

**INTRODUCING A TAKEDOWN FOR  
TRADE SECRETS ON THE INTERNET**

ELIZABETH A. ROWE\*

- I. Introduction..... 1042
- II. Background: Trade Secrets on the Internet ..... 1046
- III. A Takedown for Trade Secrets Merits Consideration..... 1049
- IV. Section 512 of the DMCA ..... 1052
  - A. The Formation of the DMCA ..... 1052
  - B. Details of the DMCA Safe-Harbor Provision..... 1056
  - C. Section 512 Protection in a Nutshell ..... 1058
  - D. Summary of DMCA Criticisms ..... 1060
- V. Anatomy of the Legislation ..... 1061
  - A. Safe Harbor ..... 1062
  - B. Dealing with Frivolous Requests ..... 1063
  - C. Carveout for Mere Conduits..... 1065
  - D. Carveout for the Press..... 1065
  - E. Subpoena Provision ..... 1066
  - F. Counternotice Not Required ..... 1067
  - G. Strict Compliance Required ..... 1069
  - H. Prospective Application ..... 1070
- VI. Other Potential Concerns ..... 1071
  - A. First Amendment Objections ..... 1071
    - 1. The Statute Operates as a Prior Restraint on  
Speech ..... 1074
      - a. Internet Posters Analogous to Traditional  
Media? ..... 1075
      - b. Adequate Safeguards ..... 1076
      - c. Lesser Protection for Commercial Speech ..... 1077
    - 2. The Statute Acts as a Punishment for Lawfully  
Obtained Truthful Information About a Matter of

---

\* Assistant Professor of Law, University of Florida, Levin College of Law. I am very grateful to Scott Baker, Alfred Brophy, Christine Farley, Christine Klein, Lyrissa Lidsky, John Nagle, Bill Page, and Sharon Rush for comments on earlier drafts of this Article. I also thank, for their comments, participants at the Jurisgenesis 2007 conference, hosted by Washington University and St. Louis University Schools of Law, the SEALS New Scholars Workshop, and the 2007 Intellectual Property Scholars Conference, hosted by DePaul University College of Law. Finally, for research assistance I gratefully acknowledge Allison Imber, who worked diligently from the inception of this project, as well as Todd Rich and Gary Sobolevskiy, who subsequently joined the team.

Public Significance ..... 1078

    a. Unlawfully Obtained..... 1079

    b. Public Significance..... 1080

    c. An Observation on the Public-Versus-Private-  
        Concern Labels..... 1081

    d. Trade Secrets as Quasi-Property..... 1083

    B. Trade-Secret-Identification Issues ..... 1085

    C. Technological Puzzles ..... 1085

    D. International Materials..... 1088

VII. Conclusion..... 1089

I. INTRODUCTION

Late on a Friday afternoon in October, Wal-Mart executives discover that the content of their sales circulars for the entire Christmas season has just been posted on fatwallet.com, a bargain-shoppers discussion forum. The posted content includes Wal-Mart’s closely guarded sale prices. Fearing that competitors may use the valuable pricing information to compete unfairly, Wal-Mart’s attorneys immediately contact the operators of the Web site to request that they remove Wal-Mart’s trade-secret information. The operators refuse. They contend, correctly, that since the information is not copyrighted, they have no obligation to remove it under the Digital Millennium Copyright Act (DMCA), which does not cover trade secrets. The information remains posted throughout the weekend and for another four days until Wal-Mart obtains a temporary restraining order from the court to have the material removed. By then, however, overjoyed shoppers have distributed the circulars all over the Internet, and, using this information, Wal-Mart’s competitors are modifying their planned promotions.<sup>1</sup>

This Article explores, for the first time, an existing void in trade-secret law. When a trade-secret owner discovers that its trade secrets have been posted on the Internet, there is currently no legislative mechanism by which the owner can request that the information be taken down. The only remedy to effectuate removal of the material is to obtain a court order, usually either a temporary restraining order or a preliminary injunction.<sup>2</sup> When a trade secret appears on the Internet,

---

1. This hypothetical is loosely based on a real event. Eddan Katz, *Bargain Shoppers Chilled by Retailers’ DMCA Threats*, CHILLING EFFECTS CLEARINGHOUSE, Nov. 22, 2002, <http://www.chillingeffects.org/weather.cgi?WeatherID=280>.

2. See, e.g., *DVD Copy Control Ass’n, Inc. v. Bunner*, 75 P.3d 1, 7–8 (Cal. 2003) (requiring plaintiff to file suit against Web-site operators after they ignored

2007:5 *Takedown for Trade Secrets on the Internet* 1043

the owner often loses the ability to continue to claim it as a trade secret and to prevent others from using it.<sup>3</sup> Accordingly, trade-secret owners bear the burden of being vigilant and acting quickly if there is to be any chance of preserving the trade-secret status of the information. The current requirement of a court order for a takedown not only is costly but also is too slow for trade-secret owners because of the speed with which users distribute information over the Internet. Obtaining a temporary order from a court would likely take no fewer than several days.<sup>4</sup>

Given that secrecy is vital to preserving trade-secret status, time is of the essence to trade-secret owners, and each hour that a trade secret is available on the Internet is an hour too long. In order to address this time-lapse problem, this Article explores a proposal for trade-secret takedown legislation similar to that which provides for the immediate removal of suspected copyright violations under the DMCA. A takedown provision for trade secrets would provide self-regulation and privatized enforcement in an effort to permit trade-secret owners to save their trade secrets from near-certain death on the Internet. A takedown provision would offer an expedited process for disabling access to trade-secret information in the interim period between discovery of the misappropriated material and issuance of a ruling by a court.

The threat of trade secrets appearing on the Internet occurs with sufficient frequency<sup>5</sup> and potentially poses grave threats to trade-secret

---

the plaintiff's request to remove the plaintiff's allegedly trade-secret information from their Web sites). Another procedural approach might be to file an in rem action seeking removal of the posting. See Victoria A. Cundiff, *Trade Secrets and the Internet: Preventing the Internet from Being an Instrument of Destruction*, in 12TH ANNUAL INSTITUTE ON INTELLECTUAL PROPERTY LAW 403, 412 (PLI Intellectual Property, Course Handbook Series No. G-877, 2006).

3. Elizabeth A. Rowe, *Saving Trade Secret Disclosures on the Internet Through Sequential Preservation*, 42 WAKE FOREST L. REV. 1, 46 (2007) (explaining that, generally, when a trade secret appears on the Internet and becomes public, the owner loses the ability to claim it as a trade secret and prevent others from using it).

4. Plaintiffs seeking injunctive relief in trade-secret cases face a delicate struggle between moving quickly to stem further dissemination of the secret and proceeding with deliberation after careful investigation of the facts and preparation of the pleadings. Otherwise, plaintiffs not only may fail to obtain relief but also may expose themselves to possible sanctions or counterclaims. See generally JAMES POOLEY, TRADE SECRETS § 10.06[1] (1997).

5. See, e.g., *United States v. Lange*, 312 F.3d 263, 265 (7th Cir. 2002) (involving an employee who solicited potential buyers of his employer's trade secrets over the Internet); *United States v. Martin*, 228 F.3d 1, 19 (1st Cir. 2000) (e-mailing trade secrets outside the company without authorization); *O'Grady v. Superior Court*, 44 Cal. Rptr. 3d 72, 76 (Cal. Ct. App. 2006) (seeking identity of sources who disclosed Apple's trade secrets); *Religious Tech. Ctr. v. Netcom On-Line Commc'ns*

owners and the functioning of the economy. Thus, the threat merits action or at least an open discussion. The fact that no less than forty-two amicus briefs supporting the trade-secret owner were filed in *DVD v. Bunner*, a significant trade-secret-disclosure case, is but one salient indication of this issue's importance to industry.<sup>6</sup>

Indeed, there might be an even larger number of reported trade-secret-disclosure cases were it not for the nature of trade secrets and the lack of a takedown mechanism. Unlike copyright law, which has yielded many instances of reported and unreported cases involving copyright infringement on the Internet,<sup>7</sup> trade-secret law has not provided adequate remedies. This might have caused trade-secret owners who suffered from Internet postings to disguise their claims in copyright clothing in order to request a takedown under the DMCA.<sup>8</sup>

---

Servs., Inc., 907 F. Supp. 1361, 1365–66 (N.D. Cal. 1995) (involving the posting of the Church of Scientology's secret documents); *NewSouth Commc'ns Corp. v. Universal Tel. Co.*, No. CIV.A. 02-2722, 2002 WL 31246558, at \*1, \*9 (E.D. La. Oct. 4, 2002) (e-mailing trade secrets outside the company without authorization); *Edelman v. N2H2, Inc.*, 263 F. Supp. 2d 137, 138 (D. Mass. 2003) (involving a computer researcher seeking declaratory judgment allowing him to post potentially trade-secret information on the Internet); *Chrysler Corp. v. Sheridan*, No. 227757, 2003 Mich. App. LEXIS 312, at \*10 (Mich. Ct. App. Feb. 11, 2003) (mentioning employee's disclosure of Chrysler's confidential information to others, including an online publication); *Ford Motor Co. v. Lane*, 67 F. Supp. 2d 745, 753 (E.D. Mich. 1999) (involving the posting of Ford's secret documents); *United States v. Genovese*, 409 F. Supp. 2d 253, 254 (S.D.N.Y. 2005) (involving the posting of Microsoft source code on the Internet); *Religious Tech. Ctr. v. Lerma*, 908 F. Supp. 1362, 1368 (E.D. Va. 1995) (involving the posting of the Church of Scientology's secret documents); *DVD Copy Control Ass'n, Inc. v. Bunner*, 75 P.3d 1, 1 (Cal. 2003) (posting a secret program regarding encryption of DVDs); *Immunomedics, Inc. v. Doe*, 775 A.2d 773, 774 (N.J. Super. Ct. App. Div. 2001) (seeking identity of individual who posted trade secret on Internet).

6. See Mike McKee, *"Friends" in High Places: In a Sign of What's at Stake, California Justices Deluged with 42 Amicus Briefs in Trade Secrets Dispute*, MIAMI DAILY BUS. REV., Aug. 30, 2002, at A10.

7. In the last three years approximately seventy reported decisions were issued addressing copyright infringement and the DMCA. A search of the Westlaw federal-court-cases database for "'DMCA D.M.C.A.' 'Digital Millennium Copyright Act' & 'copyright infring!'" & "da(last 3 years)" yielded sixty-nine cases. A similar search conducted in the LexisNexis federal-court-cases database yielded seventy-eight cases. The Chilling Effects database contained 1,248 takedown notices related to the DMCA safe harbor provisions. Chilling Effects Clearinghouse, <http://www.chillingeffects.org/graph.cgi> (last visited Oct. 18, 2007).

8. See *infra* note 129 and accompanying text. Indeed, attempting to use the DMCA takedown to address trade-secret harm may have led to liability for misrepresentation. See, e.g., *Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195, 1204 (N.D. Cal. 2004) (finding defendant liable under 17 U.S.C. § 512(f) for misrepresenting potentially trade-secret-protectable information as entitled to copyright protection). Because the takedown provision under the DMCA applies exclusively to copyright law, it may have had the unintended consequence of an overreporting of

2007:5 *Takedown for Trade Secrets on the Internet* 1045

Moreover, because the value of a trade secret lies in its secrecy, most misappropriators who have acquired others' trade secrets and plan to use them for their own competitive advantage have no incentive to publicize the secrets.<sup>9</sup> Thus, historically, trade-secret-misappropriation cases have only implicated disclosure of the secrets in a very limited fashion, such as to a new employer.

