] The tension escalated between the two parties when Lane sent Ford a letter indicating that he had obtained several "sensitive"[103] Ford documents, which came from a source within the

---

magazines and newspapers.

MILGRIM, *supra* note 4, at § 17.03.

94. 923 F. Supp. at 1256. Further, the court held:

> While the Internet has not reached the status where a temporary posting on a newsgroup is akin to publication in a major newspaper or on a television network, those with an interest in using the Church's trade secrets to compete with the Church are likely to look to the newsgroup. Thus, posting works to the Internet makes them 'generally known' to the relevant people--the potential 'competitors' of the Church.

Id.

95. *Id.* Judge Whyte commented that "[t]he Court is troubled by the notion that any Internet user, including those using 'anonymous remailers' to protect their identity, can destroy valuable intellectual property rights by posting them over the Internet, especially given the fact that there is little opportunity to screen postings before they are made." *Id.*

96. *Id.* at 1256. *See also* Underwater Storage, Inc. v. United States Rubber Co., 371 F.2d 950, 955 (D.C. Cir. 1966) (holding that "[o]nce the secret is out, the rest of the world may well have a right to copy it at will; but this should not protect the misappropriator or his privies.")

97. For additional background see *supra* notes 10-16 and accompanying text.

98. 67 F. Supp. 2d 745 (E.D. Mich. 1999).

99. Robert Lane, *BlueOvalNews.com, at* http://www.blueovalnews.com (last visited Nov. 13, 1999).

100. At the time, the domain name of Lane's site was "fordworldnews.com." 67 F. Supp. 2d at 747.

101. A "domain name" is the "address of a network connection that identifies the owner of that address in a hierarchical format: *server.organization.type*. For example, www.whitehouse.gov identifies the Web server at the White House, which is part of the U.S. government." MICROSOFT PRESS, COMPUTER DICTIONARY 158 (3rd ed. 1997).

102. *Id.*

103. The "sensitive" documents included unreleased photographs of the new Ford Thunderbird. *Id.*

company.[104] Lane further threatened to publish materials[105] on his Web site that the company would find "disturbing."[106] Although Lane initially agreed to obtain the automaker's approval before posting any documents on his site, he later went back on his agreement and posted a story about problems with the Ford Mustang Cobra engine.[107] This story quoted internal Ford documents that Lane had received from inside sources.[108] Over the next couple of weeks, Lane published several other articles on his Web site containing information that he obtained from confidential[109] sources within the corporation.[110] The very day that Ford filed its complaint, the court granted the company's request for a temporary restraining order against Lane blocking him from disclosing any more of the company's internal documents.[111] Lane accepted the court's order on every ground[112] except the restriction from "using, copying or disclosing

---

104. *Id.*

105. In fact, even after Judge Edmunds' final ruling in the case, Lane has continued to post Ford documents on his site, including the specifications for a line of diesel engines that the company intends to build. Justin Hyde, *Ford Appeals Web Site Decision*, AP ONLINE, Oct. 18, 1999.

106. 67 F. Supp. 2d at 747.

107. *Id.*

108. *Id.*

109. *Id.* The court noted that Lane did not know the identity of his informants. *Id.*

110. *Id.* The court included a detailed laundry list of confidential Ford documents that Lane posted on his Web site:

> On July 27, 1999, Lane published information from another document that Lane received from an anonymous source, a document entitled "Powertrain Council Strategy & Focus." This was an internal Ford memo containing Ford's strategies relating to fuel economy, vehicle emissions through the year 2010, and powertrain technology advances. Lane also published a Ford engineering blueprint on his site, and stated that he planned to offer other blueprints for sale. In addition, Lane stated that he possessed other confidential Ford documents. When Ford advised Lane that the Company intended to file a lawsuit and to seek an injunction against him, Lane responded by posting approximately forty Ford documents online, including materials with high competitive sensitivity.

Id. (citations omitted).

111. *Id.* at 748.

