University of Florida Levin College of Law
UF Law Scholarship Repository

UF Law Faculty Publications | Faculty Scholarship

2007

Saving Trade Secret Disclosures on the Internet Through Sequential Preservation

Elizabeth A. Rowe
University of Florida Levin College of Law, rowe@law.ufl.edu

Follow this and additional works at: https://scholarship.law.ufl.edu/facultypub

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

Recommended Citation

Elizabeth A. Rowe, *Saving Trade Secret Disclosures on the Internet Through Sequential Preservation*, 42 Wake Forest L. Rev. 1 (2007), *available at http://scholarship.law.ufl.edu/facultypub/62*

This Article is brought to you for free and open access by the Faculty Scholarship at UF Law Scholarship Repository. It has been accepted for inclusion in UF Law Faculty Publications by an authorized administrator of UF Law Scholarship Repository. For more information, please contact kaleita@law.ufl.edu.

WAKE FOREST LAW REVIEW

VOLUME 42 2007 NUMBER 1

ARTICLES

SAVING TRADE SECRET DISCLOSURES ON THE INTERNET THROUGH SEQUENTIAL PRESERVATION

*Elizabeth A. Rowe**

TABLE OF CONTENTS

I. INTRODUCTION 2
A. The Power of the Internet 3
B. Legal Complications 5
C. The Article's Mission 5
II. TRADE SECRET LAW BACKGROUND 7
A. Lawful Use of Another's Trade Secrets 8
B. Equitable Nature of Trade Secret Law 9
III. SUMMARY OF RELEVANT CASE LAW 10
A. The Church of Scientology Cases 11
B. *DVD Copy Control Ass'n v. Bunner* 12
C. *United States v. Genovese* 13
IV. ANALYZING THE THIRD PARTY PROBLEM 14

* Assistant Professor of Law, University of Florida, Levin College of Law. I am very grateful to Pamela Samuelson and Andrea Matwyshn for their comments on earlier drafts of this Article. I also thank, for their comments, participants at the 2006 Intellectual Property Scholars Conference held at the University of California Berkeley Boalt Hall School of Law and students in the IP Scholarship Seminar at Boalt Hall. Luke Napodano and Dana Sellers provided valuable research assistance. Finally, I acknowledge the editors of the *Wake Forest Law Review* for their excellent work and professionalism.

A. Is it a Trade Secret? 15
1. Is a Posting on the Internet "Generally Known"? 17
2. Is a Posting on the Internet "Readily Ascertainable"? 19
B. Is it Misappropriation? 21
V. OTHER OBSTACLES TO TRADE SECRET PROTECTION 23
A. First Amendment 24
B. Fourth Amendment 25
C. Patent Law 26
VI. ASSISTANCE FROM ATTORNEY-CLIENT PRIVILEGE CASES 27
A. *In re Grand Jury Proceedings Involving Berkley & Co.* 28
B. *Resolution Trust Corp. v. Dean* 28
C. *Smith v. Armour Pharmaceutical Co.* 28
D. *United States ex rel. Mayman v. Martin Marietta Corp.* 29
VII. THE SEQUENTIAL PRESERVATION MODEL 29
A. Threshold Issue—Establish Trade Secret Status 30
B. The Three Factors 31
1. Time and Action 32
2. Extent of Disclosure 33
3. Recipient's Reason to Know the Information Was a Trade Secret 34
VIII. SUMMARY AND APPLICATION OF THE SEQUENTIAL PRESERVATION MODEL 38
A. Theoretical Checklist of the Model 38
B. Application with Case Examples 39
1. *Religious Technology Center v. Lerma* 39
2. *DVD Copy Control Ass'n v. Bunner* 40
3. *O'Grady v. Superior Court* 41
4. *United States v. Genovese* 43
IX. REMEDIES 44
X. CONCLUSION 46

I. INTRODUCTION

Soft Corporation is a leading maker of software and operating systems. It undertakes great measures to protect the secrecy of its new products under development, plans to launch new products, technical product specifications, and product source codes, all of which it considers company trade secrets. A disgruntled employee, John Sneaky, one of the few persons with access to the source code to Soft's soon to be released operating system, Win100, posts the source code (labeled "Confidential—Soft Proprietary Information") on a members-only Web site critical of Soft, Softsucks.com.

Soft discovers the posting within six hours of its appearing on the site, and after informing the site operator that the information is a stolen Soft trade secret, it is immediately removed. Prior to its removal, however, Sam Quickbuck had downloaded the source code. When he realized the next day that the source code was no longer

available on Softsucks.com he decided to capitalize on the opportunity.

He posted a notice on his Web site offering the code for sale: "Win100 source code, original, (jacked from inside) available for sale. Get it here before it's even released and stick it to Soft. If you wanna buy it ($50), I'll give you a password to download it."

Soft sues Quickbuck for misappropriation of trade secrets, seeking a preliminary injunction to prohibit his use and sale of the source code. After a hearing, the court denies relief to Soft, reasoning that, despite Soft's best efforts to keep the source code secret, it has lost its trade secret status by virtue of it appearing on the Internet and that Quickbuck cannot be enjoined from using it. Soft now faces widespread use of its source code by other competitors and a resulting loss of market share for its Win100 operating system. As a result of the ruling, it can no longer claim the source code as a trade secret.

This hypothetical[1] introduces the problem and accompanying questions tackled by this Article. When, for instance, an employee discloses an employer's trade secrets to the public over the Internet, does our current trade secret framework appropriately address the consequences of that disclosure? What ought to be the rule that governs whether the trade secret owner has lost not only the protection status for the secret, but also any remedies against use by third parties? Should the ease with which the Internet permits instant and mass disclosure of secrets be taken into consideration in assessing the fairness of a rule that calls for immediate loss of the trade secret upon disclosure?

A. The Power of the Internet

Although trade secret owners have always risked disclosure of their highly sensitive and confidential information, today the Internet magnifies that risk exponentially.[2] It facilitates complete

---

1. This hypothetical is loosely based on United States v. Genovese, 409 F. Supp. 2d 253 (S.D.N.Y. 2005) (discussed *infra* Parts III.C and VIII.B.4).

2. The Internet has become an important part of daily life, connecting approximately 800 million people to a global network. *See* Xuan-Thao N. Nguyen & Jeffrey A. Maine, *Taxing the New Intellectual Property Right*, 56 HASTINGS L.J. 1, 4-5 (2004). Over fifty percent of all households are connected to the Internet. *See* Daniel W. Park, *Trade Secrets, the First Amendment, and Patent Law: A Collision on the Information Superhighway*, 10 STAN. J.L. BUS. & FIN. 46, 47 (2004). Its presence has changed the way in which the world does business and its impact on the economy is far reaching. *See generally* Andrea M. Matwyshyn, *Of Nodes and Power Laws: A Network Theory Approach to Internet Jurisdiction Through Data Privacy*, 98 NW. U. L. REV. 493, 499-500 (2004) (discussing trends in the Internet economy).

destruction of a trade secret in an instant, and the law strips the trade secret owner's power to control or contain the damage. Even when the party posting[3] the information may not have intended to cause harm to the trade secret owner, the injury can be no less devastating.[4] One court, while refusing to enjoin publication of a company's trade secrets on First Amendment grounds, nevertheless noted the shift in balance of power made possible by the Internet: "With the Internet, significant leverage is gained by the gadfly, who has no editor looking over his shoulder and no professional ethics to constrain him. Technology blurs the traditional identities of David and Goliath."[5]

Unlike other mass media, which generally have staff who decide what materials will be published, the Internet has no such filter. Any person sitting at a computer can post information onto the Internet, resulting in immediate and irreparable harm. One judge captured the problem in these words:

> The court is troubled by the notion that any Internet user . . . 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. Nonetheless, one of the Internet's virtues, that it gives even the poorest individuals the power to publish to millions of readers can also be a detriment to the value of intellectual property rights. The anonymous (or judgment proof) defendant can permanently destroy valuable trade secrets, leaving no one to hold liable for the misappropriation.[6]

The power of the Internet has added complexity to the archetypal two person misappropriation framework traditionally encountered in trade secret law. Misappropriation claims often arise in an employment context, for instance, where an employee

---

3. This Article often refers to trade secret information being posted on the Internet. Posting "consists of directly placing material on or in a Web site, bulletin board, discussion group, newsgroup, or similar Internet site or 'forum,' where it will appear automatically and more or less immediately to be seen by anyone with access to that forum." O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 91 (Ct. App. 2006). It therefore allows direct self-publication of information, or one may also send information to a site, the owners or moderators of which make decisions about what to post. *See id.*

4. *See* Jerome Stevens Pharms., Inc. v. FDA, 402 F.3d 1249, 1254 (D.C. Cir. 2005) (reversing district court dismissal, holding that FDA could be liable for misappropriation of trade secrets where it posted plaintiff's trade secrets on its Web site for five months).

5. Ford Motor Co. v. Lane, 67 F. Supp. 2d 745, 753 (E.D. Mich. 1999).

6. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 923 F. Supp. 1231, 1256 (N.D. Cal. 1995) (citations omitted).

leaves for new employment with a competitor and takes the former employer's trade secrets. The employer, or trade secret owner, can state misappropriation claims against the former employee and often the new employer.[7] In the case of an Internet disclosure, however, the current law suggests that there is no claim against third parties who discover the information, and thus no feasible way to contain the dissemination of the trade secret.[8]

B. Legal Complications

Further complicating the situation is that trade secret law only protects secret information. Therefore, it is difficult to argue that information which appears on the World Wide Web, and which is admittedly no longer secret, can retain trade secret protection. Yet, trade secret law is also equitable and intended to regulate the morality of the business world. Why then should we create incentives for inappropriate and unethical conduct by permitting a single individual's disclosure of a trade secret to destroy that which has been so well guarded by a trade secret owner? A sound analysis of this complicated problem calls for a balancing of the right of the trade secret owner to preserve its trade secret information, the right of an innocent independent third party to use information found in the public domain, and the policies favoring fair competition.

A view from outside trade secret law also provides guidance for and against retention of trade secret status after an Internet disclosure. On one hand, constitutional law and patent law considerations lean toward prohibiting restrictions on the use of publicly available information. On the other hand, attorney-client privilege cases, in analogous circumstances, support preservation. Some of these areas of law provide further insight into analogous incentives for wrongdoing.

C. This Article's Mission

Several commentators have identified the general problem posed by trade secret disclosures over the Internet, but none have analyzed the problem with the same depth and approach used in this Article.[9] Moreover, much of the literature addresses First

---

7. *See, e.g.*, Elizabeth A. Rowe, *When Trade Secrets Become Shackles: Fairness and the Inevitable Disclosure Doctrine*, 7 TUL. J. TECH. & INTELL. PROP. 167, 176-80 (2005) (detailing several representative cases).

8. *See infra* Part IV.

9. *See, e.g.*, Victoria A. Cundiff, *Trade Secrets and the Internet: Preventing the Internet from Being an Instrument of Destruction*, *in* 11TH ANNUAL INSTITUTE ON INTELLECTUAL PROPERTY LAW 347, 355-59 (PLI Intellectual Property, Course Handbook Series No. 842, 2005); Park, *supra* note 2; Bruce T. Atkins, Note,

Amendment challenges, with top scholars arguing from both ends of the spectrum about the role of the First Amendment in trade secret cases.[10] I enter the discussion from a different perspective, ultimately landing somewhere near the middle of the spectrum between those who would extend broad First Amendment protection to anyone who posts trade secrets on the Internet and those who would protect the status of trade secrets over First Amendment and Internet challenges.

My objective is to articulate a workable test that courts can use when deciding whether a trade secret that has been disclosed on the Internet can still be preserved as secret, regardless of whether there is or is not a First Amendment defense in the case. This Article critically examines relevant trade secret doctrines, dissecting assumptions and methodically examining whether it is possible to retain trade secret protection in the face of a disclosure over the Internet. It also draws guidance from other areas of law, and together this critical examination informs what I coin a "sequential preservation model." Accordingly, this model is a unique and novel approach to the problem.[11]

Trading Secrets in the Information Age: Can Trade Secret Law Survive the Internet?, 1996 U. ILL. L. REV. 1151; Ryan Lambrecht, Note, *Trade Secrets and the Internet: What Remedies Exist for Disclosure in the Information Age?*, 18 REV. LITIG. 317 (1999); Matthew R. Millikin, Note, *www.misappropriation.com: Protecting Trade Secrets After Mass Dissemination on the Internet*, 78 WASH. U. L.Q. 931 (2000).

10. For those favoring trade secret protection over First Amendment rights, see, for example, Andrew Beckerman-Rodau, *Prior Restraints and Intellectual Property: The Clash Between Intellectual Property and the First Amendment from an Economic Perspective*, 12 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1, 5 (2001); Richard A. Epstein, *Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalism*, 52 STAN. L. REV. 1003, 1035-46 (2000); Franklin B. Goldberg, Recent Development, Ford Motor Co. v. Lane, 16 BERKELEY TECH. L.J. 271 (2001); Adam W. Johnson, *Injunctive Relief in the Internet Age: The Battle Between Free Speech and Trade Secrets*, 54 FED. COMM. L.J. 517 (2002); Atkins, *supra* note 9.