The Internet's rise, however, has spawned a motivation to acquire trade secrets for a reason other than competitive advantage—employee revenge. The ease with which virtually anyone can post information on the Internet, coupled with the Internet's "disinhibiting effect"<sup>10</sup> and a general decline in employee loyalty,<sup>11</sup> has allowed disgruntled employees to achieve the ultimate revenge against their former employers by destroying trade secrets. One court noted the shift in the 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."<sup>12</sup> Accordingly, Internet disclosures are likely to become a greater problem than they have been in the past. Trade-secret owners also

---

instances of alleged copyright infringement and a corresponding underreporting of suspected trade-secret-misappropriation cases on the Internet. Thus, trade-secret law has not benefited from the rise in reported cases under the DMCA. Interestingly, a by-product of enacting trade-secret-takedown legislation might be that it alleviates some of the misuse of the DMCA's takedown notices whereby claimants disguise what really are trade-secret claims as copyright infringement in order to make use of § 512. See Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling Effects"?: Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621, 678, 684 (2006) (discussing use of § 512 notices for unfair competition and privacy claims and the extent to which the notices appeared to be used against competitors).

9. See, e.g., *DVD Copy Control Ass'n, Inc. v. Bunner*, 10 Cal. Rptr. 3d 185, 195 (Cal. Ct. App. 2004) (stating that a defendant in a trade-secret case typically "has as much interest as the plaintiff has in keeping the secret away from good faith competitors and out of the public domain").

10. Lyriisa Barnett Lidsky & Thomas F. Cotter, *Authorship, Audiences, and Anonymous Speech*, 82 NOTRE DAME L. REV. 1537, 1575 (2007) (discussing the phenomenon whereby users of the Internet are less inhibited when expressing themselves).

11. See generally Katherine V.W. Stone, *The New Psychological Contract: Implications of the Changing Workplace for Labor and Employment Law*, 48 UCLA L. REV. 519, 552 (2001) (discussing the old psychological contract, which required the employee to give loyalty to the employer in exchange for job security and indicating that it has been replaced with lower expectations from both the employee and the employer); Benjamin Aaron & Matthew Finkin, *The Law of Employee Loyalty in the United States*, 20 COMP. LAB. L. & POL'Y J. 321, 339 (1999) (examining various components of employee loyalty).

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

hesitate to file suits because they fear that such lawsuits will incite even greater discussion or even disclosure of their trade secrets online. One trade-secret owner resorted to filing suit as an anonymous plaintiff in order to avoid further economic harm from the publicity, but the court ultimately prohibited the owner from proceeding anonymously.<sup>13</sup>

Despite the apparent necessity for this kind of legislative mechanism, Congress should tread cautiously to maintain an appropriate balance between protection for trade-secret owners, on the one hand, and the public's right to free expression and the use of information in the public domain, on the other hand. Ultimately, the objective should be for policy makers to create legislation that a trade-secret owner can use as a shield to protect its intellectual property rather than as a sword to suppress publication of embarrassing content.<sup>14</sup> It is also important that Congress tailor any legislation to fit existing trade-secret-law principles in order to ensure consistency in implementation and application by courts. The legislation proposed in this Article keeps these objectives in mind.

Part II of this Article provides relevant background about the law pertaining to trade secrets on the Internet. Part III explains why a takedown provision for trade-secret law merits consideration. Part IV summarizes the DMCA safe-harbor provision. Part V introduces components of trade-secret-takedown legislation while Part VI addresses potential areas of concern, such as the First Amendment and technological challenges. Part VII concludes by arguing that in light of the various considerations explored in the Article, Congress should consider takedown legislation for trade secrets using the DMCA safe-harbor provision as a starting point.

## II. BACKGROUND: TRADE SECRETS ON THE INTERNET

Trade-secret law only protects secret information.<sup>15</sup> The Internet makes information publicly available.<sup>16</sup> Naturally, these opposing

---

13. *Am. Online, Inc. v. Anonymous Publicly Traded Co.*, 542 S.E.2d 377, 385 (Va. 2001) (finding that the plaintiff had not carried its burden of showing special circumstances to justify anonymity, the court granted the ISP's motion to quash).

14. *See Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195, 1205 (N.D. Cal. 2004).

15. *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."). For a more detailed analysis of trade secrets on the Internet, see Rowe, *supra* note 3, at 7–10.

2007:5 *Takedown for Trade Secrets on the Internet* 1047

functions set the stage for conflict. Thus, many courts assume that a trade secret posted on the Internet has become generally known and consequently has lost its trade-secret status.<sup>17</sup> Even when a party posting<sup>18</sup> trade-secret information may not have intended to cause harm to the trade-secret owner, the nature of the Internet is such that the posting could still destroy the secret.<sup>19</sup> Unlike other mass media, the Internet has no editors who scrutinize submissions and decide what materials to publish. Any person sitting at a computer can post information on the Internet, and the posting can result in immediate and irreparable harm. One judge described the problem:

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)

---

16. *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.") (internal citation omitted); *Jerome Stevens Pharms., Inc. v. FDA*, 402 F.3d 1249, 1251 (D.C. Cir. 2005) (stating that trade secrets posted on the FDA's Web site are available to the public); *Am. Booksellers Found. v. Dean*, 342 F.3d 96, 100 (2d Cir. 2003) (stating that posting information to a Web site available to the public is distribution).

17. *See* *Religious Tech. Ctr. v. Netcom On-Line Comm'n Servs., Inc.*, No. C-95-20091 RMW, 1997 U.S. Dist. LEXIS 23572, at \*39-41 (N.D. Cal. Jan. 3, 1997); *Religious Tech. Ctr. v. Lerma*, 908 F. Supp. 1362, 1368 (E.D. Va. 1995). *But see* *DVD Copy Control Ass'n, Inc. v. Bunner*, 10 Cal. Rptr. 3d 185, 190 (Cal. Ct. App. 2004) (finding that the mere posting of information on the Internet does not destroy a trade secret).

18. 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 (Cal. Ct. App. 2006). Posting, therefore, allows direct self-publication of information. A person may also send information to a site, but the owners or moderators of the site of decide what to post. *See id.* at 91 n.15.

19. *See, e.g., Jerome Stevens Pharms., Inc.*, 402 F.3d at 1254-55, 1258 (reversing the district court's dismissal by holding that the FDA could be liable for misappropriation of trade secrets where it posted plaintiff's trade secrets on its Web site for five months and remanding the case to the district court).

defendant can permanently destroy valuable trade secrets, leaving no one to hold liable for the misappropriation.<sup>20</sup>

To make matters worse, the trade-secret owner may never know the identity of the person making the disclosure, and the person posting the information may very well be far removed from the person who originally misappropriated the secret.

Under very limited circumstances a trade-secret owner might be able to save its trade secret from the near-certain death sentence imposed by the Internet.<sup>21</sup> Critical to this preservation model, however, is how long the trade secret is exposed and how quickly its owner acts to prevent further dissemination of the trade secret. The rate at which information spreads across the Internet dictates that a trade-secret owner's actions should be correspondingly rapid. Information that has been posted for more than one or two days is much more likely to have become "generally known," and deemed to have lost its status as a trade secret, than information that has been posted for a shorter amount of time.<sup>22</sup>

Accordingly, a trade-secret owner who discovers its trade-secret information on the Internet must respond immediately and show that it took prompt action to remove the information or stem its further dissemination.<sup>23</sup> In seeking to retain trade-secret protection of information that has been posted, the goal is to separate trade-secret owners who have "slept on their rights" upon discovering the potentially fatal disclosure from those who have responded promptly.<sup>24</sup> Unfortunately, given the special concerns associated with trade-secret cases involving Internet postings, the tools currently in place for addressing removals from Web sites are not satisfactory. If trade-secret owners are to bear the burden of acting swiftly to remove trade secrets from Web sites, then the legal system should provide appropriate, efficient, and effective mechanisms for trade-secret owners to do so.

---

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

21. *See Rowe, supra* note 3, at 29–39 (discussing a preservation model for analyzing when trade-secret protection may be retained despite disclosure).

22. *Id.* at 32–33.

23. The appropriate strategy must be carefully tailored in light of the circumstances. *See Cundiff, supra* note 2, at 408–13 (discussing considerations in litigating to remove trade secrets from the Internet).

24. *Rowe, supra* note 3, at 32–33.

## III. A TAKEDOWN FOR TRADE SECRETS MERITS CONSIDERATION

A trade secret can be any information of value that is used in a business, has been kept secret, and provides an economic advantage over competitors.<sup>25</sup> The wide range of information entitled to trade-secret protection includes costs, sales records, customer lists and information, marketing strategies, secret contract terms, unpublished pricing information, and chemical formulas.<sup>26</sup> Trade secrets encompass approximately eighty percent of the assets of some companies.<sup>27</sup> In addition, prior to obtaining patent protection, virtually all inventions are covered by trade-secret protection.<sup>28</sup>

From an efficiency perspective, trade secrets deserve strong protection because of their importance to industry and the economy.<sup>29</sup> Trade secrets are integral to the economy because they protect and encourage innovation.<sup>30</sup> Publicly traded U.S. companies own an estimated \$5 trillion in trade-secret information.<sup>31</sup> Trade secrets are important to businesses of all sizes, from the smallest mom-and-pop shops to the largest multinational entities.<sup>32</sup> Trade secrets are often the most valuable intangible assets of a company,<sup>33</sup> and the survival of a company may depend on its ability to protect its trade secrets. In the Internet age, securing information can be especially daunting because

---

25. See UNIF. TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 538 (2005); RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

26. See, e.g., *PepsiCo v. Redmond*, 54 F.3d 1262, 1265–70 (7th Cir. 1995); *ConAgra, Inc. v. Tyson Foods, Inc.*, 30 S.W.3d 725, 728–30 (Ark. 2000); *McFarland v. Brier*, No. C.A. 96-1007, 1998 WL 269223, at \*3 (R.I. Super. Ct. May 13, 1998).

27. See John P. Hutchins, *The Corporation's Valuable Assets: IP Rights Under Sox*, in 26TH ANNUAL INSTITUTE ON COMPUTER & INTERNET LAW 289, 291 (PLI Intellectual Property, Course Handbook Series No. G-859, 2006).

28. See *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141, 155 (1989).

29. See Richard A. Epstein, *Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalism*, 52 STAN. L. REV. 1003, 1037 (2000) (“[T]he full set of efficiency arguments opts strongly for the protection of trade secrets, given their essential role in modern industry.”).

30. See *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 493 (1974); Marina Lao, *Federalizing Trade Secrets Law in an Information Economy*, 59 OHIO ST. L.J. 1633, 1633–35 (1998) (noting that corporations are increasingly relying on trade-secret protection).

31. See Hutchins, *supra* note 27, at 292.

32. See generally *id.*; ROBERT P. MERGES, PETER S. MENELL & MARK A. LEMLEY, *INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE* 34–35 (4th ed. 2006) (discussing the importance of trade secrets to small companies).