112. The court's order provided that:

> A. Defendant is restrained from destroying, despoiling or electronically deleting or erasing documents in his possession originated by or for Ford Motor Company.
>
> B. Defendant is ordered to file with the Court, and serve upon Ford Motor Company, within ten (10) days, a sworn statement (1) identifying with particularity all documents within his possession, custody or control which were originated by or for Ford Motor Company, (2) the source (by name or description) of each document, and (3) provide details as to how defendant Robert Lane acquired each document.
>
> C. Defendant is restrained from (1) using, copying or disclosing any internal document of Ford Motor Company (including the information contained therein), (2) committing any acts of infringement of Ford Motor Company's copyrights, including unpublished works known by defendant Robert Lane to have been prepared by a Ford Motor Company employee within the scope of his or her employment, or specially ordered or commissioned by Ford Motor Company, if not an employee, (3) interfering with Ford's contractual relationship with its

any internal document of Ford Motor Company."[113]

When the court considered Lane's response, it sided with the Web site operator and refused to enter a preliminary injunction against him with respect to the internal Ford documents.[114] In doing so, the court held that even though Lane possibly violated the Michigan Uniform Trade Secrets Act, the use of an injunction would violate the prior restraint doctrine and thus the First Amendment.[115]

The Court cited *Reno v. American Civil Liberties Union*[116] to support the proposition that the First Amendment applies to speech on the Internet.[117] The court then reviewed both *Near*[118] and the *Pentagon Papers Case*[119] to demonstrate the high threshold that plaintiffs seeking an injunction must show in order to overcome the free speech defense.[120] The court specifically rejected any contention that information transmitted to the general populace by way of the Internet should be analyzed differently than traditional print media.[121] The court, cognizant of the possibility that Lane's behavior was an attempt to "extort concessions or privileges from Ford, by threatening to sell blueprints or other confidential documents," indicated that Ford may have a proper remedy through criminal prosecution, though not civil injunction.[122]

---

employees by soliciting Ford employees to provide Ford trade secrets or other confidential information.

Id. at 748-49.

113. *Id.* at 749.

114. *Id.* at 753.

115. *Id.*

116. 521 U.S. 844 (1997). See *supra* notes 52-60 and accompanying text for a discussion of *Reno v. American Civil Liberties Union.*

117. 67 F. Supp. 2d at 751.

118. 283 U.S. 697 (1931). For a discussion of *Near v. State of Minnesota*, see *supra* notes 37-43 and accompanying text.

119. 403 U.S. 713 (1971). For a discussion of *New York Times Co. v. United States*, see *supra* notes 45-51 and accompanying text.

120. 67 F. Supp. 2d at 751.

121. *Id.* at 752-53. The court rationalized its rejection as follows:

> While it may be true that publication on the Internet is subject to fewer editorial restraints than The New York Times, Business Week, or The Washington Post, the material here is no more inflammatory than the anti-semitic tabloid at issue in *Near.* And while the reach and power of the Internet raises serious legal implications, nothing in our jurisprudence suggests that the First Amendment is circumscribed by the size of the publisher or his audience.

Id.

122. *Id.* at 753.

II. THE FAILINGS OF TRADITIONAL APPROACHES TO TRADE SECRET MISAPPROPRIATION AND THE INTERNET

A. The Problem

As *Reno,* the *Scientology Cases*, and *Lane* all demonstrate, in cases where the Internet and the First Amendment have clashed, courts have granted great deference to the primacy of the First Amendment.[123] With regard to misappropriation of trade secrets, the *Scientology Cases* and the *Lane* court represent the two schools of thought on balancing the interests of the trade secret holder and the Internet user. The *Scientology* courts take the view that once a trade secret is available on the Internet, it is by definition no longer secret.[124] Although the courts in the *Scientology Cases* quickly pointed out that this approach does not shield the *initial* misappropriator from liability, the approach fails insofar as it provides no protection from subsequent use by competitors who have no connection to the initial misappropriation.

Because of the logical inconsistencies created by the *Scientology* courts, the *Lane* court wisely avoided the issue of the potential destruction of trade secret protection.[125] Ford's interest in protecting its trade secrets rests not on a fear that its proprietary documents might fall into the hands of car enthusiasts. Rather, the real danger exists in the possibility that its major competitors in the auto industry might come to possess such information. If the *Lane* court had ruled that once disseminated on the Internet, the Ford documents were no longer considered trade secrets, then any of Ford's competitors could have used them with impunity.

The *Lane* approach keeps open the possibility that criminal sanctions may provide the originator with a remedy; however, civil injunctions or any other form of prior restraint most likely will not succeed.[126] The *Lane*

---

123. Judge Edmunds perhaps stated it best in *Lane*:

> In the realm of law, we are only beginning to grapple with the impact of the communications revolution, and this case represents just one part of one skirmish--a clash between our commitment to the freedom of speech and the press, and our dedication to the protection of commercial innovation and intellectual property. In this case, the battle is won by the First Amendment.

67 F. Supp. 2d at 746.

124. *See supra* notes 25-26.