For those advocating First Amendment rights over trade secret protection, see, for example, David Greene, *Trade Secrets, the First Amendment, and the Challenges of the Internet Age*, 23 HASTINGS COMM. & ENT. L.J. 537 (2001); Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147, 229-31 (1998); Eugene Volokh, *Freedom of Speech and Intellectual Property: Some Thoughts After* Eldred, 44 Liquormart, *and* Bartnicki, 40 HOUS. L. REV. 697, 739-48 (2003).

11. Attempts to address the problem effectively must take into consideration the various issues identified in this Article and tread a delicate balance, being ever mindful of the goals and constraints of trade secret law and its interaction with other areas of law. To do otherwise may risk undermining the general principles of trade secret law. The state of Nevada, for instance, enacted legislation in 2001 that provides that a trade secret disseminated on

The sequential preservation model calls for a threshold determination of whether the information was entitled to trade secret protection *before* the Internet disclosure. If and only if it was, then a three factor test will be used to evaluate whether it retained the trade secret status and was ultimately misappropriated. Those three factors are (1) the amount of time the information was exposed on the Internet and the promptness of any action by the trade secret owner to have the information removed, (2) the extent of the disclosure, and (3) the likelihood that the recipient knew the information was a trade secret.

Part II of the Article provides a background summary of trade secret law. Part III summarizes the relevant case law in this area. Part IV analyzes the third party disclosure problem. Insights from other areas of law are provided in Parts V and VI. Part VII presents the proposed model and the three factor test for analyzing these cases, followed by a theoretical summary and application of the model in Part VIII. Part IX addresses remedies available to a trade secret owner, and the Article concludes in Part X.

II. TRADE SECRET LAW BACKGROUND

Unlike the other areas of intellectual property (copyrights, patents, and trademarks), there is no federal statutory law governing trade secrets. Rather, trade secrets are protected by state law. Most states have adopted the Uniform Trade Secrets Act ("UTSA"), and, as a result, there is some uniformity in defining trade secrets and trade secret misappropriation.[12] The states that have not adopted the UTSA tend to rely on common law based on the *Restatement of Torts*.[13] Finally, and more recently, the *Restatement (Third) of Unfair Competition*[14] also addresses trade secrets.[15] Its rules apply to actions under both the UTSA and the

---

the Internet shall remain a trade secret if the owner obtains an injunction to have it removed within a "reasonable time." NEV. REV. STAT. ANN. § 600A.055 (LexisNexis 2005). For a host of reasons discussed *infra*, this legislation is not well grounded. *See infra* Parts V, VI, and VIII.

12. It has been adopted in whole or part by forty-four states and the District of Columbia.

13. *See* MICHAEL A. EPSTEIN, EPSTEIN ON INTELLECTUAL PROPERTY § 1.02, at 1-4 (4th ed. Supp. 2005). The UTSA provides broader protection than the *Restatement* in that it does not require that a trade secret be in use to be protected, and it protects negative information. A negative trade secret is the knowledge of what not to do or what does not work, a lesson learned from a certain process or research and development effort that failed. *See* JAMES POOLEY, TRADE SECRETS § 4.02 [3] (1997).

14. RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 39-45 (1995).

15. This is an interesting shift in the overall treatment of this area of the law, which corresponds with the growing union of trade secret and unfair

Restatement of Torts.[16] Most courts appear to rely on the definitions in the UTSA[17] or in the *Restatement of Torts*,[18] and, as such, this Article will as well for most of the analysis which follows.

A. *Lawful Use of Another's Trade Secrets*

Unlike patent law, which grants exclusive use to a patent holder, the owner of a trade secret does not enjoy the same level of exclusivity.[19] Not only can the same information be considered a trade secret by more than one owner, but not all use of a trade secret is an unlawful misappropriation.[20] Rather, only trade secrets that

---

competition issues becoming evident in the case law. For instance, unfair competition claims involving trade secrets often mirror trade secret misappropriation claims. *See, e.g.*, GlobeSpan, Inc. v. O'Neill, 151 F. Supp. 2d 1229, 1235-36 (C.D. Cal. 2001); IBM v. Seagate Tech., Inc., No. 3-91-630, 1991 U.S. Dist. LEXIS 20406, at *11 (D. Minn. Dec. 31, 1991).

16. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39, Reporters' Note, at 438 (1995).

17. The UTSA defines a trade secret as:

> [I]nformation, 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.

UNIF. TRADE SECRETS ACT § 1 (amended 1985), 14 U.L.A. 538 (2005). The UTSA requires only reasonable efforts, not all conceivable efforts, to protect the confidentiality of trade secrets. *See* Surgidev Corp. v. Eye Tech., Inc., 828 F.2d 452, 455 (8th Cir. 1987); *see also* Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs. Inc., 923 F. Supp. 1231, 1253-54 (N.D. Cal. 1995) (stating that the church made reasonable efforts under UTSA to protect secrecy of religious documents through the use of locked cabinets and safes, logging and identification of materials, electronic sensors, alarms, photo identifications, security personnel, and confidentiality agreements for all those given access to materials).

18. *See* EPSTEIN, *supra* note 13, § 1.02, at 1-4. 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* then provides examples, stating that a trade secret "may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers." *Id.*

19. *See* Junker v. Plummer, 67 N.E.2d 667, 670 (Mass. 1946) ("The owner of a trade secret, in contradistinction to the owner of a patent, has no such right in the idea as will enable him to exclude others from using it. Thus if one acquires a secret by honest means he may use it.").

20. *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475-76 (1974); Chicago Lock Co. v. Fanberg, 676 F.2d 400, 404 (9th Cir. 1982).

have been acquired through improper discovery are unlawful.[21] A trade secret owner may grant permission to use a trade secret, and, even without consent or permission, a party may make lawful use of another's trade secrets in three main ways.

First, one who independently discovers or invents a trade secret is entitled to use it.[22] Second, one who actually reverse engineers a trade secret (obtained fairly and honestly) is not subject to liability for trade secret misappropriation.[23] Finally, and most relevant to this Article, where a party learns a trade secret through a disclosure that was not made in breach of a contract or special relationship, or with knowledge of such a breach, she is entitled to use it.[24] Thus, a trade secret owner has no protection for a trade secret that is accidentally disclosed.[25] Of even greater significance is that once disclosed, the trade secret no longer exists as to other parties because the requisite level of secrecy cannot be met.[26]

B. Equitable Nature of Trade Secret Law

Trade secret law is the branch of intellectual property law that most closely regulates standards of commercial ethics, guides morality of the business world, and underscores fair dealing.[27] It is probably in part for this reason that trade secret law is now codified in the *Restatement of Unfair Competition* rather than in the *Restatement of Torts*.[28] Its equitable nature is evident in most court

---

21. *See Kewanee*, 416 U.S. at 475-76.

22. *Id.* at 476.

23. *See, e.g., id.*; *Chicago Lock Co.*, 676 F.2d at 405 (stating that locksmiths may reverse engineer codes and then provide them for compilation); Smith v. Dravo Corp., 203 F.2d 369, 375 (7th Cir. 1953) ("It is unquestionably lawful for a person to gain possession, through proper means, of his competitor's product and, through inspection and analysis, create a duplicate, unless, of course, the item is patented."); UNIF. TRADE SECRETS ACT § 1 cmt. (amended 1985), 14 U.L.A. 538 (2005).

24. *See* RESTATEMENT (FIRST) OF TORTS § 757 cmt. a (1939).

25. *See Kewanee*, 416 U.S. at 476; Fisher Stoves, Inc. v. All Nighter Stove Works, Inc., 626 F.2d 193, 196 (1st Cir. 1980) ("[E]ven a bona fide trade secret is not protected against discovery by fair means, including accidental disclosure.").

26. *See* Lockridge v. Tweco Products, Inc., 497 P.2d 131, 134 (Kan. 1972) ("Once the secret is published to the 'whole world,' . . . it loses its protected status and becomes available to others for use and copying without fear of legal reprisal from the original possessor.").

27. *See, e.g., Kewanee*, 416 U.S. at 481-82; RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. a (1995); MELVIN F. JAGER, TRADE SECRETS LAW § 1.05, at 1-15 (1997).

28. Although the precise reason for this change is not explicitly stated, perhaps it is because trade secret law is inextricably tied to the values of our competitive marketplace. As the authors note:

[T]he law of trade secrets . . . reflects the accommodation of numerous

opinions, as judges struggle to decide what is fair by assessing, sometimes impliedly, elements such as good faith, honesty, and fair dealing.[29]

Consistent with these underlying ethical and equitable approaches, all three statutory frameworks of trade secret law described above prohibit the use of improper means to acquire trade secrets.[30] This is not an insignificant fact and is crucial to analyzing the third party problem presented in this Article. Thus, the extent to which acquisition of another's trade secrets over the Internet involved "improper means"[31] by both the original misappropriator and the third party user ought to be the central inquiry once the threshold question has been answered.[32]

III. SUMMARY OF RELEVANT CASE LAW

The cases in this Part are representative of the trade secret disclosure problem. They reflect the courts' attempts to wrestle with the bright line rule against protecting non-secret information and the equitable considerations underlying trade secret law. The cases also reveal the range of potential actors who could expose secrets, from insiders (like employees) to outsiders who purportedly are motivated by the public interest.

> interests, including the trade secret owner's claim to protection against the defendant's bad faith or improper conduct, the right of competitors and others to exploit information and skills in the public domain, and the interest of the public in encouraging innovation and in securing the benefits of vigorous competition.

RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. b (1995). *See* James J. Mulcahy & Joy M. Tassin, Note, *Is PepsiCo the Choice of the Next Generation: The Inevitable Disclosure Doctrine and Its Place in New York Jurisprudence*, 21 HOFSTRA LAB. & EMP. L.J. 233, 242-45 (2003).

29. *See, e.g.*, Smith v. Snap-On Tools Corp., 833 F.2d 578, 579 (5th Cir. 1987) ("The essence of the tort of trade secret misappropriation is the inequitable use of the secret."); *see also* N. Petrochemical Co. v. Tomlinson, 484 F.2d 1057, 1060 (7th Cir. 1973) (discussing the limited nature of remedies available for theft of trade secrets).

30. UNIF. TRADE SECRETS ACT § 1 (amended 1985), 14 U.L.A. 537 (2005); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 (1995); RESTATEMENT (FIRST) OF TORTS § 757 cmt. a (1939).

31. Under the UTSA, "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." UNIF. TRADE SECRETS ACT § 1(1).

32. See *infra* Part VII.A for an explanation of the threshold question—whether the information was entitled to trade secret protection before it was misappropriated.

A. *The Church of Scientology Cases*

In *Religious Technology Center v. Lerma,*[33] Lerma, a disgruntled former member of the Church of Scientology ("the Church"), published documents taken from a court record onto the Internet.[34] The Church[35] considered these documents to be trade secrets and obtained a Temporary Restraining Order prohibiting Lerma from publishing the alleged trade secrets.[36] The Church also sued *The Washington Post* for publishing a story related to and quoting the alleged trade secret documents.[37] The court granted summary judgment in favor of the *Post* on the trade secret misappropriation claims, reasoning in part that the documents no longer qualified as trade secrets.[38] The court was not moved by the fact that the Church had taken extraordinary measures to keep the documents secret, including having a Church member sign out the court file on a daily basis.[39]

In another Scientology case, the Church sought an injunction against another disgruntled former member who posted Church writings on an Internet USENET group.[40] In examining the Church's claim that the writings were trade secrets, the court stated that while the defendant could not rely on his own improper posting of the writings to the Internet to support the argument that the writings were no longer secrets, evidence that an unrelated third party posted them would result in a loss of secrecy and a loss of trade secret rights.[41] The court held that since the writings were posted on the Internet, they were generally available to the relevant public and there was no trade secret right available to support an injunction.[42]

In a motion six months later, the Church again sought an injunction on trade secret grounds, this time introducing consumer surveys to show that the writings were not generally known.[43] The

---

33. 908 F. Supp. 1362 (E.D. Va. 1995).

34. *Id.* at 1364.

35. The Religious Technology Center is a non-profit corporation formed by the Church of Scientology to protect its religious course materials. *See* Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc. (*Netcom I*), 923 F. Supp. 1231, 1239 (N.D. Cal. 1995).

36. *Lerma*, 908 F. Supp. at 1364.

37. *Id.* at 1365. The *Post* had obtained the documents from Lerma and from the court file. *Id.* at 1364-65.

38. *Id.* at 1368-69.

39. *Id.* at 1365.

40. *Netcom I*, 923 F. Supp. at 1239.

41. *Id.* at 1256.