33. R. Mark Halligan, *Trade Secrets and the Inevitable Disclosure Doctrine*, in TRADE SECRETS 2002: HOW TO PROTECT CONFIDENTIAL BUSINESS & TECHNICAL INFORMATION 145, 151 (PLI Intellectual Property, Course Handbook Series No. G-719, 2006).

once a trade secret has been disclosed, even if inadvertently, it ceases to be a trade secret.<sup>34</sup>

Part of the appeal of choosing trade-secret protection over other kinds of intellectual property protection is the broad scope of protectable information and the relative ease with which a business can claim such protection.<sup>35</sup> A business can, for example, protect trade secrets without complying with a governmental registration system.<sup>36</sup> Unlike copyright law, trade-secret law, by definition, protects only economically valuable information.<sup>37</sup> Copyright law covers “original works of authorship fixed in any tangible medium of expression.”<sup>38</sup> Trade-secret law protects invention and information whereas copyright law does not “extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.”<sup>39</sup> Accordingly, the kind of proprietary information and innovative concepts that drive the economy tend to fall outside the copyright paradigm and into the ambit of trade-secret law.<sup>40</sup>

---

34. While the risk of loss is one that is inherent in choosing this form of protection, it does not necessarily suggest that a trade-secret owner should have instead chosen patent protection. The choice of trade-secret protection or patent protection must be based on a very careful assessment of the particular information involved and thorough consideration of business and legal factors involving, for example, the nature of the information, the ease with which it can be reverse engineered, and the feasibility and cost of obtaining patent protection. *See generally* Andrew Beckerman-Rodau, *The Choice Between Patent Protection and Trade Secret Protection: A Legal Business Decision*, 84 J. PAT. & TRADEMARK OFF. SOC'Y 371 (2002). Accordingly, an owner that chooses trade-secret protection over patent protection has not necessarily forgone a “better” form of protection, especially since there is a wide range of information that is eligible for trade-secret protection but not patent protection. *See* POOLEY, *supra* note 4, § 3.01[1][a] (comparing patent protection and trade-secret protection).

35. Brooks W. Taylor, *You Can't Say That!: Enjoining Publication of Trade Secrets Despite the First Amendment*, 9 COMP. L. REV. & TECH. J. 393, 394–95 (2005) (discussing reasons why corporations rely on trade-secret protection).

36. Copyright protection may attach without registration, but registration is necessary before a plaintiff files suit for infringement. Thus, prior to registration a copyright owner is in a similar situation as the owner of a trade secret who does not know whether the targeted material will indeed be protectable. Registration of a copyright provides a presumption of validity. *Bibbero Sys., Inc. v. Colwell Sys., Inc.*, 893 F.2d 1104, 1106 (9th Cir. 1990).

37. Roger M. Milgrim, *Commission Proposed Capital Punishment—By Definition—for Trade Secrets, A Uniquely Valuable IP Right*, 88 J. PAT. & TRADEMARK OFF. SOC'Y 919, 941 (2006) (“[U]nlike both patent and copyright law . . . trade secret law offers protection *solely* to matter of value . . .”).

38. 17 U.S.C. § 102(a) (2000).

39. *Id.* § 102(b).

40. Lao, *supra* note 30, at 1634.

2007:5 *Takedown for Trade Secrets on the Internet* 1051

If, similar to copyrights, trade-secret information is of such importance that it warrants special protection in the context of the Internet, then the next inquiry must involve the manner in which such protection is offered. To the extent that part of copyright law's impetus for providing a safe-harbor takedown for Internet-service providers (ISPs) is meant to address any potential liability for copyright infringement, the same concerns also apply to trade-secret law.<sup>41</sup> An ISP may be liable for trade-secret misappropriation if the ISP knows or has reason to know that a subscriber is misappropriating a trade secret.<sup>42</sup> Arguably, the notice from the trade-secret owner would be sufficient to create the requisite level of knowledge. Accordingly, it makes sense to consider a similar framework for both trade secrets and copyrights because the underlying reasons for the legislation and the ultimate objectives are comparable.

It is noteworthy that trade-secret law does not include anything akin to copyright law's fair-use doctrine.<sup>43</sup> Thus, the wide range of possible defenses available to one who posts allegedly infringing copyright material on the Internet is not available in the trade-secret context. This suggests that trade-secret law more clearly defines whether the use of material is inappropriate and that, consequently, takedown notices for trade secrets will rarely lack a legitimate basis.<sup>44</sup> However, trade-secret law suffers from its own gray areas, including the fluid nature of identifying trade secrets and the fact that, unlike copyright law,<sup>45</sup> trade-secret law must confront First Amendment principles.<sup>46</sup> Nevertheless, the damage from unauthorized copyright infringement is likely to be less than the damage from the posting of a trade secret.

---

41. Some commentators question whether ISPs should ever be liable for copyright infringement. *See, e.g.*, MARJORIE HEINS & TRICIA BECKLES, BRENNAN CENTER FOR JUSTICE, WILL FAIR USE SURVIVE? 5 (2005). This debate is beyond the scope of this Article.

42. *See* UNIF. TRADE SECRETS ACT § 1(2)(ii) (1985). The RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 (1995) and RESTATEMENT (FIRST) OF TORTS § 757 (1939) include definitions that are consistent with the Uniform Trade Secrets Act.

43. *See* Eugene Volokh, *Freedom of Speech and Intellectual Property: Some Thoughts After Eldred*, 44 *Liquormart*, and *Bartnicki*, 40 *HOUS. L. REV.* 697, 717–18 (2003).

44. *See infra* notes 125 and 131 and accompanying text.

45. Copyright cases are generally not subject to First Amendment scrutiny because copyright law already includes fair-use and other free-expression safeguards. *Eldred v. Ashcroft*, 537 U.S. 186, 221 (2003); *Harper & Row, Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 560 (1985).

46. *See infra* Part VI.A.

## IV. SECTION 512 OF THE DMCA

A. *The Formation of the DMCA*

With the rise of the Internet came many changes to everyday life. Arguably, one of the greatest transformations was the way the world adapted its protection of intellectual property. Recognizing the dire need to defend copyrights in the digital realm as well as the need to “facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age,”<sup>47</sup> Congress developed the DMCA. Initially propagated by the Clinton administration, the DMCA was created to deal with the inevitable conflict between copyright protection and the dissemination of works over the Internet.<sup>48</sup>

Among the many contentious areas between copyright law and the Internet, Congress noted that without a strong form of protection from copyright-infringement liability, the incentive for ISPs to increase efficiency and to improve existing technology faced significant roadblocks from IP owners.<sup>49</sup> To address these competing interests, Congress stated that one of its objectives in creating the DMCA was simultaneously to clarify liability facing ISPs and to promote the online environment as a place to disperse copyrighted works.<sup>50</sup> Indeed, Congress was aware that copyright owners would be justifiably hesitant to place their works on the Internet should there be no readily available method to protect them against the potential “massive piracy” that could result from Internet distribution.<sup>51</sup>

While there was a consensus about the DMCA’s desired effect, there was great disagreement about how to accomplish it.<sup>52</sup> The Working Group on Intellectual Property Rights created a developmental report, called the “White Paper,” which advocated making ISPs strictly liable for their users’ copyright infringement.<sup>53</sup> Among the reasons the White Paper held this view was that ISPs are more aware than copyright owners of the identities and actions of their users. Thus, ISPs

---

47. S. REP. NO. 105-190, at 1–2 (1998).

48. Emily Zarins, *Notice Versus Knowledge Under the Digital Millennium Copyright Act’s Safe Harbors*, 92 CAL. L. REV. 257, 263 (2004).

49. S. REP. NO. 105-190, at 2, 8 (1998).

50. *Id.* at 8.

51. *Id.*

52. See Zarins, *supra* note 48, at 264–66.

53. THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 114, 122 (1995), available at <http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf>.

2007:5 *Takedown for Trade Secrets on the Internet* 1053

arguably are more capable of detecting and preventing infringing uses.<sup>54</sup> Further, in rejecting the notion that knowledge should be a necessary element for ISP liability, the White Paper noted that copyright infringement could be accomplished without intent or inquiry into the infringer's state of mind.<sup>55</sup> The White Paper concluded that ISPs could mitigate their copyright liability by declining to provide service to infringing users, requiring proof of licensing, and requiring indemnification and warranty agreements from all users.<sup>56</sup>

While the White Paper promoted the strict-liability avenue for ISPs, it also acknowledged the many viable arguments against it.<sup>57</sup> Most notably, the report recognized the strong ISP contention that, given the volume of information the ISPs would be responsible for, it would be impossible for ISPs to monitor and identify infringing material.<sup>58</sup> Furthermore, even if they were capable of such a feat, the ISPs would be statutorily prohibited by the Electronic Communications Privacy Act from accessing any stored communications without authorization.<sup>59</sup>

Moreover, critics of the White Paper questioned why it neglected to consider other arguably analogous case law regarding landlord-tenant relationships.<sup>60</sup> For instance, likening the landlord to an ISP, one case implied that liability should not flow to the ISP given the limited capacity it has to supervise and inspect its respective digital premises.<sup>61</sup> Further, commentators argued that extending ISP responsibility to these areas would cause ISPs to monitor and significantly reduce the amount of information they allow online—impeding information dissemination, increasing the costs of ISP services, and chilling free exchange.<sup>62</sup> Ultimately, these arguments carried the day for ISPs; Congress refused to enact many of the White Paper's ideas.<sup>63</sup>

---

54. *Id.* at 117.

55. *Id.* at 101. *See* *Sega Enters. Ltd. v. Maphia*, 857 F. Supp. 679 (N.D. Cal. 1994); *Playboy Enters., Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993).

56. THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, *supra* note 53, at 123.

57. *Id.* at 114–15.

58. *Id.* at 115.

59. *See* 18 U.S.C. § 2701 (2000); Pamela Samuelson, *The Copyright Grab*, WIRE, Jan. 1996, available at [http://www.wired.com/wired/archive/4.01/white.paper\\_pr.html](http://www.wired.com/wired/archive/4.01/white.paper_pr.html); Zarins, *supra* note 48, at 266.

60. Samuelson, *supra* note 59.

61. *Fonovisa, Inc. v. Cherry Auction, Inc.*, 847 F. Supp. 1492, 1496 (E.D. Cal. 1994), *rev'd*, 76 F.3d 259, 261 (9th Cir. 1996).

62. *See* Niva Elkin-Koren, *Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Operators*, 13 CARDOZO ARTS & ENT. L.J. 345, 406–07 (1995); Zarins, *supra* note 48, at 266.

63. Zarins, *supra* note 48, at 267.

Into this contentious environment came the California district-court decision in *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, which inadvertently helped dictate the direction of ISPs' liability under the DMCA.<sup>64</sup> The Church of Scientology sued a former member, Dennis Erlich, who was allegedly posting the church's copyrighted information on the Internet by using a bulletin-board service (BBS) that used Netcom On-Line Communications (Netcom) as an ISP.<sup>65</sup> When Religious Technology Center petitioned the BBS and Netcom to cease allowing Erlich to post, both companies refused its request and were consequently added as defendants under a direct-copyright-infringement theory.<sup>66</sup>

Even though *Religious Technology Center* recognized that direct copyright infringement does not normally "require intent or any particular state of mind,"<sup>67</sup> the court still held that Religious Technology Center had not shown the requisite likelihood of success on the merits for a preliminary injunction against the BBS and Netcom.<sup>68</sup> Directly contradicting the theories espoused in the White Paper, *Religious Technology Center* stated that "[a]lthough copyright is a strict liability statute, there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party."<sup>69</sup> Moreover, *Religious Technology Center* denied that this "volition" requirement could be satisfied by the ISP's "warning to delete the message" but noted that it could be relevant to a contributory infringement theory.<sup>70</sup>

*Religious Technology Center* left open the question of whether Netcom could be liable as a contributory infringer<sup>71</sup> but noted that "a mere unsupported allegation of infringement by a copyright owner" may not be adequate to establish the knowledge required for contributory liability.<sup>72</sup> In advocating what can best be described as a balancing of the burdens analysis for the knowledge requirement, the court stated:

---

64. See H.R. REP. NO. 105-551, pt. 1, at 11; *Religious Tech. Ctr. v. Netcom On-Line Commc'ns Servs., Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995).

65. *Religious Tech. Ctr.*, 907 F. Supp. at 1365-66.

66. *Id.* at 1366.

67. *Id.* at 1367.

68. *Id.* at 1383.

69. *Id.* at 1370.

70. *Id.*

71. *Id.* at 1374.