125. Although the court does successfully avoid this problem, it is perhaps correct to ask why the court failed to cite *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470 (1974). *See supra* note 26. The other courts that have addressed this problem have done so with the notion that once a document is released to the entire world it loses its trade secret status. It is unclear where the *Lane* court stands on this point.

126. *Lane*, 67 F. Supp. 2d at 753.

court does not answer the most crucial question—what happens if any of Ford's competitors attempt to use the material that was posted on Lane's Web site. The court left open the possibility of both civil and criminal recovery action against Lane, but the *Lane* opinion provides no guidance on the issue of potential liability for secondary users of the information.[127]

B. Remedies

If courts will not consider enjoining misappropriators from posting the fruits of their acts on the Internet, holders of trade secrets can protect themselves only through the various remedies available after their documents appear on the Internet. The two major categories of remedies are civil damages and criminal sanctions.[128]

The realm of civil damages[129] for misappropriation of trade secrets makes available to the aggrieved party three methods of calculation: 1) any direct loss incurred by the trade secret owner; 2) the gain of the misappropriator; and 3) a reasonable royalty for the use of the secret.[130]

An aggrieved party may pursue criminal sanctions at both the state and federal levels. State sanctions are usually provided for under the state's version of the Uniform Trade Secret Act.[131] Federal criminal sanctions

---

127. This does not appear to have been an issue before the court.

128. It goes without saying, of course, that companies can, and often do, settle out of court. In March 1998, Texas Instruments agreed to settle a lawsuit brought by 3Dlabs Inc. for allegedly posting proprietary information owned by 3Dlabs on the Internet in violation of California's trade secret law. *TI, 3Dlabs Settle Dispute OverTtrade Secrets*, DALLAS MORNING NEWS, Mar. 27, 1998, at 11D.

129. Although the specifics vary from state to state, generally a plaintiff pursuing a cause of action for misappropriation of trade secrets must show: 1) that the information is protectable as a trade secret; 2) that the owner took reasonable steps to ensure secrecy; and 3) that the defendant acted improperly in acquiring the information. *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475 (1974); *see also* Rothschild v. Ford Motor Co., 2 F. Supp. 2d 941, 950 (E.D. Mich. 1998) ("In Michigan, to succeed on a claim for misappropriation of a trade secret, a plaintiff must prove the following elements by a preponderance of the evidence: 1) the existence of a trade secret; 2) its acquisition in confidence; and 3) the defendant's unauthorized use of it.").

130. Lambrecht, *supra* note 35, at 358.

131. Remedies under the Uniform Trade Secrets Act include damages:

> (a) Except to the extent that a material and prejudicial change of a 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. Damages can include both the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss. In lieu of damages measured by any other methods, the damages caused by misappropriation may be measured by imposition of liability for a reasonable royalty for a misappropriator's unauthorized disclosure or use of a trade secret.
>
> (b) If willful and malicious misappropriation exists, the court may award exemplary damages in an amount not exceeding twice any award made under subsection (a).

U.T.S.A. § 3 (1985). There also exists the potential for the award of reasonable attorneys fees if

include the Economic Espionage Act,[132] the Federal Trade Secrets Act,[133] and the Mail[134] and Wire Fraud[135] statutes. Although prosecutions under the Economic Espionage Act and the Federal Trade Secrets Act occur infrequently, federal prosecutors have utilized them with increasing regularity.[136]

However, these remedies all suffer from the same limitation in that they can only discourage people from leaking the information in the first place. As *Lane* demonstrated, oftentimes no one knows who originally disclosed the information.[137] Likewise, neither the state nor the federal statutes expressly address how to protect misappropriated information that enters the public domain by virtue of its mass dissemination and what recourse the originator of the information has to prevent other companies from using the information in a meaningful way.

III. PROPOSED LIABILITY TO PROTECT TRADE SECRETS FROM KNOWING SUBSEQUENT USE

As previously demonstrated, current trade secret protection in the Internet age falls short in two serious respects. First, the Internet now makes ideas, business designs, and proposals subject to mass disclosure no matter how much an individual or business tries to protect those secrets. Second, the nature of the Internet knows no state boundaries, and rarely will theft of such secrets constitute a uniquely *intra*state problem. Therefore, the federalization of trade secret laws based on the Uniform Trade Secret Act would serve as a much-needed first step by ensuring that original misappropriators of trade secrets are punished consistently across the country, regardless of the jurisdiction in which the initial theft took place.[138]

The new federal trade secrets legislation must provide protection for companies who lose their trade secrets when a misappropriator or other

---

"willful and malicious misappropriation exists." U.T.S.A. § 4(iii) (1985).