42. *Id.* at 1256-57.

43. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc. (*Netcom*

court struck the surveys as irrelevant because they were surveys of the general public and not of the Church's competitors.[44] However, the court retreated from its earlier statement that posting to the Internet destroys trade secret protection.[45] Instead, the court announced that a determination of trade secret protection "requires a review of the circumstances surrounding the posting and consideration of the interests of the trade secret owner, the policies favoring competition and the interests, including first amendment rights, [sic] of innocent third parties who acquire information off the Internet."[46] Because the trade secret status of the Church's documents was an open question under this new test, the court granted a preliminary injunction.[47]

B. DVD Copy Control Ass'n v. Bunner[48]

In *DVD Copy Control Ass'n v. Bunner*, the plaintiff association controlled the rights to an encryption program called controlled scramble system ("CSS"), which restricted playback of encrypted DVDs to DVD players and computers that could decrypt CSS.[49] The plaintiff alleged that by reverse engineering plaintiff's program, a Norwegian teen created a program called DeCSS that allowed encrypted DVDs to be played on any DVD player or computer.[50] Defendant Bunner found and posted that program on the Internet for anyone to use.[51] The plaintiff filed a suit for injunctive relief to prevent Bunner from posting or linking to the DeCSS program on the Internet.[52] The court noted that while Bunner did not use improper means to *acquire* trade secrets under the Uniform Trade Secrets Act, Bunner *disclosed* trade secrets that he knew or should have known were proprietary information.[53] However, the court denied the preliminary injunction, finding that it would be a prior restraint of pure speech.[54]

II), No. C-95-20091, 1997 U.S. Dist. LEXIS 23572, at *24, *26 (N.D. Cal. Jan. 3, 1997).

44. *Id.* at *26.

45. *Id.* at *40-41.

46. *Id.* at *41.

47. *Id.* at *42.

48. 113 Cal. Rptr. 2d 338 (Ct. App. 2001), *rev'd*, 75 P.3d 1 (Cal. 2003), *remanded to* 10 Cal. Rptr. 3d 185 (Ct. App. 2004).

49. *Id.* at 341.

50. *Id.*

51. *Id.*

52. *Id.* at 341-42.

53. *Id.* at 346.

54. *Id.* at 350-51.

The court held that traditional intellectual property exceptions to the prior restraint doctrine do not apply since Bunner did not actually use the information or breach a contractual obligation.[55] After an appeal to the California Supreme Court, which held that an injunction would not violate the First Amendment if there was a trade secret,[56] the court was asked on remand to determine whether a trade secret still existed.[57] The court noted that widespread publication of a trade secret over the Internet will destroy its status as a trade secret.[58] However, the court went further, reasoning that the information retains its value to the creator if the Internet publication is sufficiently obscure or transient so that it does not become generally known to those who would consider it valuable.[59] The court rejected plaintiff's public policy arguments for protecting trade secrets, holding that allowing an injunction once a trade secret has become public could theoretically put the entire general public at risk for liability.[60] Since the trade secret had been widely disseminated, the court held that an injunction would not prevent any further harm from occurring to the plaintiff and denied the injunction.[61]

C. United States v. Genovese[62]

In *United States v. Genovese*, defendant Genovese was charged with offering Microsoft's source code for sale on the Internet in violation of the Economic Espionage Act of 1996[63] ("EEA").[64] Genovese challenged the indictment on the grounds that the statute, which makes downloading and selling a trade secret a crime, violated the First Amendment.[65] The court noted that the First Amendment protects computer source code and other trade secrets,

---

55. *Id.* at 349.

56. DVD Copy Control Ass'n v. Bunner, 75 P.3d 1, 14 (Cal. 2003).

57. DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 187 (Ct. App. 2004).

58. *Id.* at 192.

59. *Id.*

60. *Id.* at 194.

61. *Id.* at 196.

62. 409 F. Supp. 2d 253 (S.D.N.Y. 2005).

63. The Act provided the first comprehensive criminal federal trade secrets law on trade secret theft and misappropriation. 18 U.S.C. §§ 1831-39 (1996). The EEA criminalizes "theft of trade secrets," *id.* § 1832, and "economic espionage" for the benefit of a foreign government, instrumentality or agent. *Id.* § 1831. In order to state a claim under the Act for theft of trade secrets, the government must establish that the defendant knowingly stole or obtained information that was a trade secret without authorization. *Id.* § 1832(a).

64. *Genovese*, 409 F. Supp. 2d at 254.

65. *Id.* at 256.

but held that the First Amendment does not protect conduct such as trying to convert a trade secret for economic gain.[66] Genovese also made a due process challenge, arguing that criminalizing the download and sale of trade secrets under the statute was vague because he could not have known the source code was not generally known or that Microsoft took reasonable measures to protect it.[67] However, the court held that under the EEA, a trade secret does not lose its protection when "temporarily, accidentally, or illicitly released to the public, provided it does not become 'generally known.'"[68] The court observed that since Genovese sold the source code, it still retained some value and was not generally known.[69]

IV. ANALYZING THE THIRD PARTY PROBLEM

This Article tackles the problem that arises when an independent third party[70] discovers another's trade secrets on the Internet and uses or intends to use it. Under this scenario, the trade secret owner has misappropriation[71] claims against the original misappropriator, and, if the original misappropriator did not post the information himself, whoever posted the information

66. *Id.*

67. *Id.* at 257.

68. *Id.* (quoting 18 U.S.C. § 1839(3)(B) (2000)).

69. *Id.*

70. An independent third party is independent of and has no connection to or involvement with the original misappropriator of the trade secret.

71. The UTSA defines "misappropriation," as:

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

UNIF. TRADE SECRETS ACT § 1(2) (amended 1985), 14 U.L.A. 537 (2005).

may also be liable.[72] As against an independent third party who comes upon the information once posted, however, it is unclear whether the trade secret owner has any remedies under trade secret law to prevent use of the information.

Indeed, the current status of trade secret law would suggest that the third party is entitled to use information she obtained from the public domain, assuming that she did not employ improper means to obtain the trade secret, has no knowledge that it was obtained by improper means, or is not bound by any contractual or special relationship with the trade secret owner.[73] However, that initial conclusion necessarily makes several underlying assumptions about trade secret law and Internet publication.

Among these assumptions are that (1) the information was not a trade secret at the time it was discovered, (2) the fact that the information appeared on the Internet makes it public, generally known, and readily ascertainable, and (3) the discovery was not through improper means. This Part will dissect each assumption to analyze whether it is reasonable to conclude that the trade secret owner is not likely to prevail against an independent third party, either because the information was not a trade secret at the time it reached the third party or because even if the information is determined to be a trade secret it was not misappropriated by the third party. Parts V and VI will then turn for guidance to a broader view outside of trade secret law, followed by the proposed model.

A. Is it a Trade Secret?

The first hurdle and first step to a trade secret owner whose proprietary information has been discovered on the Internet is proving that the information has not lost its trade secret status by virtue of its publication in this medium. While in the typical misappropriation case a trade secret owner must prove that the information is the type of information that is protectable under trade secret law and that she took reasonable steps to maintain its secrecy, the Internet publication problem presented here is

---

72. To the extent one has exhibited discretion, akin to that of a magazine or newspaper publisher, in deciding to disclose a trade secret, then she may be liable. O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 98 (Ct. App. 2006) (noting that disclosure of confidential information about a company may expose a reporter or editor to liability).

73. *See* Lockridge v. Tweco Prods., Inc., 497 P.2d 131, 134-35 (Kan. 1972) (reasoning that there can be no recovery against those who are "not misappropriators in the first instance, or possessors of the secret by virtue of learning it from the misappropriator(s) with knowledge that it was stolen . . ." (quoting Underwater Storage, Inc. v. U.S. Rubber Co., 371 F.2d 950, 955 (D.C. Cir. 1966))).

complicated by additional layers of proof. This complication is primarily because the third party (vis-à-vis, for instance, a former employee who discloses an employer's trade secrets) would not be breaching any contract or duty to the trade secret owner and would have discovered the information in an arguably public place.[74]

Given the factual scenario presented here, the relevant applicable requirements from the UTSA's[75] definition of trade secret are that the information (i) not be "generally known" *and* (ii) not be "readily ascertainable by proper means."[76] This definition leads to further inquiry to determine whether a posting on the Internet is "generally known" and "readily ascertainable" and whether locating such information via the Internet constitutes "proper means."[77]

Because of the nature of the Internet and the relatively unique (to trade secret law) problem presented in this Article, it is important to identify the accurate point in time at which the trade secret status of the information should be determined and the party from whose perspective the relevant inquiry should be made. One possibility is to consider whether at the time the defendant (independent third party) came upon the information it was a trade secret. Another option is to consider whether the information was a trade secret before it was misappropriated by the wrongdoer. The former is a pre-misappropriation perspective, while the latter is a post-misappropriation perspective. The post-misappropriation perspective seems more consistent with trade secret law and the manner in which misappropriation cases are generally analyzed. To be sure, it is not the more favorable perspective for a trade secret owner, because it lends itself to a more ephemeral view of trade secrets when, despite a trade secret owner's best efforts, the owner may lose trade secret protection because of the intervening acts of a bad actor.[78]

---

74. In cases where the information has previously or simultaneously become available by means other than the Internet, it makes it even more difficult for the trade secret owner to attempt to argue that it should be protected. *See, e.g.*, Religious Tech. Ctr. v. F.A.C.T.NET, Inc., 901 F. Supp. 1519, 1526 (D. Colo. 1995) (noting that the information had been available in an unsealed court file).

75. I rely on the UTSA because it has been adopted by a majority of the states, and because its trade secret definition is consistent with both the *Restatement of Torts* and the *Restatement of Unfair Competition*.

76. UNIF. TRADE SECRETS ACT § 1(4)(i).

77. *Id.*

78. *See, e.g.*, DVD Copy Control Ass'n v. Bunner, 75 P.3d 1, 28 (Cal. 2003) (Moreno, J., concurring) ("[E]ven when a trade secret holder acts with perfect diligence, it has no action against the republisher of no-longer-secret information who does not act in privity with the original misappropriator.").

Although the additional layer presented here, of an independent third party discovering information on the Internet from a misappropriator, is missing from the typical two-party trade secret case, there does not seem to be sufficient reason to diverge from the same analysis. In other words, in a situation when an employee steals an employer's trade secrets, we would ask whether the information was a trade secret at the time the employee took possession of it. Similarly, with an independent third party, it seems logical to consider whether at the time she discovered the information it was a trade secret. Put in criminal terminology, in order to be guilty of stealing a trade secret, the information must have been a trade secret at the time the defendant came into possession of it.

1. Is a Posting on the Internet "Generally Known"?

It is axiomatic that publicly available information cannot qualify for trade secret status.[79] Given our understanding of the Internet, it has become an implicit assumption that any information posted on the Internet[80] is public.[81] "[T]he act of 'posting' constitutes publication to the world."[82] If "generally known" is synonymous with public, then it might explain why many courts assume that a trade secret posted on the Internet has become generally known. However, exploration below the surface of these assumptions merely leads to further questions. For instance, does it matter if the information is "known" or "knowable" to competitors? Does public mean public accessibility or public publication? Does the obscurity

79. *See* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1002 (1984) ("Information that is public knowledge or that is generally known in an industry cannot be a trade secret."); Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475 (1974) ("The subject of a trade secret must be secret, and must not be of public knowledge or of a general knowledge in the trade or business.").

80. Note that in some circumstances there can be various levels of access to a Web site, ranging from publicly available portions to those that are restricted to authorized users with passwords. However, this discussion assumes an independent third party has accessed information from a publicly available site or legitimately through a more restrictive site. *See, e.g.*, Inventory Locator Serv., LLC v. Partsbase, Inc., No. 02-2695MA/V, 2005 WL 2179185, at *2 (W.D. Tenn. Sept. 6, 2005) (discussing a Web site with four levels of access).

81. *See generally* Oja v. U.S. Army Corps of Eng'rs, 440 F.3d 1122, 1131 (9th Cir. 2006) ("Internet publication is a form of 'aggregate communication' in that it is intended for a broad, public audience, similar to print media."); Jerome Stevens Pharms., Inc. v. FDA, 402 F.3d 1249, 1251 (D.C. Cir. 2005) (stating that trade secrets posted on the FDA Web site are available to public); Am. Booksellers Found. v. Dean, 342 F.3d 96, 100 (2d Cir. 2003) (holding that posting information to a Web site available to public is distribution).

82. O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 91 (Ct. App. 2006).

of the Web site matter, or are all Internet postings equal? An attempt to answer these questions will be forthcoming after we further dissect the legal definition of a trade secret.