72. *Id.*

2007:5 *Takedown for Trade Secrets on the Internet* 1055

Where a BBS operator cannot reasonably verify a claim of infringement, either because of a possible fair use defense, the lack of copyright notices on the copies, or the copyright holder’s failure to provide the necessary documentation to show that there is a likely infringement, the operator’s lack of knowledge will be found reasonable . . . .<sup>73</sup>

Thus, Netcom acknowledged that if it had actually looked at Erlich’s posting after receiving the notice, it would have initiated an investigation for possible copyright infringement. The court, therefore, left open the question of whether Netcom could be subject to contributory liability.<sup>74</sup> The court opined that once Netcom had knowledge of Erlich’s infringing use of its services, it had a duty to “take simple measures to prevent further damage to plaintiffs’ copyrighted works.”<sup>75</sup> Still, the court equitably balanced this obligation with the recognition that making ISPs responsible for monitoring all messages going through their systems could “have a serious chilling effect on what some say may turn out to be the best public forum for free speech yet devised.”<sup>76</sup>

Congress evidently was more impressed with the reasoning of *Religious Technology Center* than it was with the White Paper. The House Report for enactment of the On-Line Copyright Infringement Liability Limitation Act explicitly endorsed *Religious Technology Center*.<sup>77</sup> This report eventually became the predicate for the DMCA’s safe-harbor provision.<sup>78</sup> Indeed, in discussing the necessity of narrowing and clarifying the liability of ISPs, the House Report referred to *Religious Technology Center* as “the leading and most thoughtful judicial decision to date.”<sup>79</sup> While being tentative not to “embark[] upon a wholesale clarification” of the doctrines of contributory and vicarious liability, the Senate Report also tacitly endorsed *Religious Technology Center* by stating that it had “decided to leave current law in its evolving state and, instead, . . . create a series of ‘safe harbors,’ for certain common activities of service providers.”<sup>80</sup> Through this relative codification of *Religious Technology Center*’s

---

73. *Id.*  
 74. *Id.* at 1374–75.  
 75. *Id.* at 1375.  
 76. *Id.* at 1377–78.  
 77. H.R. REP. NO. 105-551, pt. 1, at 11 (1998).  
 78. Mike Scott, *Safe Harbors Under the Digital Millennium Copyright Act*, 9 N.Y.U. J. LEGIS. & PUB. POL’Y 99, 116 (2006).  
 79. H.R. REP. NO. 105-551, pt. 1, at 11 (1998).  
 80. S. REP. NO. 105-190, at 19 (1998).

principles, the safe-harbor provision enumerated in 17 U.S.C. § 512 of the DMCA came to be.<sup>81</sup>

*B. Details of the DMCA Safe-Harbor Provision*

In order for an ISP to qualify for the safe harbor,<sup>82</sup> the alleged infringement generally has to occur during one of four basic activities: (1) transitory digital-network communications, (2) system caching, (3) storing information at the direction of the user, or (4) providing an information-location tool.<sup>83</sup> Furthermore, to protect ISPs' good-faith actions to help mitigate infringement, the provision provides that "[a]ny person who knowingly materially misrepresents . . . (1) that material or activity is infringing, or (2) that material or activity was removed or disabled by mistake or misidentification" will be liable for any resulting damages, including costs and attorneys' fees, to the affected ISPs.<sup>84</sup> These limitations were designed to immunize ISPs from liability for contributory infringement and to provide "strong incentives" to foster cooperation between ISPs and copyright owners in the fight against copyright infringement on the Internet.<sup>85</sup>

To qualify for this relief from liability, ISPs must comply with certain stipulations set forth in 17 U.S.C. § 512(i).<sup>86</sup> Among the conditions are the requirements that ISPs not only adopt and implement procedures that allow for termination of repeat infringers but also inform users of the policy's existence.<sup>87</sup> This provision also imposes an obligation on ISPs to accommodate technologies "that are used by copyright owners to identify or protect copyrighted works and . . . do not impose substantial costs on service providers or substantial burdens on their systems or networks."<sup>88</sup>

While these prerequisites apply to ISPs seeking limited liability under any of the subsections, ISPs that provide services other than transitory digital communications must also satisfy the notice and takedown provision of 17 U.S.C. § 512(c). The takedown provision places an affirmative duty on ISPs to "act[] expeditiously to remove, or

---

81. Scott, *supra* note 78, at 116.

82. S. REP. NO. 105-190, at 19 (1998).

83. *See id.*; 17 U.S.C. § 512(a)-(d) (2000). Recognizing that these protections may not extend far enough, Congress also extended the safe-harbor provision to provide limited liability to nonprofit educational institutions that act as ISPs for faculty and graduate students performing teaching or researching functions. *Id.* § 512(e).

84. 17 U.S.C. § 512(f)(1)-(2).

85. S. REP. NO. 105-190, at 20 (1998).

86. 17 U.S.C. § 512(i).

87. *Id.* § 512(i)(1)(A).

88. *Id.* § 512(i)(2)(C).

2007:5 *Takedown for Trade Secrets on the Internet* 1057

disable access to, the material” that is claimed to be infringing but only “upon obtaining such knowledge” of infringement or “aware[ness] of facts or circumstances from which infringing activity is apparent.”<sup>89</sup> The takedown provision is thus predicated on the fact that the ISP does not have control over or receive financial benefit from the infringing activity.<sup>90</sup>

Although the statute places no duty on an ISP performing certain services to monitor its service for activity, the statute does create what the House Report referred to as a “red flag test” to determine when an ISP has a duty to act.<sup>91</sup> In order to pass this test and to maintain their limited liability, ISPs must take action whenever they become aware of “facts or circumstances” that raise a “red flag” as to the possibility that infringing activity is occurring.<sup>92</sup> This test is thus comprised of both an objective and subjective portion—an ISP must not subjectively be aware of facts and circumstances that would lead “a reasonable person operating under the same or similar circumstances”<sup>93</sup> to conclude that there is infringing activity.

This red flag can be raised, for example, when a user gives the ISP a notification in compliance with the takedown provision. To permit this sort of notification, the ISP must designate and list an agent with the Register of Copyrights specifically designed to receive it.<sup>94</sup> Among various other procedural requirements, such as providing contact information and identifying the alleged infringing activity,<sup>95</sup> the notice must include “[a] statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.”<sup>96</sup>

The statute further requires that the copyright owner “comply substantially” with certain requirements of the takedown provision in order to ascribe sufficient knowledge to the ISP.<sup>97</sup> However, as long as the complaining party substantially identifies the copyrighted material and infringing activity and provides contact information, the ISP must

---

89. *Id.* § 512(c)(1)(A)(i)–(iii).

90. *See id.* § 512(c)(1)(B).

91. H.R. REP. No. 105-551, pt. 2, at 53 (1998).

92. *Id.*

93. *Id.*

94. 17 U.S.C. § 512 (c)(2).

95. *Id.* § 512(c)(3)(A)(i)–(iv).

96. *Id.* § 512(c)(3)(v). This provision seems to cross reference the fact that anyone who “materially misrepresents . . . that material or activity is infringing . . . shall be liable for any damages . . . incurred” as a result of the misrepresentation. *See id.* § 512(f)(1)–(2).

97. *Id.* § 512(c)(3)(B)(i)–(ii).

contact the complaining party or take other reasonable steps to bring the notification into compliance.<sup>98</sup>

Once the ISP receives a substantially compliant takedown notice and “acts expeditiously” to remove or disable access to the material,<sup>99</sup> it must notify the subscriber that the material has been removed.<sup>100</sup> The subscriber is subsequently permitted to provide a counternotification that includes “[a] statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.”<sup>101</sup> If the alleged infringer takes advantage of this procedure, then the ISP must inform the copyright owner that the ISP will replace or “cease disabling access to” the contested material within ten business days after receipt of the counternotification.<sup>102</sup>

To prevent the ISP from returning the material, the copyright owner must inform the designated agent that an action has been brought against the alleged infringer within this time frame.<sup>103</sup> To facilitate this process and to allow the action to be brought against the correct individual, the statute permits “the clerk of any United States district court to issue a subpoena” requiring that an ISP disclose the identification of the alleged infringer “to the extent such information is available to the service provider.”<sup>104</sup>

### *C. Section 512 Protection in a Nutshell*

Section 512(a) provides the broadest protection for ISPs that provide transmission and routing services and are thus mere conduits of information.<sup>105</sup> These providers—typically high-speed-Internet, broadband, and DSL providers—receive safe harbor from their users’ infringement activities without any requirement that they take down allegedly infringing material.<sup>106</sup> The only condition of their safe harbor is that they adopt a policy for terminating repeat infringers and accommodate technical protection measures.<sup>107</sup>

---

98. *See id.* § 512(c)(3)(B)(ii).

99. *Id.* § 512(c)(1)(A)(iii).

100. *Id.* § 512(g)(2)(A).

101. *Id.* § 512(g)(3)(C).

102. *Id.* § 512(g)(2)(B).

103. *Id.* § 512(g)(2)(C).

104. *Id.* § 512(h)(1), (3).

105. *Id.* § 512(a).

106. *Id.*

107. *Id.* § 512(a)(1)–(5), (b)(2)(C)–(E).

2007:5 *Takedown for Trade Secrets on the Internet* 1059

Sections 512(c) and (d) apply to ISPs providing hosting services<sup>108</sup> and search engines. The takedown provision applies mainly to these providers. To receive the safe harbor from liability, these providers are required to remove allegedly infringing content upon receipt of notice from the copyright holder.<sup>109</sup> The § 512(c) process requires that the ISP (1) “expeditiously” take down the information, (2) notify the alleged infringer that the material has been removed,<sup>110</sup> and (3) forward any counter notices from alleged infringers back to the original complainant.<sup>111</sup> If after ten to fourteen days the complainant does not notify the ISP that it has filed an action against the alleged infringer, then the ISP may put back the material.<sup>112</sup>

A brief mention of the anticircumvention provision and § 512 may also be of interest. Section 1201 of the DMCA makes it illegal to make available “anticircumvention” devices or links to anticircumvention devices.<sup>113</sup> It is interesting, however, that illegal circumvention by itself, at least in the view of one court, cannot be the subject of a § 512 notice since it is separate and distinct from copyright infringement.<sup>114</sup> It thus appears that the safe-harbor provisions arguably do not apply to this section.<sup>115</sup> Section 1201 seems to offer quasi-trade-secret protection because it essentially prohibits one from obtaining or accessing something that is being kept secret, such as the technological measures that protect the copyrighted work.<sup>116</sup> Thus, favorable rulings upholding the validity of the anticircumvention provision may offer promise to a trade-secret-takedown statute.<sup>117</sup>

---

108. Hosting services include Web sites, forums, blogs, and social networking sites.

109. *Id.* § 512(c)–(d).

110. Search engines are not required to provide notice to the alleged infringer. *See id.* § 512(d).

111. *Id.* § 512(g)(2).

112. *Id.*

113. *Id.* § 1201.

114. *See Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211, 217 (S.D.N.Y. 2000) (“Section 512(c) provides protection only from liability for copyright infringement. Plaintiffs seek to hold defendants liable not for copyright infringement, but for a violation of § 1201(a)(2), which applies only to circumvention products and technologies.”) (internal citations omitted).

115. *See* 17 U.S.C. § 1201(a)(2), (b)(1)(A).

116. It provides even greater protection than that afforded under trade-secret law in that it appears to prevent reverse engineering. It prohibits trafficking in technology that can circumvent technological measures employed by the copyright owner. *Id.* § 1201.

117. *See Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 454–55 (2d Cir. 2001) (upholding an injunction under the anticircumvention provision and finding that the government had a substantial interest in preventing unauthorized access to encrypted copyrighted material).