132. 18 U.S.C. § 1831 (Supp. IV. 1998).

133. 18 U.S.C. § 1832 (Supp. IV. 1998).

134. 18 U.S.C. § 1341 (1994).

135. 18 U.S.C. § 1343 (1994).

136. For example, in September 1999, the United States Attorney for the Eastern District of Wisconsin announced the indictment of Matthew Lange, a former employee of Replacement Aircraft Parts Co. Inc., who allegedly sold proprietary drawings owned by the corporation over the Internet. The federal government charged Lange under the Economic Espionage Act. Gretchen Schuldt, *Man Charged With Selling Trade Secrets: Ex-draftsman Allegedly Used Net in an Effort to Deliver Firm's Information*, MILWAUKEE J. SENTINEL, Sept. 9, 1999, at 1.

137. *See supra* notes 13, 109 and accompanying text.

138. *See generally*, Lao, *supra* note 27.

third party discloses the information on the Internet or through other forms of mass media. Furthermore, this new legislation should broadly encompass not only the technologies that we know now, but those that may develop in the near future.

Several amendments to the Uniform Trade Secrets Act would ensure consistent punishment for misappropriation and protect companies that lose trade secrets. The Amended[139] Uniform Trade Secrets Act would read:

> Section 1, Definitions:
>
> As used in this [Act], unless the context requires otherwise:
>
> (1) "Improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means;
>
> (2) "Misappropriation" means:
>
> (i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or
>
> (ii) disclosure or use of a trade secret of another without express or implied consent by a person who
>
> (A) used improper means to acquire knowledge of the trade secret; or
>
> (B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was
>
> (I) derived from or through a person who had utilized improper means to acquire it;
>
> (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
>
> (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
>
> (C) before a material change of his [or her] position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.
>
> (3) "Person" means a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government,

139. Proposed amendments are noted in *italics*.

governmental subdivision or agency, or any other legal or commercial entity.

(4) "Trade secret" means information, including a formula, pattern, 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.

(5) *"Mass dissemination" means the release of information by means of wire, radio, television, Internet, or similar technologies capable of reaching two or more persons at separate locations simultaneously.*

and in Section 3, Damages:

(a) Except to the extent that a material and prejudicial change of a 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. Damages can include both the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss. In lieu of damages measured by any other methods, the damages caused by misappropriation may be measured by imposition of liability for a reasonable royalty for a misappropriator's unauthorized disclosure or use of a trade secret.

(b) *A complainant is also entitled to recover damages for the unauthorized use of information that no longer qualifies as a trade secret because of the intentional mass dissemination of the trade secret by a misappropriator or any person who subsequently knows or has reason to know that information was disclosed by improper means.*

(C) If willful and malicious misappropriation exists, the court may award exemplary damages in an amount not exceeding twice any award made under subsection (a).

Applied to the facts of the *Lane* case, this new legislation would ensure that companies like Ford have protection against use of information gained by mass dissemination for a competitive advantage. For example, under

this new legislation, if one of Ford's competitors used the information that Lane posted on his Web site, and that competitor knew or had reason to know that the information constituted a trade secret belonging to Ford, then Ford could recover damages against that company. Given the amount of attention that *Ford Motor Co. v. Lane* has received in both the industry and the national press, proving the knowledge requirement would not serve as an obstacle in this hypothetical case.

CONCLUSION

By keeping the Internet a largely unregulated marketplace for the exchange of ideas, courts and legislatures have hoped that the marketplace will solve most potential injustices itself, and have left society to tolerate the harms that go unchecked. The initial challenges to this laissez-faire attitude to the Internet have resulted from regulations like the Communications Decency Act.[140] Other proposed regulations include ways of making e-commerce less susceptible to fraud and abuse by scheming entrepreneurs.[141] The history of trade secret protection demonstrates that it has developed as a reaction to the needs of a changing marketplace. The law must take the next step in that evolution and protect the rights of intellectual property owners whose ideas may not have originated on the Web, but who face a threat from the release of their property information on the World Wide Web.

Matthew R. Millikin[*]

---

140. See notes 52-55 and accompanying text.

141. *See generally* Bick, *supra* note 6.

* A.B. (1998), Washington University in St. Louis; J.D. Candidate (2001) Washington University School of Law. I would like to thank Dana for her thoughts and comments and for helping me polish the final draft.