The comments to the UTSA provide guidance in that they make clear that "generally known" does not necessarily mean known by the general public.[83] Indeed, a trade secret can be "generally known" if it is known by at least one person who can obtain economic benefit from the information.[84] It would therefore seem more precise to say that information cannot be a trade secret if it is known (delete "generally") by the relevant people[85] (i.e., those who may benefit from it).[86] Accordingly, it is difficult to challenge the emergent conclusion that "posting works to the Internet makes them 'generally known' to the relevant people . . . ."[87] Even though that conclusion makes legal sense, from an equitable perspective, it seems unfair to a trade secret owner that illegal conduct by another could destroy a heretofore well-preserved trade secret.

The case law demonstrates courts' uneasiness with a bright line rule, implying an instinctive, albeit unstated, concern for fairness and the equitable nature of trade secret law. One trial court, concerned about the incentives to wrongdoers, found that the mere posting of information on the Internet does not destroy a trade secret.[88] According to the court, "To hold otherwise would do nothing less than encourage misappropriaters [sic] of trade secrets to post the fruits of their wrongdoing on the Internet as quickly as possible and as widely as possible thereby destroying a trade secret forever."[89]

The court was willing to recognize that publication on the Internet does not automatically terminate the existence of a trade secret and considered the amount of time the information was posted and, thus, available for inspection.[90] To the court, where the posting is "sufficiently obscure or transient or otherwise limited so

83. *See* UNIF. TRADE SECRETS ACT § 1 cmt. (amended 1985), 14 U.L.A. 538 (2005).

84. *Id.*

85. This does not include people to whom the trade secret owner has disclosed the trade secret pursuant to a non-disclosure or confidentiality agreement.

86. *See* Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., No. C-95-20091 RMW, 1997 U.S. Dist. LEXIS 23572, at *40-41 (N.D. Cal. Jan. 3, 1997); DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 192-93 (Ct. App. 2004).

87. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 923 F. Supp. 1231, 1256 (N.D. Cal. 1995).

88. *DVD Copy Control Ass'n*, 10 Cal. Rptr. 3d at 190.

89. *Id.* at 190-91.

90. *Id.* at 192-93.

that it does not become generally known to the relevant people, i.e., potential competitors or other persons to whom the information would have some economic value," the trade secret status is preserved.[91] The precise measure of obscurity or transience required to protect the trade secret, however, is unsettled.

In the *Religious Technology Center* cases, one of the courts noted that the fact that the information had been posted on the Internet for ten days made it publicly available (destroying trade secret protection) because during those ten days the information was potentially available to millions of Internet users.[92] According to that court, "Once a trade secret is posted on the Internet, it is effectively part of the public domain, impossible to retrieve."[93] In another, related case, the court was wary of making the "overly broad generalization" that posting works to the Internet would destroy their trade secret status.[94] Instead, the court recommended consideration of the circumstances surrounding the posting.[95] The model presented here espouses precisely this kind of review of the factual circumstances in an attempt to decide on a case-by-case basis whether, among other things, the generally known standard has been met.

2. Is a Posting on the Internet "Readily Ascertainable"?

It is interesting that the drafters of the UTSA chose a conjunctive between "generally known" and "readily ascertainable." This necessarily implies that they have separate meaning. However, in practice, courts seem to struggle with determining the meaning of these labels[96] and more often simply do not consider the readily ascertainable prong as a separate factor, but instead appear to collapse it into the generally known prong.[97] Indeed, some states that have adopted the UTSA have chosen to remove "readily ascertainable" altogether from their definition of trade secret.[98]

---

91. *Id.*

92. Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 1368 (E.D. Va. 1995).

93. *Id.*

94. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., No. C-95-20091 RMW, 1997 U.S. Dist. LEXIS 23572, at *40-41 (N.D. Cal. Jan. 3, 1997).

95. *Id.* at *41.

96. *See, e.g.*, United States. v. Hsu, 40 F. Supp. 2d 623, 630 (E.D. Pa. 1999) ("[W]hat is 'generally known' and 'reasonably ascertainable' about ideas, concepts, and technology is constantly evolving in the modern age."); *see also* MicroStrategy, Inc. v. Bus. Objects, 331 F. Supp. 2d 396, 417 (E.D. Va. 2004) ("What constitutes *readily* ascertainable through proper means is heavily fact-dependent and simply boils down to assessing the ease with which a trade secret could have been independently discovered.").

97. *See Hsu*, 40 F. Supp. 2d at 630.

98. *See, e.g.*, CAL. CIV. CODE § 3426.1(d)(2), cmt. at 168 (West 1997)

Even without this trend, under the circumstances presented here, attempting to satisfy both "generally known" and "readily ascertainable" does appear redundant. Given the nature of the Internet, the meanings may converge, and one could posit that every Internet posting is generally known and readily ascertainable or is generally available and thus readily ascertainable.

In the context of the Internet, treating the two concepts the same does not appear problematic. The very nature of the Internet—that it allows equal access to anyone with a computer, irrespective of certain traditional limitations to accessing information, like geography and cost—means that it makes information at least readily discoverable, if not ascertainable.[99] Moreover, considering that the relevant population consists of those who could obtain economic benefit from the information, it is logical that these arguably motivated individuals would be the very persons surfing the Internet for information that would afford them a competitive advantage.

Earlier in this Part I posed certain questions which, by virtue of having dissected the definition of trade secret in the context of the Internet, may now be easier to answer. First, if courts continue to treat "generally known" and "readily ascertainable" interchangeably, then it does not seem to make a significant difference whether the information is "known" or "knowable" to competitors. The former would fall under the "generally known" category, and the latter, i.e., whether it is knowable, would be captured under the "readily ascertainable" category.

The practical reality may be that the information will be known by at least one person, typically the named defendant in the law suit. That defendant will likely argue that the information is not a trade secret because the nature of the Internet is such that others have very likely accessed the information as well. This raises another interesting question as to whether it is the trade secret owner's burden of production to show that others have not accessed the information, or the defendant's burden to show the opposite. If posting information on the Internet makes it discoverable by and thus knowable to the relevant public, then the mere fact that the information is accessible to others may be sufficient to destroy

---

(explaining that the phrase was removed because it was "viewed as ambiguous in the definition of a trade secret," but that "the assertion that a matter is readily ascertainable by proper means remains available as a defense to a claim of misappropriation").

99. The AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (Houghton Mifflin Co., 4th ed. 2000) defines ascertainable as "[t]o discover with certainty, as through examination or experimentation."

secrecy even without proof of direct knowledge or access. Accordingly, even when the trade secret owner does not necessarily know whether any specific competitors or others have accessed the information, it may nonetheless have lost trade secret protection. This approaches the bright line rule that publication in and of itself extinguishes the trade secret.

As between public accessibility and publication, the inquiry is the same, particularly in the context of the Internet. A posting on the Internet, compared to, for instance, a disclosure in a report sitting on an office shelf,[100] is both a publication[101] and a publicly accessible publication. Thus, to the extent that generally known and readily ascertainable are synonymous, the mere publication of a trade secret on the Internet and its ensuing accessibility would destroy the secret.

Finally, the many angles of the analysis seem to lead to the inexorable conclusion that a posting on the Internet would most likely defeat any trade secret protection. However, this may be true only if one accepts that all Internet postings are created equal. If, however, considerations of the obscurity of or accessibility to the Web site, as well as timing and amount of exposure, affect the "generally known" or "readily ascertainable" prongs, then perhaps a different conclusion might be possible. The factors presented later in this Paper attempt to accommodate this possibility.

B. Is it Misappropriation?

Having proved that the information is a trade secret, or likely to be a trade secret, the second hurdle to a trade secret owner whose proprietary information has been discovered on the Internet is proving misappropriation. This is difficult because, on the surface, the presence of the independent third party who has no duty to the trade secret owner to maintain his secret coupled with the public place discovery does not seem actionable. The view that any wrong to a trade secret owner occurs only at the time of the improper acquisition stems from the underlying construct of trade secret law that trade secrets are not property.[102] Rather, the presence of a confidential relationship or good faith obligation is a necessary

---

100. Such a report is arguably not publicly accessible. *Cf. In re* Cronyn, 890 F.2d 1158 (Fed. Cir. 1989) (finding in a patent case that a thesis in a college library that was not indexed or catalogued was not sufficiently publicly accessible to constitute a published prior art reference).

101. *See, e.g.*, O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 102-03 (Ct. App. 2006) (analyzing why Internet Web sites are publications).

102. The *Restatement of Torts* rejects the concept of a property interest in a trade secret, grounding trade secret protection on a general duty of good faith. RESTATEMENT (FIRST) OF TORTS § 757 cmt. a (1939).

prerequisite, and it is that breach that triggers something akin to an enforceable property right in the trade secret.[103] The key factors then appear to be whether the information was discovered by improper means and whether the third party should have known it was discovered by improper means.

All three trade secret statutory frameworks include improper means in defining misappropriation.[104] The relevant provision from the UTSA appears to make a third party liable for misappropriation if he or she "knew or had reason to know that his or her knowledge of the trade secret was derived from one who used improper means to acquire it."[105] This necessarily suggests a fact-intensive determination into the third party's state of mind, her level of knowledge that the information was a trade secret, and whether it was acquired by improper means.

With respect to third parties, not only does the *Restatement of Torts* define misappropriation to include a notice requirement when disclosure is intentional, but also when the disclosure "was made to him by mistake."[106] This raises an interesting question as to whose mistake one should consider. Arguably the original misappropriator who published the information intended to do so and thus did not do so by mistake. On the other hand, the trade secret owner could argue that it was a mistake because he or she did not intend to disclose the trade secret. It is also unclear from the *Restatement*'s definition whether "notice of the fact"[107] that the information is secret is judged at the time the trade secret is discovered or at a later time when the trade secret owner provides such notice to the defendant. The cases seem to suggest the former.[108]

It is worth considering whether the manner in which the third party obtained the information over the Internet is (or should be) "improper means."[109] The phrase certainly captures unlawful

---

103. *See* Lockridge v. Tweco Prods., Inc., 497 P.2d 131, 136 (Kan. 1972) (discussing why the misappropriation of a trade secret is not a continuing wrong).

104. UNIF. TRADE SECRETS ACT § 1 (amended 1985), 14 U.L.A. 537 (2005); RESTATEMENT (FIRST) OF TORTS § 757 cmt. a (1939); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 (1995).

105. UNIF. TRADE SECRETS ACT § 1(2)(ii). The *Restatement of Torts* and *Restatement of Unfair Competition* definitions are consistent with the UTSA.

106. RESTATEMENT (FIRST) OF TORTS § 757 (1939).

107. *Id.*

108. *See, e.g.*, Williams v. Curtiss-Wright Corp., 681 F.2d 161, 164 (3d Cir. 1982) ("[The defendant] had reason to know, and in fact knew, that the drawings were secret when he obtained them, and that their release to him was improper."); *see also* discussion *infra* Part VIII.B.3 regarding notice.

109. Improper means under the UTSA includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain

conduct, but it has also been interpreted to cover lawful conduct.[110] For the purposes of this problem, the assumption is that the third party is not a hacker and has merely accessed the information through a search engine or through another site to which she has legitimate access. Accordingly, even given a broad interpretation of improper means, it would seem very unlikely that this kind of searching, in and of itself, would constitute improper means.[111] The end result would appear to be that a defendant who does not know or have reason to know that the information is a trade secret cannot be liable for misappropriation. As one court reasoned, "Although the person who originally posted a trade secret on the Internet may be liable for trade secret misappropriation, the party who merely downloads Internet information cannot be liable for misappropriation because there is no misconduct involved in interacting with the Internet."[112]

It is noteworthy that for most courts the question of whether there was misappropriation comes back to the preliminary consideration of whether the information qualifies as a trade secret.[113] This is perfectly logical, given that one cannot misappropriate that which is not a trade secret. This observation helps inform the model presented in this Article, since the preliminary consideration of the protectable status of the information is inescapable. However, once determined in the affirmative, it must be divorced from the other factors in order to avoid a tautology and permit a clearer, more distinct analysis of the issues.

V. OTHER OBSTACLES TO TRADE SECRET PROTECTION

In addition to the hurdles to preserving the trade secret status of arguably public information within trade secret law, there are further barriers from other areas of law that may also be implicated.

---

secrecy, or espionage through electronic or other means. UNIF. TRADE SECRETS ACT § 1.

110. *See, e.g.*, Nat'l Rejectors, Inc. v. Trieman, 409 S.W.2d 1, 35-36 (Mo. 1966).

111. *See* Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 1369 (E.D. Va. 1995) ("'It is the *employment of improper means to procure the trade secret, rather than the mere copying or use*, which is the basis of [liability].'" (quoting Trandes Corp. v. Atkinson Co., 996 F.2d 655, 660 (4th Cir. 1993))).

112. *Id.* at 1368.

113. *See, e.g.*, DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 193 (Ct. App. 2004) ("[I]f the allegedly proprietary information contained in DeCSS was already public knowledge when Bunner posted the program to his Web site, Bunner could not be liable for misappropriation by republishing it because he would not have been disclosing a trade secret.").