*D. Summary of DMCA Criticisms*

Much has been written about the DMCA takedown provision.<sup>118</sup> Many commentators believe that copyright holders have abused the takedown provision<sup>119</sup> and that the provision could be improved by better balancing the benefits to copyright owners with the protections for posters of allegedly infringing material.<sup>120</sup> Despite the provision's weaknesses (perceived or actual), however, it has achieved the intended purposes that spurred the legislation: it clarifies ISP liability for contributory copyright infringement and promotes the distribution of copyrighted works over the Internet.<sup>121</sup> This Article does not address changes to the DMCA's safe-harbor provision. Rather, this Article simply uses the provision as a starting point from which to design a trade-secret-takedown provision that is carefully tailored to the principles of trade-secret law while also being mindful of the lessons learned from the DMCA.

One recent study attempted an empirical analysis of 876 DMCA takedown notices collected by the Chilling Effects<sup>122</sup> project.<sup>123</sup> The

---

118. See, e.g., HEINS & BECKLES, *supra* note 41, at 8; Michael Driscoll, *Will YouTube Sail into the DMCA's Safe Harbor or Sink for Internet Piracy?*, 6 J. MARSHALL REV. INTELL. PROP. L. 550, 566-68 (2007), available at <http://www.jmripl.com/publications/vol6/issue3/driscoll.pdf>; Malla Pollack, *Rebalancing Section 512 To Protect Fair Users from Herds of Mice-Trampling Elephants, or a Little Due Process Is Not Such a Dangerous Thing*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 547, 547-48, 554 (2006); Scott, *supra* note 78, 128-35; Urban & Quilter, *supra* note 8, at 640. Approximately forty-four law-review articles published this year and last year discuss the DMCA takedown provision. Only about three articles discuss the legislation overall in a positive light. These articles are: Emily Favre, *Online Auction Houses: How Trademark Owners Protect Brand Integrity Against Counterfeiting*, 15 J.L. & POL'Y 165, 199-201 (2007); Britton Payne, *Super-Grokster: Untangling Secondary Liability, Comic Book Heroes and the DMCA, and a Filtering Solution for Infringing Digital Creations*, 16 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 939 (2006); Yiman Zhang, *Establishing Secondary Liability with a Higher Degree of Culpability: Redefining Chinese Internet Copyright Law to Encourage Technology Development*, 16 PAC. RIM L. & POL'Y J. 257, 281-82 (2007). Half of the remainder of the forty-four law-review articles that discuss the DMCA takedown provision express criticisms of the provision, while the other half are neutral. The searches were conducted in the LexisNexis "US Law Reviews and Journals" database (DMCA and "take down" [from 12/31/2005 through 07/29/2007]) and in Westlaw's "Journal and Law Reviews" database (dmca & "take-down" & da[after 12/31/2005]).

119. See, e.g., Urban & Quilter, *supra* note 8, at 688.

120. See, e.g., *id.*

121. S. REP. NO. 105-190, at 8 (1998).

122. Since its inception in 2002, the Chilling Effects Web site has invited the public and ISPs to submit cease-and-desist and takedown letters that they have received from copyright holders. Chilling Effects Clearinghouse, <http://www.chillingeffects.org/dmca512> (last visited Oct. 18, 2007).

123. Urban & Quilter, *supra* note 8, at 641-42.

2007:5 *Takedown for Trade Secrets on the Internet* 1061

study's authors, Professor Jennifer Urban and Laura Quilter, noted several concerns regarding the takedown notices, including (1) serious legal questions relating to the merits of the underlying copyright claims, (2) failure to comply with statutory requirements in the written notice, and (3) use of the notices to address claims other than copyright infringement.<sup>124</sup>

In another study, Marjorie Heins and Tricia Beckles of the Brennan Center for Justice at New York University School of Law used a variety of research methods to examine "how well fair use and similar free expression safeguards in IP law are working."<sup>125</sup> As part of the study, they reviewed all of the DMCA takedown notices from 2004 on the Chilling Effects Web site.<sup>126</sup> While they found that over half of the notices appeared to state valid claims for copyright or trademark infringement,<sup>127</sup> they nonetheless expressed concern over the "censorship power that the law puts in the hands of IP owners."<sup>128</sup> In particular, the authors noted that over a fifth of the notices either represented weak claims or were subject to strong fair-use or First Amendment defenses.<sup>129</sup>

## V. ANATOMY OF THE LEGISLATION

This Section does not assume the intricate task of drafting trade-secret-takedown legislation. However, it is mindful of existing trade-secret-law principles in suggesting solutions. It also offers several points for consideration by identifying some of the potentially thorny issues that may arise from trade-secret regulation. The lessons learned from the implementation of § 512 of the DMCA are certainly helpful and provide guidance on the direction of the trade-secret endeavor. Those lessons, together with an understanding of the theory and practice of trade-secret law, could be instructive if Congress were to create this legislation.

The form of a trade-secret-takedown provision could be an expansion of the DMCA, an expansion of the Economic Espionage

---

124. *Id.* at 667-78.

125. HEINS & BECKLES, *supra* note 41, at 8.

126. *Id.*

127. Section 512's safe-harbor provision does not apply to trademark infringement. *See* 17 U.S.C. § 512(c) (2000); *Gucci Am., Inc. v. Hall & Assocs.*, 135 F. Supp. 2d 409, 410-11 (S.D.N.Y. 2001) (refusing to grant ISP's motion to dismiss where trademark infringement allegedly occurred on a Web site hosted by the ISP).

128. HEINS & BECKLES, *supra* note 41, at 36.

129. *Id.* at 32. They reported that another twenty-seven percent of the sample covered material, by their assessment, was possibly protected under fair use or the First Amendment. *Id.*

Act,<sup>130</sup> or a creation of an original body of legislation. The actual process by which material would be removed could be very similar to that established under the DMCA, subject to some modification to accommodate the concerns raised below. In short, the complainant would provide notice of the alleged inappropriate posting of the trade secret to the ISP. Upon receipt of the notice, the ISP would need to remove the material within a very short period of time (probably within five hours).<sup>131</sup> The trade-secret owner would then file a complaint in court within a certain number of days (probably ten days) or provide proof to the ISP of an agreement with the alleged misappropriator. Failure to take this step would result in automatic return of the information to the Web site. A notice provision to alert the subscriber of the takedown could be required, but the nature of a counternotice requirement is less clear.

#### A. *Safe Harbor*

It is worth considering whether the framework of a safe harbor is the best approach for trade-secret-takedown legislation. It probably is the optimal context in which to place a takedown requirement because it is difficult to find other workable incentives that encourage ISPs to be observant or other rubrics that could legitimately compel ISPs' compliance.<sup>132</sup> An important component of misappropriation under trade-secret law, particularly in the context of intermediary liability, is knowledge that the information is another's trade secret.<sup>133</sup> A person is liable for misappropriation if he or she turns a blind eye to or ignores the use of another's trade secret.<sup>134</sup> Accordingly, ISPs could be liable

---

130. The Economic Espionage Act, enacted in 1996, criminalizes trade-secret theft and misappropriation. 18 U.S.C. §§ 1831–39 (2000).

131. See *supra* notes 22–23 and accompanying text (explaining the need for promptness).

132. Professor Lemley proposes a uniform safe-harbor provision for ISPs that covers all areas of intellectual property. See Mark A. Lemley, *Rationalizing Internet Safe Harbors* (2007) (unpublished manuscript), available at <http://web.si.umich.edu/tprc/papers/2007/660/rationalizinginternetsafeharbors.pdf>. This would be an interesting alternative to the current piecemeal approach to safe harbors. His suggestion, nonetheless, further provides support for the safe-harbor framework as the best approach for addressing these kinds of harms.

133. See *C&F Packing Co. v. IBP, Inc.*, No. 93 C 1601, 1998 U.S. Dist. LEXIS 3221, at \*19 (N.D. Ill. Mar. 16, 1998) (explaining that constructive notice is sufficient to show that information was a trade secret).

134. See, e.g., *Curtiss-Wright Corp. v. Edel-Brown Tool & Die Co.*, 407 N.E.2d 319, 324 (Mass. 1980) (reasoning that a defendant cannot shield himself by “studious ignorance of pertinent ‘warning’ facts” (quoting R. MILGRIM, *TRADE SECRETS* § 5.04[2] (1978))).

2007:5 *Takedown for Trade Secrets on the Internet* 1063

for misappropriation when they transmit information in violation of trade-secret law with knowledge that the information is protectable.<sup>135</sup> Weighed against the realities of the tremendous burden that it would impose upon ISPs to police their users' content (at least with today's technology), a safe harbor appears to be a fair balance. The trade-secret owner bears the burden of monitoring the Internet, but the ISP, once notified, must take action to remove allegedly misappropriated material in order to avoid potential liability.

Overall, however, it is desirable to tie actual potential for liability to the kind of service offered by the ISPs. Not doing so, (i.e., being overinclusive) increases the chances of takedown notices being sent to virtually every kind of ISP, even if liability would be extremely unlikely based on the kind of services offered.<sup>136</sup> It would not only create a high compliance burden on ISPs, it would also magnify the potential for a chilling effect on speech as ISPs acting in their best interest comply with notices to preserve their immunity—even if liability would be remote.<sup>137</sup> For this reason, ISPs who are mere conduits are exempted under this proposal.<sup>138</sup>

### B. *Dealing with Frivolous Requests*

Because of the potential for misuse of a takedown for trade secrets, a complaining trade-secret owner's takedown notice should be accompanied by a bond or fee. Under the DMCA, a complainant needs a subjective "good faith belief" of infringement to request a takedown.<sup>139</sup> Although a similar requirement makes sense for trade secrets, some additional assurance is probably necessary to counteract illegitimate uses of the mechanism. The required fee should be costly enough for large companies yet not so expensive that it would be prohibitive for small businesses. Perhaps something akin to the posting of a bond for the granting of preliminary injunctive relief could be a helpful model.<sup>140</sup> Alternatively, it could be a fee to the ISP as compensation for having to divert its resources to removing or disabling information within hours of receiving a takedown request.

---

135. *See id.*

136. *See generally* Urban & Quilter, *supra* note 8, at 667–68.

137. *See, e.g., id.*; HEINS & BECKLES, *supra* note 41, at 36.

138. *See infra* Part VI.C.

139. *See* Rossi v. Motion Picture Ass'n of Am., Inc., 391 F.3d 1000, 1003 (9th Cir. 2004).

140. *See* FED. R. CIV. P. 65(c).

In addition, there should be a statutory remedy for a frivolous takedown request.<sup>141</sup> An alleged infringer whose material is improperly subjected to a takedown under the DMCA has a remedy against the copyright owner if a knowing material misrepresentation was made in the notice to the ISP.<sup>142</sup> For example, in *Online Policy Group v. Diebold, Inc.*,<sup>143</sup> a federal district court in California concluded as a matter of law that Diebold had “knowingly materially misrepresented” that publication of its e-mail archive exposing weaknesses in its voting machines was protected by copyright law. This misrepresentation was material because the takedown notice caused the Web sites to remove their e-mail archives.<sup>144</sup> Ironically, the contents of the e-mails might have been protectable under trade-secret law.

An analogous bad-faith-type standard seems appropriate for a trade-secret-takedown provision. While the standard may be difficult to meet depending on the particular circumstances of a case, it should not necessarily be any lower because the complexity and unpredictability of trade-secret law would likely render any other standard too difficult for trade-secret owners. Just as in *Diebold*, courts would expect that if a trade-secret owner submits a takedown notice for material that a court determines that the owner should have known was not protectable as a trade secret<sup>145</sup> (e.g., the owner had not taken adequate steps to protect the information), then liability under a “knowingly material misrepresentation” standard could be satisfied. Indeed, trade-secret law provides support for penalizing a trade-secret owner for asserting a trade-secret claim in bad faith. Thus, an extension of this principle in this context would be entirely consistent.<sup>146</sup> It is also important because the nature of trade-secret law is such that there is no “prima facie” certification of a trade secret that a trade-secret owner can present or upon which an ISP can rely for verification.<sup>147</sup>

---

141. Under the DMCA, if an owner misrepresented its claim in the takedown notice, then the owner is liable to the ISP for any damages resulting from an improper removal of material. 17 U.S.C. § 512(f) (2000).

142. *Id.* Under § 512(f) any of the parties involved may be awarded damages, costs, and attorneys’ fees if either the copyright owner or the alleged infringer makes a knowing, material misrepresentation in a notice or counternotice. *Id.*

143. 337 F. Supp. 2d 1195 (N.D. Cal. 2004).

144. *Id.* at 1204 (interpreting § 512(f)).

145. Evidence supporting the strength of the trade-secret claim would be relevant to the trade-secret owner’s alleged bad faith in asserting the claim. *See CVD, Inc. v. Raytheon Co.*, 769 F.2d 842, 851 (1st Cir. 1985).

146. *See, e.g., id.* (ruling in the context of an antitrust claim that “the assertion of a trade secret claim in bad faith, in an attempt to monopolize, can be a violation of the antitrust laws.”) (internal citations omitted).

147. *See infra* Part VI.B.

*C. Carveout for Mere Conduits*

ISPs that only provide transmission and routing services and are merely conduits of alleged trade secrets should be exempt from the takedown-notice procedure for two reasons.<sup>148</sup> First, as a practical matter, because material resides on their users' computers rather than on the ISPs' servers, the ISPs have no ability to remove offending material from their systems.<sup>149</sup> Second, it is highly unlikely that the mere transmission of trade-secret information under these circumstances would constitute actionable trade-secret misappropriation. Accordingly, since liability would not be well-grounded in trade-secret law, it makes little sense to include these transmitters as part of the takedown scheme; in fact, doing so would impose unnecessary costs and burdens to comply.<sup>150</sup>

*D. Carveout for the Press*

Because liability for trade-secret misappropriation against publishers in established news organizations is currently unsettled and, indeed, any consensus (to the extent one exists) points away from such liability, it may be advisable to exempt "established news organizations"<sup>151</sup> from the takedown statute. In particular, where members of such organizations both played no part in illegally obtaining a trade secret that is a matter of public concern and lawfully accessed the trade secret, current Supreme Court jurisprudence appears to shield the press from liability for disclosure under the First Amendment.<sup>152</sup> To be clear, providing a carveout in this statute for the

---

148. Congress, in § 512(a), codified the decision in *Religious Technology Center v. Netcom*. See 17 U.S.C. § 512(a) (2000); *Religious Tech. Ctr. v. Netcom On-Line Commc'ns Servs., Inc.*, 907 F. Supp. 1361, 1372 (N.D. Cal. 1995) ("It would be especially inappropriate to hold liable a service that acts more like a conduit, in other words, one that does not itself keep an archive of files for more than a short duration."). It thus preserves immunity for ISPs that do no more than move packets of information on the Internet. See H.R. REP. NO. 105-796, at 19-20 (1998) (Conf. Rep.).

149. See Urban & Quilter, *supra* note 8, at 675 (discussing § 512(a) takedown notices to ISPs acting as conduits).

150. To the extent there is concern about the possibility of liability, a blanket safe harbor or exemption from liability for these providers may be advisable.

151. This phrase is meant to capture traditional news organizations, such as television stations, newspapers, and magazines, that have editorial staff who review and make decisions about publication. The phrase excludes bloggers, Web-site operators, and all nontraditional newsmen. See *infra* Part VI.A.1.a (discussing such persons' legal status as publishers).

152. See *Bartnicki v. Vopper*, 532 U.S. 514, 525 (2001); *infra* Part VII.A.2.

press does not provide immunity. Rather, where the trade secret appears on a Web site belonging to a covered news organization, a trade-secret owner could not use the takedown statute to have the information removed. Instead, the currently existing process of filing suit and moving for a preliminary injunction would be required.

This carveout is further supported by other considerations that aim to make the provisions of the proposed legislation consistent with current principles of trade-secret law. For instance, one practical effect of having the deliberative review of information by an editorial staff before it is posted or published is that it serves as a filter for the intent of the poster: information that is newsworthy, rather than information which is posted mainly to exact revenge or to harm a trade-secret owner, is more likely to be protected.<sup>153</sup> Furthermore, it would be consistent with the privilege in trade-secret law to disclose trade secrets that are “relevant to public health or safety, or to the commission of a crime or tort, or to other matters of substantial public concern.”<sup>154</sup> From a practical perspective, it would also mean that the *Wall Street Journal* or the *New York Times* would not need to take down news articles from their online editions that nonetheless appear in the print version of the newspaper.

#### *E. Subpoena Provision*

Similar to the DMCA, a provision permitting the trade-secret owner to obtain a subpoena for the identity<sup>155</sup> of the alleged misappropriator might be of value.<sup>156</sup> Nonetheless, recognizing that this kind of provision could be fraught with hazards, a careful analysis—perhaps including an evaluation of the implementation of the DMCA’s corollary provision—would be wise. For instance, the subpoena provision in § 512 does not appear to apply to ISPs who are mere conduits, that is, those who do not store material on their servers.<sup>157</sup>

---

153. *See* *Shoen v. Shoen*, 5 F.3d 1289, 1293 (9th Cir. 1993) (recommending a focus on whether there was intent to disseminate the information to the public at the beginning of the news gathering process).

154. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. c (1995).

155. A key first step in filing suit against an alleged misappropriator is to obtain the identity of the individual. Cundiff, *supra* note 2, at 409.

156. *See* 17 U.S.C. § 512(h) (2000). The subpoena is granted on the condition that the identity will only be used in relation to the protection of the intellectual-property rights of the copyright owner. *Id.* § 512(h)(2)(C).

157. *See* *Recording Indus. Ass’n of Am., Inc. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229, 1233 (D.C. Cir. 2003) (“We conclude from both the terms of § 512(h) and the overall structure of § 512 that . . . a subpoena may be issued only to an ISP

Whether it should remain the same for trade secrets and the implications flowing from any resulting position would be an important consideration.

The ability to subpoena the identity of an alleged misappropriator would permit a trade-secret owner to pursue a misappropriation action against the individual posting the information,<sup>158</sup> as is required under this proposal. However, the provision must be carefully tailored to avoid abuses.<sup>159</sup> The DMCA subpoena provision empowers a court clerk, not a judge, to issue the subpoena. While the application for the subpoena must be accompanied by the takedown notice, additional safeguards should be required to help ensure, for instance, that (1) the subpoena is sought by a bona-fide owner of a trade secret, (2) it is intended to be used for the exclusive purpose of enforcing trade-secret rights, and (3) the alleged misappropriator has notice and an opportunity to object to its issuance.<sup>160</sup> These considerations must nevertheless balance the inherent tensions between offering adequate protections to the subscriber and the trade-secret owner while also maintaining a speedy and efficient process.

*F. Counternotice Not Required*

Section 512 allows an ISP “subscriber”<sup>161</sup> to submit a counternotice contesting an allegation of copyright infringement.<sup>162</sup> After receiving a counternotice claiming that the targeted material is not

---

engaged in storing on its servers material that is infringing or the subject of infringing activity.”).

158. One potential problem with obtaining subpoenas based on the Internet Protocol (IP) address of a computer is that the owner of the computer may not necessarily have been the alleged misappropriator. Someone else could have used the computer. *See, e.g.*, Emily Umbright, *DMCA Proof Internet Law Still Evolving*, ST. LOUIS DAILY REC., Aug. 29, 2003 (discussing the music industry’s subpoenas to alleged copyright infringers).

159. *See generally* Lidsky & Cotter, *supra* note 10, at 1594–98 (discussing tort actions against anonymous defendants).

160. The burden could be placed on the ISP or the alleged misappropriator to obtain a protective order against issuance of the subpoena, or to have it quashed.

161. The DMCA does not define “subscriber,” but the context in which the term is used suggests that a subscriber is one who has an account or similar business relationship with the ISP. *See* 17 U.S.C. § 512(g)(2) (2000) (referring to “a subscriber of the service provider”). Thus, “subscriber” would not include, for instance, a person contributing to ongoing discussions in newsgroups.

162. *Id.* § 512(g)(3). The provisions do not require notice before the material has been removed; notice has been required only after it has been removed. *See id.* § 512(g)(2)(A).

infringing,<sup>163</sup> the ISP must notify, within ten business days, the party providing the notice of the subscriber's objection.<sup>164</sup> If after receiving such notice the copyright owner does not file suit within fourteen days, the material must then be reposted.<sup>165</sup> While notice of the takedown to the subscriber is important, it is worth rethinking whether a counternotice should be required and for what purpose.

To some extent, a counternotice may not be an effective component for a trade-secret takedown. First, the filing of a lawsuit under § 512 appears contingent upon the alleged misappropriator providing the counternotice. Unless the subscriber submits a counternotice, nothing in the statute requires the copyright owner to file an action.<sup>166</sup> However, in order to provide tighter restrictions and help avoid potential abuses by trade-secret owners, this proposal requires that complainants file suit or provide proof of an agreement with the alleged misappropriator to avoid the material being put back within a short period of time.<sup>167</sup> The alleged misappropriator may request the put back after the requisite time has passed by providing notice to the ISP with a copy to the complainant. Initiating a lawsuit may present practical difficulties for trade-secret owners, but this requirement could serve as another safeguard against frivolous notices.

Although the ISP would be required to notify the subscriber that its material has been removed and is the subject of a trade-secret-misappropriation allegation, it is unclear that a counternotice procedure would be worthwhile.<sup>168</sup> It is unlikely that an alleged misappropriator's counternotice—that the information was removed by mistake or misidentification—would sway a trade-secret owner. Thus, the counternotice would not appear to serve a substantive purpose. Perhaps the result may be different if a counternotice (containing more than just a summary denial) were part of a procedure whereby a third party (like an arbitrator) would make a preliminary determination about the merit

---

163. By way of defense, the counternotice merely requires a statement under penalty of perjury that the material was removed by mistake or misidentification. *Id.* § 512(g)(3)(C).

164. *Id.* § 512(g)(2)(B).

165. *Id.* § 512(g)(2)(C). Material which has been taken down is apparently unlikely to be put back. *See* Urban & Quilter, *supra* note 8, at 670–80 (surmising that a possible reason is because alleged infringers move the material to another hosting service).

166. *See* 17 U.S.C. § 512(g)(2)(C).

167. *See supra* Part V.

168. While it seems unfair, on some level, not to allow a response from the person who posted the allegedly trade-secret information, unless a substantively useful purpose for the counternotification can be identified, the end result would be a counternotice process without a function—one that serves no purpose other than to create paperwork or the appearance of providing due process.

2007:5 *Takedown for Trade Secrets on the Internet* 1069

of the complainant's claim. The nature of trade-secret law, however, is such that it would be, at best, very difficult to make such a finding in an abbreviated manner or forum. There is no clear defense, such as a certificate of ownership of the trade secret, that the challenger can present to establish some presumption of a meritorious defense.

### G. *Strict Compliance Required*

Given the fluid nature in which trade secrets are identified as well as the drastic *ex ante* restraint that a takedown requirement imposes, it would appear that strict compliance with the notice provisions ought to be mandatory. Thus, a provider receiving an incomplete takedown notice may reject the notice for failure to comply with the statutory provisions.<sup>169</sup> One of the problems facing implementation of the DMCA's takedown provision has been the failure to comply with the strict notice requirements.<sup>170</sup> As a result, the question of whether an ISP can be protected by the liability limitations when the takedown notice has, for instance, failed to identify the allegedly infringing material with sufficient specificity has been met with mixed results.<sup>171</sup>

Requiring compliance with the notice requirement is also consistent with trade-secret law because in order to succeed on a misappropriation claim, a trade-secret plaintiff must identify the alleged trade secret with particularity.<sup>172</sup> Moreover, given the inability to precertify a trade secret,<sup>173</sup> a strict compliance requirement in the trade-secret context seems reasonable. This measure would also help alleviate potential abuses by providing an additional incentive for those submitting a takedown notice to be especially cautious about following the notice requirements. In addition, it would eliminate any uncertainty for providers that receive incomplete notices and are unsure about whether to proceed with the takedown.