Both constitutional law and patent law lean toward prohibiting restrictions on the use of publicly available information. The applicable First Amendment, Fourth Amendment, and patent law doctrines are summarized below.

A. *First Amendment*

Defendants in these types of cases have asserted a First Amendment right to disclose allegedly trade secret information discovered on the Internet.[114] "[T]he First Amendment generally prohibits limitations, absent some extraordinary showing of governmental interest, on the publication of information already made public."[115] When weighing the jealously guarded First Amendment rights against the commercial interests in protecting trade secrets, courts are often reluctant to enjoin disclosures of trade secrets.[116] By implication, it would seem that if the First Amendment always trumps an owner's right to protect against disclosure, then trade secret law would be powerless to enforce non-disclosure agreements or otherwise prevent disclosure of their secret information. Accordingly, the California Supreme Court has rejected a similar argument and made clear that an injunction against disclosure of information that qualifies as a trade secret does not violate the First Amendment.[117]

Nonetheless, the obvious hole remains: where a trade secret has been disclosed (and thus no longer qualifies as a trade secret under current trade secret law), the First Amendment could protect the disclosure.[118] This returns full circle to the ever critical determination whether information, once posted on the Internet, loses its trade secret status. A positive response to that question leads to the likely conclusion that the information, for a whole host of reasons, including the First Amendment, can be used freely.

Furthermore, in the absence of a fiduciary duty or confidentiality agreement not to publish trade secret information, one court has ruled that the First Amendment prevails. In *Ford*

---

114. For further discussion about the First Amendment in this context, see generally Lambrecht, *supra* note 9.

115. DVD Copy Control Ass'n v. Bunner, 75 P.3d 1, 27 (Cal. 2003) (Moreno, J., concurring).

116. *See* Procter & Gamble Co. v. Bankers Trust Co., 78 F.3d 219, 225 (6th Cir. 1996) (refusing to enjoin publication of trade secrets improperly obtained in violation of a protective order, noting that "[t]he private litigants' interest in protecting their vanity or their commercial self-interest simply does not qualify as grounds for imposing a prior restraint").

117. *Bunner*, 75 P.3d at 19.

118. *See id.* at 10 n.5.

Motor Co. v. Lane,[119] the defendant operated a Web site with news about Ford and its products.[120] Lane received confidential Ford documents from an anonymous source and initially agreed not to disclose most of the information.[121] However, Lane eventually published some documents on his Web site relating to the quality of Ford's products,[122] thinking that the public had a right to know. He did so despite knowing that the documents were confidential.[123] Ford sought a temporary restraining order to prevent publication of the documents, claiming the documents were trade secrets.[124] The court acknowledged (without any discussion) that Ford could show Lane had misappropriated its trade secrets, but denied the injunction on First Amendment grounds, considering an injunction to prevent Lane from publishing trade secrets a prior restraint.[125] Despite evidence that Lane had used the Internet and the confidential material to extort Ford, the court noted that Ford's trade secrets were not more important than the documents in the *Pentagon Papers* case and not more inflammatory than the article in the *Near* case.[126] Since a prior restraint was not justified in either of those cases, a prior restraint could not be justified in this case.[127]

B. Fourth Amendment

Further constitutionally based obstacles to restricting use of publicly available information lies in Fourth Amendment jurisprudence. Some scholars have explored analogies between Fourth Amendment privacy interests and the secrecy requirement of trade secret law.[128] In particular, when a person unlawfully invades one's zone of privacy to steal private, incriminating information and then reveals that information to the police or the public, courts have held that this conduct does not violate the Fourth Amendment.[129]

---

119. 67 F. Supp. 2d 745 (E.D. Mich. 1999).

120. *Id.* at 747.

121. *Id.*

122. *Id.*

123. *Id.* at 748.

124. *Id.*

125. *Id.* at 750.

126. *Id.* at 751-53 (citing New York Times Co. v. United States, 403 U.S. 713 (1971) and Near v. Minnesota, 283 U.S. 697 (1931)).

127. *Id.* at 753.

128. *See, e.g.*, Atkins, *supra* note 9, at 1182-83; Note, *Trade Secret Misappropriation: A Cost-Benefit Response to the Fourth Amendment Analogy*, 106 HARV. L. REV. 461, 465-66 (1992).

129. *See generally* Rodney A. Smolla, *Information as Contraband: The First Amendment and Liability for Trafficking in Speech*, 96 NW. U. L. REV. 1099, 1135-36 (2002) (discussing the "silver platter" doctrine which permits an independent agent to break the law to obtain incriminating evidence, and turn

Thus, the fact that trade secret law similarly provides incentives to break the law is not a unique concept.[130]

C. *Patent Law*

Attempts to restrict the use of information found in the public domain are outside the purview of trade secret law and instead are covered by patent law, which governs property rights in publicly known information. The underlying premise is that "all ideas in general circulation [are] dedicated to the common good unless they are protected by a valid patent."[131] Accordingly, attempts to use state trade secret law to restrict use of information in the public domain are preempted by patent law.[132]

Patent law further lends support to the idea that the intervening illegal act of a misappropriator could negatively affect the rights of the owner. The two cases discussed below make clear that even when a misappropriator steals an invention while it is a trade secret and then, unbeknownst to the inventor, puts it on sale or uses it publicly one year before the inventor files a patent application on the invention, that use or sale prevents the inventor from obtaining a patent.

In *Lorenz v. Colgate-Palmolive-Peet Co.*,[133] plaintiff Lorenz sued defendant Colgate for a declaration that Lorenz's soap manufacture patent was valid and Colgate's was void.[134] Lorenz alleged that he disclosed the invention to Colgate and that disclosure gave Lorenz priority over the invention.[135] Colgate asserted that its use of the patented process more than a year before Lorenz filed the patent application rendered Lorenz's patent invalid under prior public use.[136] Lorenz in turn argued that prior use does not apply when an

---

that evidence over to law enforcement on a "silver platter").

130. However, unlike the Fourth Amendment "silver platter" cases, which justify such incentives by arguing that the Fourth Amendment only proscribes government action, an analogous rationale in trade secret law is not as strongly supported. *See id.* at 1136-38.

131. Kewanee Oil Co. v. Bircron Corp., 416 U.S. 470, 481 (1974) (quoting Lear, Inc. v. Adkins, 395 U.S. 653, 668 (1969)).

132. *See* Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 164 (1989) ("That which is published may be freely copied as a matter of federal right." (quoting Bailey v. Logan Square Typographers, Inc., 441 F.2d 47, 51 (1971))); DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 195 (Ct. App. 2004) ("[T]hat which is in the public domain cannot be removed by action of the states under the guise of trade secret protection." (citing *Kewanee*, 416 U.S. at 481)).

133. 167 F.2d 423 (3d Cir. 1948).

134. *Id.*

135. *Id.* at 424.

136. *Id.*

invention is "pirated" by another person.[137] However, the court held that the prior public use statute had no exceptions and any intervening public use bars the inventor from obtaining a patent.[138] The court stated that the policy behind the statute was to protect the public's interest, and therefore it was up to the inventor to protect his discovery from being used.[139]

In *Evans Cooling Systems, Inc. v. General Motors Corp.*,[140] Evans filed suit against General Motors ("GM") for infringing upon Evans's patent on engine cooling.[141] GM moved to declare the patent invalid on the basis that GM sold cars with the invention before Evans sought a patent, but Evans asserted that GM should not be able to invalidate the patent because GM stole his engine cooling invention and allowed dealers to sell vehicles containing the invention.[142] After reviewing prior case law, the court concluded that since the public use of the invention by the dealers was innocent, the public use bar should apply.[143]

VI. ASSISTANCE FROM ATTORNEY-CLIENT PRIVILEGE CASES

Despite the seemingly uphill battle in trying to preserve the trade secret status of information disclosed on the Internet, one area of law provides some hope, even if only by analogy. Cases involving inadvertent disclosure of materials protected by the attorney-client privilege are in some ways analogous to the trade secret problem identified here. As the summary below reveals, the courts tend to protect the privileged status of the information, especially where the necessary precautions were taken and the disclosure occurred inadvertently or through misconduct. Thus, even where confidentiality of the materials may have been lost, the privilege can be preserved. Although there is no direct parallel to trade secret law, in that once secrecy is lost, the trade secret status is also lost, the model presented here attempts to capture the spirit of those cases by recognizing that there may be certain exceptional circumstances where trade secret status may be retained.

---

137. *Id.* at 425.
138. *Id.* at 429.
139. *Id.* at 429-30.
140. 125 F.3d 1448 (Fed. Cir. 1997).
141. *Id.* at 1450.
142. *Id.*
143. *Id.* at 1454. However, the court noted that if GM did misappropriate the invention, Evans could still sue for misappropriation of trade secrets. *Id.*

A. In re Grand Jury Proceedings Involving Berkley & Co.[144]

In *In re Grand Jury Proceedings Involving Berkley & Co.*, Berkley moved to suppress evidence stolen by a former employee from a grand jury, asserting that it was protected by attorney-client privilege.[145] The court initially held that historically the attorney-client privilege did not apply to stolen or lost documents as a matter of law.[146] On motion to reconsider, the court noted that the more modern approach is that when attorneys and clients take reasonable precautions to ensure confidentiality, the attorney-client privilege is not lost.[147] Since the former Berkley employee stole the documents, the court held that the theft is analogous to an attorney disclosing privileged information in bad faith, which does not result in a loss of privileged status under modern precedent.[148]

B. Resolution Trust Corp. v. Dean[149]

In this case, the *Washington Post* published excerpts from an Authority to Sue Memorandum prepared by plaintiff Resolution Trust Corporation's ("RTC") counsel.[150] When defendant Symington moved to order discovery of the memo, RTC asserted the attorney-client privilege.[151] Symington argued that unless RTC could prove the memo was stolen, the privilege was waived when the memo was leaked to the newspaper.[152] Citing *Berkley*, the court rejected Symington's argument and noted that disclosure of the memo was a criminal act.[153] The court held that since RTC proved they took precautions to ensure the memo's confidentiality, they established that the release of the memo was not voluntary and that they did not waive the attorney-client privilege of the memo.[154]

C. Smith v. Armour Pharmaceutical Co.[155]

In *Smith v. Armour Pharmaceutical Co.*, defendant Miles, Inc., inadvertently included a document from in-house counsel in a

144. 466 F. Supp. 863 (D. Minn. 1979).
145. *Id.* at 865.
146. *Id.* at 868 (citing 8 WIGMORE ON EVIDENCE § 2325 (McNaughton rev. 1961)).
147. *Id.* at 869.
148. *Id.*
149. 813 F. Supp. 1426 (D. Ariz. 1993).
150. *Id.* at 1427.
151. *Id.* at 1428.
152. *Id.* at 1428-29.
153. *Id.* at 1429 (citing In re Grand Jury Proceedings Involving Berkley & Co., 466 F. Supp. 863, 869 (D. Minn. 1979)).
154. *Id.* at 1429-30.
155. 838 F. Supp. 1573 (S.D. Fla. 1993).

document production given to plaintiff Smith.[156] When Smith's lawyer subsequently leaked the document to the press, and accounts of the document appeared in newspapers from Florida to Alaska, Miles filed a protective order, asserting attorney-client privilege to the documents.[157] The court noted that wide circulation of a document is not, by itself, grounds for revoking attorney-client privilege.[158] The court found a distinction between the document losing its confidentiality and losing its privilege, stating that a document can retain its privilege even if it is no longer confidential.[159] Even though the document was no longer confidential, it still retained the attorney-client privilege because Miles did not waive the privilege.[160]

D. United States ex rel. Mayman v. Martin Marietta Corp.[161]

In this case, the government sought access to privileged documents via a discovery request, asserting that defendant Martin Marietta waived the privilege by allowing a former employee to possess a draft of the document.[162] The court found that whoever gave the privileged documents to the former employee was not authorized to have them,[163] that the former employee was not authorized to keep them,[164] and that he made false statements to keep them.[165] Since the confidentiality of the documents was breached due to the unauthorized actions of a former employee, the court refused to conclude that reasonable precautions were not taken and held that the privilege was not waived.[166]

VII. THE SEQUENTIAL PRESERVATION MODEL

The complexity of the problem presented here lies not necessarily in the analytical framework of trade secret law available for determining whether information is deserving of trade secret protection. Rather, it is the recognition of the injustice that could result from strict application of the law and the ensuing incentives for illegal conduct that is disturbing. Given the equity rationale underlying trade secret law, these concerns compel an exploration

156. *Id.* at 1575.
157. *Id.*
158. *Id.* at 1576.
159. *Id.*
160. *Id.* at 1577.
161. 886 F. Supp. 1243 (D. Md. 1995).
162. *Id.* at 1244.
163. *Id.* at 1245-46.
164. *Id.*
165. *Id.*
166. *Id.* at 1246.

for a more just result. There is an underlying recognition that perhaps something more than a bright line rule may be appropriate in some cases.