---

169. Technical errors that are not defects in the substance of the notice, such as the misspelling of a name or a typographical error, may not be fatal.

170. See Urban & Quilter, *supra* note 8, at 667–78.

171. See, e.g., *ALS Scan, Inc. v. Remarq Cmty. Inc.*, 239 F.3d 619, 620, 626 (4th Cir. 2001) (reversing dismissal where the notice required that the newsgroup host delete an entire newsgroup and finding that notice was “substantially” compliant); *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1090 (C.D. Cal. 2001) (finding that notice did not substantially comply with statutory notice provisions for failing to provide sufficient information to identify the allegedly infringing auction listings).

172. See, e.g., *Computer Econ., Inc. v. Gartner Group, Inc.*, 50 F. Supp. 2d 980, 985 (S.D. Cal. 1999) (explaining the importance of identifying trade secrets); *Utah Med. Prods., Inc. v. Clinical Innovations Assocs., Inc.*, 79 F. Supp. 2d 1290, 1313 (D. Utah 1999) (granting summary judgment against the plaintiff for failure to identify trade secrets).

173. See *infra* Part VI.A.

This requirement does not espouse that a complaining trade-secret owner must disclose the details of the trade secret publicly in its takedown request because such disclosure would destroy the secret and cause the very harm the law is trying to avoid. Rather, consistent with already existing procedural practice in trade-secret-misappropriation cases, no more than what is necessary to meet the pleading requirements of a complaint should be provided.<sup>174</sup> Thus, the takedown request should call for a description of the trade secret in a manner adequate to permit the ISP to recognize and identify the objectionable posting. The request should also identify the particular location of the material by, for instance, a link or Web address.

#### *H. Prospective Application*

The Wal-Mart hypothetical presented at the beginning of this Article would be different if this proposal were enacted. Upon discovering the content of the sales circular on fatwallet.com on Friday afternoon, Wal-Mart would immediately submit a statutorily compliant takedown request to the operators of the Web site, along with the required fee.<sup>175</sup> The material would be removed within five hours. Wal-Mart would obtain the identity of the poster via the subpoena provision and would initiate an action within ten days of submitting the takedown or submit proof of an agreement with the poster. Otherwise, the material would be put back on the site. Thus, by Friday evening the information would be disabled. This is a far-shorter period of time than the approximately seven days that may have elapsed under the current regime.<sup>176</sup>

---

174. A plaintiff must generally plead (1) ownership of a trade secret, (2) misappropriation by the defendant, and (3) harm. *See* POOLEY, *supra* note 4, § 10.07[1]. Detailed descriptions of the trade secret are generally filed under seal and are subject to a protective order later in the litigation. *See id.*; FED. R. CIV. P. 26(b)(5) (allowing parties to describe the nature of information that is privileged without having to disclose or produce the privileged information itself).

175. It may also be wise to submit a takedown to the search engines, which may have already captured the information.

176. Wal-Mart may still have to contend with the fact that some people may have already accessed the information during the time that it was available. This is the kind of weakness that is inevitable when trade secrets appear on the Internet. However, the question of whether Wal-Mart may be able to enjoin its competitors from using the information is a separate issue that will necessitate a careful consideration of several factors, such as whether the information retained trade-secret protection despite having appeared on the Web site for a few hours and whether the competitor knew it was a trade secret when it came upon the information. *See* Rowe, *supra* note 3, at 29–37 (discussing a model for analyzing this kind of inquiry). Nonetheless, as part of the analysis, Wal-Mart's argument for retaining trade-secret protection will be strengthened by its having used the takedown provision instead of waiting about a week or more, at

2007:5 *Takedown for Trade Secrets on the Internet* 1071

Consider another example of a well-known company's trade secret being posted on the Internet. Assume that a disgruntled former Microsoft employee, Dave, who had access to the top-secret source code of a soon-to-be-released operating system, keeps the source code after leaving the company (in violation of his agreement) and decides to sell it on a Web site critical of Microsoft, *microsoftsucks.com*.<sup>177</sup> Dave posts it anonymously on the site and describes it as "jacked from Microsoft" and "not available anywhere else."

Microsoft discovers the posting immediately after it appears on the site and contacts the Web site to have it removed. The operators refuse to do so. Post enactment of a trade-secret-takedown provision, that refusal would most likely be replaced by compliance because of the promise of immunity. Assume, however, that Dave, in defending himself in a misappropriation action, claims that the takedown provision is unconstitutional because it violates his rights under the First Amendment. The next Part provides a framework within which to address such an argument.

## VI. OTHER POTENTIAL CONCERNS

While the discussion above has suggested some ways to strengthen this kind of trade-secret legislation, there may be other, more workable solutions. Moreover, takedown legislation is only one piece of the puzzle in dealing with the larger problem of trade secrets on the Internet, and any real solutions must involve a multifaceted approach that includes technological and international considerations. On balance, the potential benefits of this legislation outweigh the drawbacks, and it is a necessary initial step toward a resolution of the problem. However, this Part highlights a few additional issues that deserve consideration.

### A. *First Amendment Objections*

One of the strongest potential challenges facing a scheme that causes an ex ante removal of information from the Internet, without a court having had the opportunity to issue a ruling, is the First Amendment. "[T]he First Amendment generally prohibits limitations, absent some extraordinary showing of governmental interest, on the

---

which point the information would, in all likelihood, be deemed generally known and thus unprotectable.

<sup>177</sup>. This hypothetical is loosely based on *United States v. Genovese*, 409 F. Supp. 2d 253, 254-55 (S.D.N.Y. 2005).

publication of information already made public.”<sup>178</sup> When weighing First Amendment rights against the commercial interest in protecting trade secrets, courts are often reluctant to enjoin disclosures of trade secrets.<sup>179</sup> While the kind of speech restriction proposed here presents thorny issues, they are not insurmountable or fatal to trade-secret-takedown legislation. Ultimately, in practical terms, the goal is to strike the proper balance between preventing disclosures motivated by vengeance and reprisal and permitting those that are more readily recognized as being in the public interest.<sup>180</sup>

It is beyond the scope of this Article to enter the larger discussion about the role of the First Amendment in trade-secret law.<sup>181</sup> Nevertheless, this Article necessitates an underlying belief about the place of the First Amendment: limited exceptions for the use or disclosure of another person’s trade secrets without the privilege to do so ought not constitute protected expression under the First Amendment.<sup>182</sup> As a result, First Amendment rights may trump trade-secret protections in some circumstances, but not in most.

---

178. DVD Copy Control Ass’n, Inc. v. Bunner, 75 P.3d 1, 26–27 (Cal. 2003) (Moreno, J., concurring).

179. 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 and 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”).

180. For instance, a person may be privileged to disclose trade-secret information “that is relevant to public health or safety, or to the commission of a crime or tort, or to other matters of substantial public concern.” RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. c (1995). Some whistleblowing statutes also privilege disclosures of trade secrets. See, e.g., 5 U.S.C. § 2302(b)(8) (2000); N.Y. Lab. Law § 740 (McKinney 2002 & Supp. 2007).

181. For scholars 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); Epstein, *supra* note 29, at 1035–46; Franklin B. Goldberg, *Ford Motor Co. v. Lane*, 16 BERKELEY TECH. L.J. 271, 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, 534 (2002). For scholars 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, 542 (2001); Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147, 229–31 (1998); Volokh, *supra* note 43, at 739–48. For a recent expression of a middle ground between the two camps, see, Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777 (2007).

182. Cf. *In re Charter Commc’ns, Inc.*, 393 F.3d 771, 779–83 (8th Cir. 2005) (Murphy, J., dissenting) (reasoning that copyright infringement over the Internet is not protected expression).

2007:5 *Takedown for Trade Secrets on the Internet* 1073

To the extent trade-secret misappropriation often involves breaches of contract or breaches of confidence, the First Amendment would generally not be implicated.<sup>183</sup> Where the person posting the information is under a duty or is otherwise bound by an agreement not to disclose the trade secret, courts are more likely to address the incident as a contractual issue and such a posting would not present First Amendment concerns.<sup>184</sup> Thus, when an employee discloses his or her employer's trade secrets on the Internet, it is expected that the First Amendment would not sanction the conduct.

Nonetheless, where a contract did not bind an alleged misappropriator or the person posting the trade secret (a potentially relevant distinction on the Internet), the potential for running afoul of the First Amendment may be greater.<sup>185</sup> Thus, as to company outsiders who themselves are not bound by any duty of confidentiality, First Amendment concerns may be implicated.<sup>186</sup> Accordingly, the First Amendment question is relevant here to the extent that trade-secret takedown legislation would cover these persons.<sup>187</sup> In order to frame the issues in a succinct manner within the morass of First Amendment law,

---

183. See *Cohen v. Cowles Media Co.*, 501 U.S. 663 (1991) (holding that contracts not to speak are enforceable); Lidsky & Cotter, *supra* note 10, at 1595 (exploring anonymous speakers and tortious speech).

184. See *Snepp v. United States*, 444 U.S. 507 (1980); *Am. Motors Corp. v. Huffstutler*, 575 N.E.2d 116 (Ohio 1991); Samuelson, *supra* note 181, at 780 (discussing why the First Amendment is often not applicable in trade-secret cases).

185. See *Ford Motor Co. v. Lane*, 67 F. Supp. 2d 745 (E.D. Mich. 1999). The defendant operated a Web site with news about Ford and its products. Lane received confidential Ford documents from an anonymous source and initially agreed not to disclose most of the information. However, Lane eventually published some documents relating to the quality of Ford's products on his Web site because he believed that the public had a right to know. He did so despite knowing that the documents were confidential. Ford sought a restraining order to prevent publication of the documents, claiming the documents were trade secrets. The court acknowledged, without any discussion, that Ford could show Lane had misappropriated its trade secrets, but the court reversed the order on First Amendment grounds, concluding that considering an injunction to prevent Lane from publishing trade secrets was a prior restraint. *Id.* at 747-50.

186. The First Amendment may not protect a person who tries to convert a trade secret for economic gain. See *United States v. Genovese*, 409 F. Supp. 2d 253, 256 (S.D.N.Y. 2005).

187. One interesting side note is whether ISPs would have a recognized First Amendment right to assist in the disclosure of a trade secret. As a practical matter, the issue will likely be moot. Since compliance with a takedown provision would provide safe harbor to ISPs, they are unlikely to raise the issue. Beyond that, however, they are at least one step removed from the disclosure—mere vessels or a medium to transmit the information—thus, assertion of a right to speak appears attenuated. They are therefore neither like the individual posting the trade secret nor like the press in the First Amendment analysis.

the next Section discusses what will likely be the two main First Amendment objections to a trade-secret-takedown statute.

As long as the enacted regulation provides sufficient safeguards to ensure that complainants are owners of protectable trade secrets and there is recognition of certain exceptions to allow for expressions that are in the public interest, such as the health and safety exceptions already recognized by trade-secret law,<sup>188</sup> takedown legislation should withstand First Amendment scrutiny.<sup>189</sup> Moreover, the fact that the DMCA has withstood First Amendment challenges<sup>190</sup> suggests that a trade-secret-takedown provision ought to fare at least as well.