With that in mind, I propose below what I coin a "sequential preservation model" as a tool to achieve a fairer result in those limited cases where the injustice would otherwise be especially grave. When properly applied, the factors should provide relief in extraordinary circumstances. For the vast majority of cases, however, the default rule under the current trade secret framework should apply. Publication of trade secrets via the Internet will cause a loss of trade secret protection. This may appear harsh in some circumstances, but trade secret owners have a duty to be vigilant. Having chosen this method of intellectual property protection, they must be ready to face the possible disadvantages of the regime.[167]

A prudent approach to addressing these types of cases requires deliberate and careful consideration of the many issues raised in the Article, including the rights of a trade secret owner to maintain the protection of his or her valued information versus the right of the public (and competitors) to use information found in the public domain. The conduct leading to the disclosure does not necessarily change the analysis; thus, an inadvertent disclosure by the trade secret owner or one of her agents is treated in the same manner as a disclosure resulting from criminal or other illegal conduct by an employee or third person. Nonetheless, the model is informed by the various legal frameworks and theories discussed thus far.

A. *Threshold Issue—Establish Trade Secret Status*

As a threshold matter, preliminary consideration must be given to determine whether the trade secret owner can reasonably establish that the information in question was entitled to trade secret protection *before* it was misappropriated on the Internet.[168] In particular, the most critical part of that inquiry should be whether the trade secret owner took reasonable steps to preserve the secrecy of the information. This is consistent with the law and practice already required in trade secret misappropriation cases, as the trade secret owner bears the burden of establishing the trade secret status

167. As discussed earlier, the harshness of such a rule is not unique to trade secret law and is supported by both constitutional and patent law principles. *See supra* Part I.B.

168. The standard utilized for this inquiry should be akin to the likelihood of success on the merits standard used in preliminary injunction cases. Most trade secret cases, particularly in the context of the problem presented here, will be decided at a preliminary injunction hearing. Thus, use of this standard should present no further difficulty and may very well fold into the injunction test.

of the information. Furthermore, the extent to which the alleged trade secret information is available or has been disclosed through sources other than the Internet will also be relevant to determining trade secret status.[169]

If the court determines that the trade secret owner is not likely to succeed in proving that the information was a trade secret, then the bright line rule of trade secret disclosure should apply and the inquiry need not proceed any further. That is, the trade secret owner is not entitled to enjoin use of the alleged trade secret information disclosed on the Internet. As a practical matter, this is reasonable in light of the fact that failure to prove trade secret status is fatal to any claim for misappropriation, and is especially so where, as here, the action would involve an independent third party who accessed the information from the public domain.

If a court determines that the information was deserving of trade secret status before it was allegedly misappropriated, then the next step is to determine, via the factors below, whether, despite the disclosure, it has nonetheless retained its trade secret status.[170] The choice to phrase the inquiry in terms of retention of status, rather than loss of status, is deliberate, as it underscores the underlying expectation that retention of trade secret status after disclosure is the exception, not the rule. Accordingly, it is expected that with rigorous application and weighing of these factors, only a very small number of cases would qualify for retention status.

B. The Three Factors

Of the three factors identified below, the first two focus on the trade secret owner and the trade secret. The first factor considers the time interval of trade secret exposure and whether the owner was sufficiently prompt in acting to save the trade secret *after* discovering the disclosure. The second factor looks at whether the trade secret has essentially entered the public domain as a result of the disclosure. In light of the equitable considerations underlying trade secret law, however, it also seems fair to introduce a third factor which considers the recipient's good faith. This factor will

169. *See, e.g.*, Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 1368 (E.D. Va. 1995) (noting that, in addition to having been posted on the Internet, the information was available in a public court file for twenty-eight months).

170. This is consistent with some courts finding that accidental disclosures may not lead to loss of trade secret protection. *See* B.C. Ziegler & Co. v. Ehren, 414 N.W.2d 48, 53 (Wis. Ct. App. 1987). Further, some courts will provide "limited" protection to a trade secret after incidental disclosure. *See, e.g.*, Healthpoint, Ltd. v. Ethex Corp., No. SA-01-CA-646-OG, 2004 WL 2359420, at *32 (W.D. Tex. July 14, 2004); *see also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. f (1995).

specifically answer whether the independent third party has misappropriated the trade secret and therefore should be enjoined. This inquiry is entirely consistent with the definition of misappropriation, which includes consideration of the recipient's knowledge that the information is another's trade secret.[171] The factors ought to be evaluated sequentially, at least to the extent that the first two must be considered before the third.

1. Time and Action

This first factor would require consideration of the amount of time that the information was exposed on the Internet and the promptness of any action by the trade secret owner to have the information removed. More favorable consideration will be given to situations where (a) the information has been posted for a very short period of time (twenty-four to forty-eight hours) *and* (b) the owner discovered the publication and took action immediately (within twenty-four to forty-eight hours) to have it removed. By analogy, given the importance of trade secrets to a business, this factor expects the trade secret owner to treat the discovery of a disclosure as a parent who discovers a child is missing.

In light of the threat to trade secrets posed by the Internet, trade secret owners have an obligation to monitor the Internet for potential wrongful disclosures. Were there any question of the existence of this obligation, the examination of the issues in this Article leaves no doubt that such must be the case. In deciding to choose trade secret protection over other options to protect intellectual property (e.g., patent law), a trade secret owner undertakes this responsibility as part of the bundle of disadvantages associated with trade secret protection.

The amount of time of exposure and promptness of action that will be considered sufficient will depend on the circumstances. However, the rate at which information moves through the Internet dictates that the promptness be correspondingly rapid. Information that has been posted for more than approximately twenty-four to forty-eight hours is much more likely to have become "generally known" and is thus much less likely to meet the test for trade secret protection.

A trade secret owner who discovers the information must respond immediately and can show that it took prompt action by, for

171. This reasoning is also similar to the tipper/tippee theory of liability in insider trading, which extends liability to tippees who trade based on inside information received from a misappropriator, provided that the tippee knows or has reason to know the tipper breached a duty of trust and confidence. *See* 17 C.F.R. § 240.10b5-1 (2006); *see also* Dirks v. SEC, 463 U.S. 646, 660 (1983).

instance, filing a lawsuit, seeking an emergency temporary injunction, contacting the Internet service provider to have the information removed,[172] or sending a cease and desist letter.[173] While this is not an exclusive list, the goal is to separate those who have "slept on their rights" upon discovering the potentially fatal disclosure from those who have acted consistent with the danger that has befallen their business. This requirement also implicitly provides corroborative evidence of the true value of the trade secret to the business.

2. Extent of Disclosure

The second factor considers the extent of the disclosure. This includes not only how much of the trade secret was disclosed, but is also related to the first factor in trying to ascertain the nature of the site on which the information was posted (public availability). It attempts to address the necessary element of whether the secret became "generally known or knowable." It further permits exploration of the premise that "[p]ublication on the Internet does not necessarily destroy the secret if the publication is sufficiently obscure or transient or otherwise limited so that it does not become generally known to the relevant people, i.e., potential competitors or other persons to whom the information would have some economic value."[174]

This factor evaluates the specific site on which the information was posted. A more prominent disclosure on a highly visited webpage might require more prompt action and greater concern than a disclosure on an obscure, members-only chat room with limited membership. If the information was published on a network with controlled access to a specific membership, particularly where the membership is a small, well-defined, and finite group, then this factor weighs in favor of the trade secret owner. If, however, the

172. The tools currently in place for addressing removals from Web sites are not satisfactory given the special concerns posed in these kinds of cases. If trade secret owners are to bear the burden of acting swiftly to remove trade secrets from Web sites, then it is incumbent upon our legal system to provide the appropriate, efficient, and effective mechanisms to do so. A mechanism akin to the Digital Millennium Copyright Act's safe harbor provisions for Internet service providers who post copyright protected materials is a useful starting point. *See* 17 U.S.C. § 512 (2000). The author plans to address this topic in a separate forthcoming paper.

173. The appropriate strategy must be carefully tailored in light of the circumstances. *See* Cundiff, *supra* note 9 (discussing considerations in litigating to remove trade secrets from the Internet).

174. DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 192-93 (Ct. App. 2004).

group consists of precisely the relevant people who would most benefit from the information, then it may be more difficult to argue that the trade secret has not become "generally known." A further reason why a closed network favors retention of the trade secret is that the members' identities are known, and it might be easier to obtain injunctive relief against them.[175]

The amount of secret information that was disclosed may also be probative of whether the information deserves to retain its trade secret status. In circumstances where only portions of the trade secret were disclosed and the remaining undisclosed portions continue to maintain their competitive value to the trade secret owner, a court could find that the trade secret protection has not been completely lost.[176]

This examination of the extent of the disclosure is supported by non-Internet related cases that require something more than mere public accessibility of the trade secret, namely publication, before finding loss of the protection. For instance, in cases addressing unsealed filing of trade secret information in public court records, evidence of further publication of the trade secret is required to destroy trade secret protection.[177] Admittedly, the nature of the Internet—unlike a public court file in a court house—is such that publication to the relevant public can be virtually instantaneous, and, as such, there is a significantly smaller window of opportunity for the trade secret owner to protect the secret status of the information. Nonetheless, this factor allows for a court to give a thoughtful assessment to the extent of exposure, rather than a presumption that the disclosure (particularly in isolation) destroyed the secret.

3. *Recipient's Reason to Know the Information Was a Trade Secret*

This final factor turns from the trade secret owner's actions to the recipient's state of mind and is an important part of the definition of misappropriation. Related to the first factor, if the trade secret owner provided notice to the recipient in a timely fashion that the information was a trade secret, then the acquisition by "improper means" may be a stronger case. Furthermore, if the

175. *See* Lambrecht, *supra* note 9, at 338.

176. *See* Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 923 F. Supp. 1231, 1257 (N.D. Cal. 1995); Smokenders, Inc. v. Smoke No More, Inc., No. 73-1637, 1974 WL 20234 (S.D. Fla. Oct. 21, 1974).

177. *See* Hoechst Diafoil Co. v. Nan Ya Plastics Corp., 174 F.3d 411, 418-19 (4th Cir. 1999) (discussing cases dealing with disclosure of trade secrets in court files); *see also* Gates Rubber Co. v. Bando Chem. Indus., Ltd., 9 F.3d 823, 849 (10th Cir. 1993).

evidence independently suggests that the recipient knew or should have known the trade secret status of the information, then this factor will weigh in favor of the trade secret owner.

Under the UTSA, one is liable for misappropriation if "he obtains information from a third person and then 'discloses or uses' that information, knowing, or possessing information from which he should know, at the time of disclosure or use that the information is a trade secret and that it had been misappropriated by the third person."[178] The defendant's knowledge that the information was a trade secret is also evidence of misappropriation under the *Restatement of Torts*.[179] Circumstantial evidence can be weighed to determine the likelihood that the defendant knew the acquisition was wrongful, and a defendant cannot shield himself by "studious ignorance of pertinent 'warning' facts."[180] Defendant's constructive notice that the information was a trade secret is sufficient.[181] The *Restatement*'s definition of notice provides guidance:

> One has notice of facts . . . when he knows of them or when he should know of them. He should know of them if, from the information which he has, a reasonable man would infer the facts in question, or if, under the circumstances, a reasonable man would be put on inquiry and an inquiry pursued with reasonable intelligence and diligence would disclose the facts.[182]

Accordingly, if the evidence suggests that a reasonable person would have been on notice[183] that the information received was the wrongfully disclosed trade secret of another, then the defendant should be liable for misappropriation.[184]

Even though the burden of proof remains with the trade secret owner to prove the defendant's guilty state of mind, it will be important for the defendant to marshal facts to effectively prove a negative: that she did not have reason to know the information was a trade secret. In doing so, she may rely on the argument that the trade secret, through its posting, had become generally available. In

178. IMED Corp. v Sys. Eng'g Assocs. Corp., 602 So. 2d 344, 346 (Ala. 1992) (interpreting state version of the UTSA).

179. *See id.* at 346-49; *see also supra* Part IV.B.

180. Curtiss-Wright Corp. v. Edel-Brown Tool & Die Co., 407 N.E.2d 319, 324 (Mass. 1980).

181. *See* C&F Packing Co. v. IBP, Inc., No. 93C1601, 1998 U.S. Dist. LEXIS 3221, at *19 (N.D. Ill. Mar. 16, 1998).

182. RESTATEMENT (FIRST) OF TORTS § 757 cmt. *l* (1939) (citation omitted).

183. This generally refers to notice at the time of the disclosure. However, notice from the trade secret owner after the initial disclosure may also suffice. *See C&F Packing Co.*, 1998 U.S. Dist. LEXIS 3221, at *17.

184. *See id.* at *19.

expressing that position, it is important to try to avoid the tautological reasoning that has befallen some courts, i.e., whether the information was a trade secret in the first place.[185] Thus, the line between the defendant's state of mind and the general availability of the information may become blurred in the analysis. As one court noted, for instance:

> In a case that receives widespread publicity, just about anyone who becomes aware of the contested information would also know that it was allegedly created by improper means. . . . [I]n such a case the general public could theoretically be liable for misappropriation simply by disclosing it to someone else. This is not what trade secret law is designed to do.[186]

One value of this model and the factors presented here is that the question of whether information qualifies as a trade secret would have already been answered positively as a threshold matter. Thus, at this point in the model, an analysis of the facts supporting the defendant's state of mind would be separate from that question.[187] Evidence of the defendant's state of mind relative to the trade secret status of the information will also depend on the particular circumstances and will consider any bad faith on the part of the defendant. A defendant could also present any First Amendment or other defenses at this juncture.

Evidence of the trade secret owner's proactive steps or prior relationship with the defendant may also bear on the defendant's bad faith or culpable knowledge. Materials that are clearly labeled and stamped indicating that they are confidential, proprietary, or a trade secret will be helpful.[188] Evidence that this particular defendant has previously tried, legitimately or illegitimately, to obtain the trade secret from the owner may also be relevant. Attempts to extort benefits from the trade secret owner in exchange for returning the materials will also signal culpability.[189] Finally,

---

185. *See, e.g.*, DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 194 (Ct. App. 2004) (suggesting that knowledge about the unethical origin of the information is insufficient to prevent use of information that has become publicly available).

186. *Id.*

187. This knowledge requirement is consistent with the criminal claim for theft of trade secrets found in the Economic Espionage Act, which requires that the defendant knowingly stole or otherwise obtained the trade secret information. *See* 18 U.S.C. § 1832 (2000).

188. *See, e.g.*, O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 79 (Ct. App. 2006) (noting that electronic slides were "conspicuously marked as 'Apple Need-to-Know Confidential'").

189. *See, e.g.*, Ford Motor Co. v. Lane, 67 F. Supp. 2d 745, 747, 753 (E.D. Mich. 1999) (defendant threatened to publish "disturbing" materials about

evidence that the defendant knew the trade secrets were obtained in violation of a confidentiality agreement, license agreement, or a fiduciary obligation weighs in favor of the plaintiff.[190]

If someone other than the original misappropriator posted the information (and is the first to do so), then she, as the publisher, ought to be in a worse position than the independent third party who discovers the posting.[191] That person or entity is likely to fall within a conspiracy-type analysis for obtaining the secret from the misappropriator with knowledge of the wrongful acquisition.[192] Receiving the information directly from the original misappropriator or an associate/agent, and deciding to post it, carries, at the very least, a taint of misappropriation.[193] Posting the information does not purge that taint and precludes the poster, like the original misappropriator, from claiming that the information has now become generally known and is not a trade secret.[194]

---

plaintiff on his Web site and to solicit trade secrets from plaintiff's employees).

190. *See, e.g.*, DVD Copy Control Ass'n v. Bunner, 75 P.3d 1, 7-8 (Cal. 2003) (discussing how trade secrets were obtained through reverse engineering in violation of license agreement and that defendants knew of this improper means of acquiring the trade secret).

191. This would encompass owners and operators of Web sites who make decisions about what materials to publish on their sites. Analogous to their traditional media counterparts, newspaper and magazine editors and reporters for instance, they could be liable to the trade secret owner and subject to an injunction. This is an unsettled area of the law, however, and the argument espoused here appears to be novel. *See* O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 99-106 (Ct. App. 2006) (reasoning that operators of Web sites are "publishers"); *see also* Bartnicki v. Vopper, 532 U.S. 514 (2001) (addressing whether the media may be liable for using information unlawfully obtained by a third party); MARC A. FRANKLIN, DAVID A. ANDERSON, & LYRISSA BARNETT LIDSKY, MASS MEDIA LAW CASES AND MATERIALS 536-547 (7th ed. 2005). *But see* Procter & Gamble Co. v. Bankers Trust Co., 78 F.3d 219, 225 (6th Cir. 1996) (refusing to enjoin publication of trade secrets improperly obtained in violation of a protective order); Ford Motor Co. v. Lane, 67 F. Supp. 2d 745, 753 (E.D. Mich. 1999) (refusing to enjoin publication where no fiduciary duty or confidentiality agreement exists).

192. *See* Lockridge v. Tweco Prods., Inc., 497 P.2d 131, 135 (Kan. 1972).

193. *Cf.* Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 1369 (E.D. Va. 1995) ("Because there is no evidence that The Post abused any confidence, committed an impropriety, violated any court order or committed any other improper act in gathering information from the court file or down loading information from the Internet, there is no possible liability for The Post in its acquisition of the information."). Some Supreme Court cases also support the proposition that the conduct of a publisher may be taken into consideration in deciding whether to grant First Amendment protection. *See, e.g.*, Cohen v. Cowles Media Co., 501 U.S. 663 (1991); Seattle Times Co. v. Rhinehart, 467 U.S. 20 (1984).

194. *See* Underwater Storage, Inc. v. U.S. Rubber Co., 371 F.2d 950, 955

VIII. SUMMARY AND APPLICATION OF THE SEQUENTIAL PRESERVATION MODEL

To more clearly illustrate the connection between the components of the model and their theoretical underpinnings, I present the summary below. In the subpart that follows I then work through some of the case examples to illustrate application of the model.

A. Theoretical Checklist of the Model

A court faced with an Internet disclosure problem can utilize this model (in conjunction with application of the preliminary injunction standard)[195] to determine whether the trade secret status of the information has been preserved and whether to enjoin an independent third party. One value of this process is that it provides for deliberate consideration of the trade secret law requirements, avoiding automatic and potentially erroneous assumptions on a case by case basis.

A. Was the disclosed information deserving of trade secret protection before it was posted on the Internet? This is the threshold determination. If the answer is no, there is no need to apply the model; there cannot be misappropriation and an injunction cannot issue. If yes, proceed to the rest of the model.

B. Did the information retain its trade secret status despite the Internet posting? To answer this question, apply the first two factors—time and action and the extent of disclosure—to the facts of the case. If the answer is no, end the analysis; there cannot be misappropriation or an injunction for that which is not a trade secret. If yes, proceed to the final step.

C. Was there misappropriation by the defendant independent third party? To answer this question, apply

---

(D.C. Cir. 1966) ("Once 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."); *see also Lockridge*, 497 P.2d at 135 ("We do not believe that a misappropriator or his privies can 'baptize' their wrongful actions by general publication of the secret."); *cf.* Jerome Stevens Pharms., Inc. v. FDA, 402 F.3d 1249, 1254 (D.C. Cir. 2005) (holding that where FDA had posted plaintiff's trade secrets on its Web site without authorization, it could still be liable for misappropriation even though the trade secrets had been publicly available on the Web site for five months).

195. *See generally* Rowe, *supra* note 7, at 201-07 (discussing implications of seeking injunctive relief in a misappropriation case).

the third factor—recipient's reason to know the information was a trade secret. If the answer is yes, an injunction should issue; otherwise, there is no trade secret liability and an injunction is not appropriate.

B. *Application with Case Examples*

The case examples below illustrate the impact of the various phases of the model. For ease of reference, I have used cases that have already been discussed in this Article, which also happen to be among the main cases of relevance in this area. Relying on the facts as reported in the respective opinions is limiting insofar as we are bound by the context and posture of the case as it was originally presented. Taken together, however, they are nonetheless useful for illustrating various aspects of the model. In some instances the original outcome of the case is consistent with the outcome that would have been achieved using the model. That may very well be because of the court's attempt to reach an equitable result, rather than a more principled reasoning process, such as that offered by the sequential preservation model.

1. Religious Technology Center v. Lerma

This case likely fails the threshold part of the model because the information arguably lost its trade secret protection before Lerma posted it on the Internet (and thus well before the *Post* obtained it). The documents were present in an open court file for about twenty-eight months prior to Lerma's Internet publication,[196] signifying a failure to protect the secret status of the information. The court could have been persuaded, however, by the Church's argument that the appearance in the court file was beyond its control and despite its best efforts. Indeed, not only had the Church filed a motion seeking that the court seal the file,[197] but after denial of that motion it took the extraordinary precaution of having a church member check out the court file every day to prevent others from seeing it.[198]

Even if a court were swayed by that argument, and the analysis moved to the second part of the model, it would certainly fail at this stage. In considering the first two factors of the model, the fatal blow would be dealt by the fact that before the *Post* acquired the information for its story, the documents had been posted on the Internet (by Lerma) for more than ten days[199] (exceeding the twenty-

196. *See* Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 1368 (E.D. Va. 1995).

197. *Id.* at 1364.

198. *Id.* at 1365.

199. *Id.* at 1368.

four to forty-eight hour guideline suggested in the model) on a publicly available Web site and would thus be generally known.[200] Accordingly, the model would direct that the trade secret status of the information had not been preserved. The court's holding that the *Post's* actions did not constitute misappropriation is consistent with the outcome under the model.

2. DVD Copy Control Ass'n v. Bunner

Whether the disclosed information in this case was deserving of trade secret protection before it was posted on the Internet by Bunner is a question that the court ought to have addressed in greater detail.[201] The precise information that the plaintiff claimed as a trade secret was DeCSS, which plaintiff had not, in fact, created, but rather had been created through reverse engineering.[202] Because a person may lawfully reverse engineer another's trade secrets,[203] and given that the defendants in this case had not themselves reverse engineered the plaintiff's code, it is highly questionable that the DeCSS should have been entitled to trade secret protection.[204] Moreover, the evidence suggests that by the time Bunner posted the code on his Web site, it had already been "distributed to a worldwide audience of millions."[205] Accordingly, a rigorous analysis under the model would have failed the threshold.

Since the court assumed, however, that the reverse engineered code was entitled to trade secret protection, then the analysis would proceed to the second part of the model. After discovering his posting, it took DVD CCA approximately two months to file a legal action against Bunner.[206] Such delayed action would not survive the prompt action required under the model. Further crippling the

200. *Id.*

201. In one sentence, the court notes, "We have only very thin circumstantial evidence of when, where, or how [the reverse engineering] actually happened or whether an enforceable contract prohibiting reverse engineering was ever formed." DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 194 (Ct. App. 2004).

202. *Id.* at 188.

203. *See supra* Part II.A.

204. The plaintiff claimed that the reverse engineering occurred in breach of a license agreement. *DVD Copy Control Ass'n*, 10 Cal. Rptr. 3d at 188. Nevertheless, under the facts of the case, the presence of a trade secret is dubious. *See also* Pamela Samuelson, Principles for Resolving Conflicts Between Trade Secrets and the First Amendment (Aug. 9, 2006) (unpublished draft manuscript), *available at* http://www.ischool.berkeley.edu/~pam/papers/TS%201st%20A%204th%20dr.pdf (discussing use of mass market licenses to override the reverse engineering privilege of trade secret law).

205. *DVD Copy Control Ass'n,* 10 Cal. Rptr. 3d at 193.

206. *Id.* at 188.

plaintiff at this stage is the extensive level of disclosure: "by the time [the] lawsuit was filed hundreds of Web sites had posted the program, enabling untold numbers of persons to download it and to use it."[207] Consequently, there was no preservation and no trade secret to misappropriate. The court's denial of an injunction fits the model.[208]

3. O'Grady v. Superior Court

Although the focus of this case was on resolving a discovery dispute[209] rather than deciding a trade secret misappropriation case, the facts provide a useful illustration for the model. The case presents some thorny issues, the implications of which are worth wrestling with under the model, even if only at the margins. More specifically, unlike the other cases discussed in this Part, here, the third party, O'Grady, did not obtain the alleged trade secrets from an Internet posting, but rather was the first to post the information on the Internet after having obtained it elsewhere.[210]

The less challenging part of the analysis is that the threshold determination is more easily met here than in the two prior cases. Apple Computer, Inc.'s ("Apple") plans to release a new product would likely qualify for trade secret protection before it was posted by O'Grady or sent to him by e-mail. Some of the information was derived from an Apple electronic presentation clearly labeled "Apple Need-to-Know Confidential," and Apple would have demonstrated that it "undertakes rigorous and extensive measures to safeguard information about its unreleased products."[211] Apple was further prepared to show that the information "could have been obtained only through a breach of an Apple confidentiality agreement."[212] Given all of these indicia of steps to protect the secrecy of the information and of its competitive value to the company, the threshold requirement would be satisfied.[213]

---

207. *Id.* at 195.

208. Under the reasoning stemming from the model, the defendant's First Amendment defense would not have been reached because there would be no need to invoke the third part of the model (which would have considered defendant's state of mind and defenses).

209. Petitioners in the case sought a protective order to prevent Apple Computer, Inc. from discovering the identities of anonymous persons who had provided allegedly trade secret information to them about Apple's plans to release a new product. O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 76 (Ct. App. 2006). The petitioners posted the information on their Web sites. *Id.* at 76-79.

210. *Id.*

211. *Id.* at 79-80.

212. *Id.* at 80.

213. While distinguishing *Bunner*, the court, in the context of its First

At this point the retention analysis becomes complicated. O'Grady does not fit the third party who finds the trade secret on the Internet mold because he allegedly received the trade secret information via e-mail from Apple insiders.[214] Accordingly, the underlying principles supporting the model would suggest that we bypass the question of retention and proceed to the misappropriation inquiry.[215] In analyzing O'Grady's state of mind and reason to know that the information was a trade secret, a court should weigh such factors as the "taint" associated with his having received (and perhaps solicited) the trade secrets from Apple insiders against him.[216] As a publisher, however, he would be entitled to raise a First Amendment defense regarding the newsworthiness of the disclosure and ultimately may prevail.

Finally, permit me to indulge in one more modification in order to create a true third-party Internet disclosure scenario and engage in a retention analysis under the model. Assume that an Apple competitor discovered the product release plans from O'Grady's

---

Amendment analysis, suggests that certain types of information are more worthy of trade secret protection than others. In particular, the court mentions that the kind of information at issue here (plans to release a product) may not rise to the same level as technical information about how to create the product. *Id.* at 113. While that kind of reasoning might be of some merit (albeit limited) in a First Amendment analysis of newsworthiness, *see id.* at 113-15, it is not appropriate for determining whether information is entitled to trade secret protection in the first instance. The UTSA and other applicable trade secret frameworks already provide the criteria for such determinations, and those ought to be sufficient. There is no sliding scale: either something is a trade secret or it is not. As even the *O'Grady* court has expressed in reference to information that is worthy of publication, "courts must be extremely wary about declaring what information is worthy of [trade secret protection] and what information is not" because to do otherwise would undermine trade secret law. *Id.* at 114.

214. *See id.* at 83-84.

215. Although e-mails involve use of the Internet, they generally do not rise to the same level as Internet postings for the purposes of the analyses presented in this paper. Because they are typically directed to a relatively small number of people or a finite group, e-mails do not generally have the instant mass dissemination quality of an Internet posting on a publicly available Web site. (I recognize, however, that spam e-mails and the ability of recipients to forward e-mails to others in virtually unlimited fashion, could be problematic. Thus, in the event a trade secret is disseminated in this fashion, the analysis may be affected). Accordingly, the likelihood of the information having entered the public domain and having lost its trade secret status is not as strong when transmitted by e-mail. As a result, the theoretical framework would more closely resemble non-third party Internet cases and proceed to the misappropriation finding, once the trade secret owner has established key elements such as value and secrecy.

216. *See supra* notes 191-94 and accompanying text.

postings, and Apple files a misappropriation action against the competitor. The facts of the case would suggest that the trade secret would not be preserved.

The retention inquiry would focus on Apple's reaction to O'Grady's postings, and the nature of those postings. O'Grady's articles about the new product ran on five separate days, and Apple's first "cease and desist" contact to O'Grady came nineteen days after the first article appeared.[217] It took five more days after that to file the complaint.[218] While this may have been relatively prompt action for a plaintiff merely seeking to identify the sources of a breach of confidentiality, it is not enough for one seeking to prevent information from becoming generally known to the relevant public. The fact that O'Grady's Web site was "devoted to news and information about Apple Macintosh computers" leaves little doubt that the trade secret reached the relevant people.[219]

The nature and amount of information disclosed would also weigh against Apple. To the extent it claims its plan to release this particular product as a trade secret in order to control "timing and publicity for its product launches,"[220] then O'Grady's articles stole its thunder and there was nothing left of the secret to preserve. The trade secret would therefore be lost, and the competitor would be entitled to use it.[221]

4. United States v. Genovese

As a result of its procedural posture and context, this case does not provide sufficient relevant details to work through each sequence of the model.[222] It does, however, provide a useful illustration for the third part of the model, and as such, I will make certain assumptions and draw inferences where the voids exist. First among those assumptions is that the Microsoft source code was a trade secret before it was posted on the Internet. Genovese himself "acknowledged both that the source code was proprietary to Microsoft and that someone else penetrated whatever safeguards

217. *See O'Grady*, 44 Cal. Rptr. 3d at 80.

218. *Id.*

219. *Id.* at 77.

220. *Id.* at 80.

221. Assuming, arguendo, that Apple had acted within twenty-four hours of the first article to stem further publication about the new product, then there may have been a better chance of preserving the secret. In keeping with the court's reasoning, O'Grady's First Amendment arguments in the final part of the model, however, may have saved him from a misappropriation finding.

222. It is a ruling on a motion to dismiss a criminal indictment under the EEA. *See* United States v. Genovese, 409 F. Supp. 2d 253, 254 (S.D.N.Y. 2005).

Microsoft enlisted to protect it."[223]

There are essentially no facts from which to determine whether the source code retained its trade secret protection by the time Genovese found it on the Internet.[224] I will, therefore, assume that the facts (similar to the hypothetical presented at the beginning of the paper) would show that Microsoft acted with the requisite promptness to stem the dissemination of the code and that the extent of the disclosure was minimal,[225] thereby preserving the trade secret status of the information.

Finally, we would arrive at the misappropriation stage of the model and examine Genovese's reason to know that the source code was a Microsoft trade secret and the presence of any bad faith. On that point, the evidence exists and weighs in favor of Microsoft. The court notes that Genovese (a) describes the code as "jacked,"[226] (b) indicates that others would have to "look hard" to find it elsewhere,[227] (c) was on notice that Microsoft had not publicly released the code,[228] and (d) offers the code for sale and successfully sells it because of its relative obscurity.[229] It is also highly unlikely that he would succeed on a First Amendment defense, given that he was behaving more as a salesman than a reporter. Accordingly, this would present an appropriate case for an injunction.

IX. REMEDIES

A court, finding misappropriation after hearing the facts and weighing the factors presented above should issue an injunction.[230] The scope of that injunction will vary depending on the particular circumstances.[231] Removal of the information from the Web site (if it

223. *Id.* at 258.

224. *Id.* at 254-55. The opinion does not indicate, for instance, the Web site from which he downloaded the code, how long it appeared on the site, what action (if any) Microsoft undertook to remove the information from that site, and with what degree of promptness.

225. In attempting to sell the source code, Genovese indicated that "others would have to 'look hard' to find it elsewhere." *Id.* at 257.

226. An abbreviation for "hijacked," which the court interpreted to mean "stolen" or "misappropriated." *Id.* at 257 n.3.

227. *Id.* at 257.

228. *Id.*

229. *Id.*

230. Where the defendant has made use of the trade secret, a court could also order monetary damages in addition to an injunction. *See* EPSTEIN, *supra* note 13, at § 3.02[B].

231. The three types of injunctions in trade secret cases are (1) prohibitions against disclosure or use, (2) sanctions against engagement in competitive employment, and (3) bans on the manufacture of products in which the trade secret is an essential ingredient. DAN B. DOBBS, LAW OF REMEDIES § 10.5(3), at

has not already occurred) would certainly be necessary.[232] A court could further enjoin the recipient from using the information, at least for a certain period of time. While this does not erase the information from the hands of a competitor, it could at least mitigate some of the damage by delaying use of the information in a manner that would allow the defendant to compete unfairly with the trade secret owner.[233] The injunction should also prohibit the defendant and her agent from further disseminating the information.

A more difficult problem for the trade secret owner, however, would be that members of the public, other than those named in the suit, could not be enjoined from using the information.[234] Because law and public policy favor the unfettered use of information in the public domain, and courts likely lack jurisdiction to enjoin non-parties in a lawsuit, the trade secret owner's prospects for containing use of the information are bleak.[235]

A trade secret owner can pursue a misappropriation claim against the original misappropriator (if known) and may also have claims against those who aided and abetted the misappropriation. Thus, to the extent the information was posted by someone other than the original misappropriator, that person may also be liable. Even if the misappropriator may have succeeded in destroying the trade secret status of the information vis-à-vis others, trade secret law does not permit him or her to benefit from use of the information.[236] Thus, for instance, such a person is not entitled to claim immunity on the basis that the information is no longer secret. Assuming, as is often the case, that the misappropriator does not have deep pockets, a victory against him may be hollow and unsatisfying for a trade secret owner who now suffers the

730-31 (2d ed. 1993).

232. Note that a "cached" version of information may continue to reside in search engines even after the information has been removed from an active page. Cundiff, *supra* note 9, at 351.

233. *See* DVD Copy Control Ass'n v. Bunner, 10 Cal. Rptr. 3d 185, 194 (Ct. App. 2004).

234. *See* United States v. Kirschenbaum, 156 F.3d 784, 794 (7th Cir. 1998) ("A district court may not enjoin non-parties who are neither acting in concert with the enjoined party nor are in the capacity of agents, employees, officers, etc. of the enjoined party."); *see also* Additive Controls & Measurement Sys., Inc. v. Flowdata, Inc., 154 F.3d 1345, 1351 (Fed. Cir. 1998).

235. *See DVD Copy Control Ass'n*, 10 Cal. Rptr. 3d at 194 (noting that an injunction is inappropriate where the information is no longer secret). A trade secret owner may consider turning to other areas of law for relief or to criminal prosecution. Depending on the nature of the trade secret information, copyright laws, for instance might be an alternative avenue.

236. *See* Lockridge v. Tweco Prods., Inc., 497 P.2d 131, 135 (Kan. 1972).

permanent loss of its trade secret.[237]

Given the current status of the law, it becomes clear that a trade secret owner's best and most effective weapon is protection of the trade secret information to prevent disclosure in the first place.[238] This requires absolute vigilance and knowledge of potential threats, among the most dangerous of these being the Internet. In the event that a disclosure is made despite best efforts, prompt action in addressing the situation is critical.[239] Since trade secret owners have the legal burden of proving the trade secret status of their information when they seek to enforce protection, it is incumbent upon them to be mindful of that burden long before litigation arises. Otherwise, it may be too late once the milk has been spilled.

X. CONCLUSION

At the outset of this Article, I presented the hypothetical involving Soft Corporation. Where a trade secret, such as the source code for a program, is stolen from its owner and posted on the Internet, the default rule would be that it becomes a free for all. By virtue of the fact that it has been posted, it becomes public and, consequently, loses its trade secret protection. The ensuing result is that independent third parties, including competitors, are entitled to use it, and the trade secret owner, despite years of laudable efforts to maintain the secret, suffers a fatal loss at the hands of a wrongdoer. The apparent injustice in that conclusion does not go unnoticed.

---

237. *See DVD Copy Control Ass'n*, 10 Cal. Rptr. 3d at 195.

238. Trade secret owners can take such proactive steps as entering into clear and specific non-disclosure agreements with employees and other authorized persons, limiting disclosure of information to a need-to-know basis, clearly marking documents as confidential and trade secret, and monitoring employees. *See generally* Rowe, *supra* note 7, at 192 n.171, 208, 213 (2005); Cundiff, *supra* note 9, at 353-54.

239. This is consistent with some courts finding that accidental disclosures may not lead to loss of trade secret protection. *See, e.g.*, Healthpoint, Ltd. v. Ethex Corp., No. SA-01-CA-646-OG, 2004 WL 2359420, at *32 (W.D. Tex. July 14, 2004); B.C. Ziegler & Co. v. Ehren, 414 N.W.2d 48, 53 (Wis. Ct. App. 1987); *see also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. f (1995). In light of the unique and potentially destructive power of the Internet, trade secret owners should also be provided with the necessary legal tools and resources with which to exercise their duty of vigilance and to facilitate removal of trade secret information that has been posted or where posting is imminent. In that regard, legislative action may be necessary to ensure that the laws that regulate the Internet and Internet providers incorporate considerations of the danger the Internet poses to trade secrets and, more generally, businesses.

Given that trade secret law is intended to regulate the moral and ethical pulse of competitive commercial behavior, this Article set out to explore the problem presented by trade secret Internet disclosures and to identify whether, at least in some circumstances, it may be possible to retain trade secret status after a disclosure. Review of the various legal theories supports the general rule that trade secret status is lost upon disclosure. Nevertheless, considering the equitable and doctrinal considerations underlying trade secret law and drawing from analogous attorney-client privilege cases, there is support for an argument that trade secret status may be saved in some circumstances.

Accordingly, I presented a model comprised of three factors, which may be used as a guide to decide which cases qualify for this exception. The model is drawn from and supported by the various legal issues surrounding the problem. While, in reality, it may only save a small number of cases from the general rule, its value lies in its use as an instrument that may be applied by courts to yield consistent results. It provides an avenue to work within the existing constraints of trade secret law to hopefully achieve more just results in compelling cases. It illustrates that "[t]he Internet, as a mode of communication and a system of information delivery is new, but the rules governing the protection of property rights, and how that protection may be enforced under the new technology, need not be."[240]

240. Pavlovich v. Superior Court, 109 Cal. Rptr. 2d 909, 912-13 (Ct. App. 2001).

***