1. THE STATUTE OPERATES AS A PRIOR RESTRAINT ON SPEECH

The first objection will likely be that the statute, by providing for the removal of information from the Internet prior to a full adjudication on the merits, would allow a prior restraint on speech.<sup>191</sup> Injunctive orders are a staple of trade-secret law, however, and generally do not offend the First Amendment.<sup>192</sup> Injunctions in trade-secret law serve the important purposes of encouraging innovation and helping to preserve standards of commercial morality.<sup>193</sup> Indeed, trade-secret law specifically provides for preliminary injunctive relief as a remedy for misappropriation.<sup>194</sup> Accordingly, assuming that the majority of

188. See RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. c (1995).

189. Cf. *In re Verizon Internet Servs., Inc.*, 257 F. Supp. 2d 244, 258–64 (D.D.C. 2003) (“[T]here is some level of First Amendment protection that should be afforded to anonymous expression on the Internet, even though the degree of protection is minimal where alleged copyright infringement is the expression at issue.”), *rev’d on other grounds*, 351 F.3d 1229, 1233 (D.C. Cir. 2003) (finding that the DMCA provided sufficient safeguards).

190. See, e.g., *id.*; *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 454–55 (2d Cir. 2001) (upholding an injunction under the anticircumvention provision and finding that the government has a substantial interest in preventing unauthorized access to encrypted copyrighted material). More generally, the Supreme Court has made clear that the First Amendment does not protect speech that infringes copyright. See *Harper & Row, Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 555–60 (1985).

191. See generally RODNEY A. SMOLLA, 1 SMOLLA AND NIMMER ON FREEDOM OF SPEECH §§ 15:1, 15:2 (West 2007).

192. See Samuelson, *supra* note 181, at 780 (discussing why the First Amendment is often not applicable in trade secret cases).

193. See *DVD Copy Control Ass’n, Inc. v. Bunner*, 75 P.3d 1, 13 (Cal. 2003).

194. UNIF. TRADE SECRETS ACT § 2(a) (amended 1985), 14 U.L.A. 619 (2005) (“Actual or threatened misappropriation may be enjoined.”); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 44 (1995). This legislative authority for granting injunctive relief is significant in the First Amendment analysis since the Supreme Court justices in the *Pentagon Papers* case (often cited for free-speech and trade-secret issues) were concerned about the lack of legislative authority to enjoin the press from publishing

2007:5 *Takedown for Trade Secrets on the Internet* 1075

removals under the statute will involve persons who have posted information in violation of an agreement, duty not to disclose, or with knowledge that the trade secret was misappropriated, the prior-restraint argument is likely without merit.<sup>195</sup> Where the argument carries greater weight, however, includes circumstances involving journalists or news organizations publishing arguably newsworthy trade secrets.<sup>196</sup> However, the carveout for established news organizations alleviates this concern.<sup>197</sup>

a. *Internet posters analogous to traditional media?*

A very important, yet open, question that will have a significant effect on the discussion of Internet trade secrets and the First Amendment is whether courts will treat Internet posters as traditional media publishers. In *O’Grady v. Superior Court*,<sup>198</sup> the California Court of Appeals chose not to distinguish a person who published information on his Web site from “publishers who provide news to the public through traditional print and broadcast media.”<sup>199</sup> The focus of that case was on whether Apple Computer, Inc., could discover information about anonymous sources that had provided allegedly trade-secret information to the Web site.<sup>200</sup>

Even if reasoning similar to that in *O’Grady* were to be the widely adopted view on the question of Internet publishers’ entitlement to First Amendment protections, it is unlikely that Internet postings of trade secrets would receive broad protection under the First Amendment. First, clarification of “publisher” in the context of the Internet would be necessary. For instance, it is uncertain whether bloggers should or

---

documents that potentially threatened national security. *N.Y. Times Co. v. United States*, 403 U.S. 713, 731–33 (1971) (White, J., concurring).

195. For cases providing injunctive relief without implicating the First Amendment, see, for example, *Comprehensive Tech. Int’l, Inc. v. Software Artisans, Inc.*, 3 F.3d 730, 738–40 (4th Cir. 1993); *Metallurgical Indus., Inc. v. Fourtek, Inc.*, 790 F.2d 1195, 1197–98, 1208 (5th Cir. 1986); *SI Handling Sys., Inc. v. Heisley*, 753 F.2d 1244, 1254–55 (3d Cir. 1985); *United States v. Genovese*, 409 F. Supp. 2d 253, 256 (S.D.N.Y. 2005).

196. See, e.g., *CBS Inc. v. Davis*, 510 U.S. 1315, 1317–18 (1994) (holding that a preliminary injunction against a television network was a prior restraint); *Procter & Gamble Co. v. Bankers Trust Co.*, 78 F.3d 219, 224–25 (6th Cir. 1996) (holding that a preliminary injunction against a magazine publisher was a prior restraint); *Religious Tech. Ctr. v. Lerma*, 897 F. Supp. 260, 261–62 (E.D. Va. 1995) (characterizing a preliminary injunction against a newspaper as prior restraint).

197. See *supra* Part IV.D.

198. 44 Cal. Rptr. 3d 72 (Cal. Ct. App. 2006).

199. *Id.* at 106.

200. *Id.* at 76.

would be treated as traditional publishers or journalists for First Amendment purposes.<sup>201</sup> Second, because even traditional publishers and journalists may not always be shielded under the First Amendment (depending on the nature of their conduct),<sup>202</sup> trade-secret owners may prevail against First Amendment defenses. It is therefore important to realize that of all the possible conduct the statute may capture, only a small subgroup (the quasi-journalist Internet posters) may possibly raise meritorious prior-restraint concerns.

*b. Adequate safeguards*

Regardless of whether the statute is deemed content neutral or content based,<sup>203</sup> prudence would direct that it should contain adequate safeguards to survive First Amendment scrutiny.<sup>204</sup> Thus, provisions

---

201. *See id.* at 102–03 n.21.

202. This appears to be an unsettled area of the law. *Cf.* Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 1369 (E.D. Va. 1995). The court held:

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.

*Id.* at 1369. 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, 669–70 (1991) (reasoning that the press may be restricted from publishing information it unlawfully obtains without offending the First Amendment); Seattle Times Co. v. Rhinehart, 467 U.S. 20 (1984) (upholding an order prohibiting a newspaper’s publication of information obtained through the discovery process). 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 536–47 (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).

203. This kind of regulation is likely to be deemed content neutral. *See* DVD Copy Control Ass’n, Inc. v. Bunner, 75 P.3d 1, 11 (Cal. 2003) (finding that an injunction to protect statutorily created trade-secret rights was content neutral in that it promoted the goals of trade-secret law unrelated to the content). However, at least one commentator has argued otherwise. *See, e.g.*, Volokh, *supra* note 43, at 741 (“Even if the [trade-secret] law [as applied to third parties] is seen as content-neutral, it can’t be defended as a time, place, and manner restriction, because it doesn’t leave open ample alternative channels . . .”).

204. *See* Kingsley Books, Inc. v. Brown, 354 U.S. 436, 440 (1957) (upholding a statute permitting republication injunctions of allegedly obscene books where the

2007:5 *Takedown for Trade Secrets on the Internet* 1077

such as (1) the requirement of a bond to accompany a takedown request, (2) the temporary nature of the removal prior to court intervention, (3) the requirement of court intervention (i.e., filing a lawsuit) in a very short period, and (4) the remedy for a bad-faith takedown request serve to mitigate potential problems.<sup>205</sup> It is also worth noting that the information would have already been posted. Thus, the removal would not be a prior restraint in the traditional sense but would be more like an interruption of the speech until a court can rule on the merits.<sup>206</sup> While this fact by itself is not determinative<sup>207</sup> in the analysis, it may provide some perspective to the discussion.

*c. Lesser protection for commercial speech*

An additional perspective in the First Amendment analysis is that the statute implicates both core speech, which is generally the focus of the prior-restraint cases<sup>208</sup> and commercial speech.<sup>209</sup> Trade-secret law protects business information, and, as such, it is expected that business

---

legal standards for issuing the injunction were clear and there were procedural safeguards in place).

205. See *Thomas v. Chicago Park Dist.*, 534 U.S. 316, 321 (2002) (explaining that content-based restraints must contain such safeguards, such as expeditious judicial review, brevity of the restraint, and burden of proof on the censor). Content-neutral regulations do not require such heightened procedural safeguards. *Id.* at 322.

206. The term prior restraint describes “administrative and judicial orders forbidding certain communications when issued *in advance* of the time that such communications are to occur.” MELVILLE B. NIMMER, *NIMMER ON FREEDOM OF SPEECH* § 4.03 (1984) (emphasis added).

207. This is likely a “prior administrative restraint,” which requires similar procedural protections as traditional prior restraints. See *Ctr. For Democracy & Tech. v. Pappert*, 337 F. Supp. 2d 606, 656–57 (E.D. Pa. 2004).

208. See generally Edith L. Pacillo, Note, *Getting A Feminist Foot in the Courtroom Door: Media Liability for Personal Injury Caused by Pornography*, 28 *SUFFOLK U. L. REV.* 123, 130–33 (1994) (discussing the continuum in free-speech analysis).

209. The Supreme Court has defined commercial speech as speech that does “no more than propose a commercial transaction.” *Pittsburgh Press Co. v. Pittsburgh Comm’n on Human Relations*, 413 U.S. 376, 385 (1973). Where the speech in question both proposes a commercial transaction and addresses social or political issues, it may nevertheless still be treated as commercial speech. See *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 67–68. It seems that the very language utilized in commercial-speech cases does not necessarily fit the framework of trade-secret law. Unlike in trademark law, for instance, a trade-secret misappropriator (1) does not generally propose transactions with the secret other than trying to use it for self-gain (in which case it often will not be disclosed to others) and (2) the “economic motivation” of the misappropriator is often not for personal gain but rather to harm the trade-secret owner. *Cf. Procter & Gamble Co. v. Amway Corp.*, 242 F.3d 539, 553 (5th Cir. 2001) (discussing economic motivation in the traditional context as direct economic gain to the speaker).

entities (including nonprofit organizations) will be the beneficiaries of any takedown provision.<sup>210</sup> Although commercial speech can be difficult to define,<sup>211</sup> an argument can be made that trade-secret law, and in particular the information that would be subject to the takedown, implicates commercial speech rather than core First Amendment speech.<sup>212</sup> While commercial speech is entitled to First Amendment protection,<sup>213</sup> it receives a lesser degree of protection than that afforded to other kinds of speech, such as political speech.<sup>214</sup> Therefore, any assessment of First Amendment conflicts that arise when trade-secret law restricts protected speech must launch from this platform of weaker protection. In doing so, apples are compared to apples:<sup>215</sup> the permissibility of trade-secret restrictions are evaluated in light of the restrictions in other areas of intellectual property. Moreover, given that similar speech-restrictive regulations have passed constitutional muster in other areas of intellectual property bodes well for this proposal.<sup>216</sup>

## 2. THE STATUTE ACTS AS A PUNISHMENT FOR LAWFULLY OBTAINED TRUTHFUL INFORMATION ABOUT A MATTER OF PUBLIC SIGNIFICANCE

The second set of potential First Amendment objections to the statute will be derived from the Supreme Court's opinion in *Bartnicki*

---

210. Recent data suggests that business entities comprise the majority of those utilizing the DMCA takedown-notice provisions. Urban & Quilter, *supra* note 8, at 649–50.

211. Alex Kozinski & Stuart Banner, *Who's Afraid of Commercial Speech?*, 76 VA. L. REV. 627, 638–48 (1990); David F. McGowan, Comment, *A Critical Analysis of Commercial Speech*, 78 CAL. L. REV. 359, 381–410 (1990).

212. Core First Amendment speech generally relates to political, artistic, literary, historical, cultural, and social concerns. *See generally* Harry Kalven, Jr., *The New York Times Case: A Note on "The Central Meaning of the First Amendment,"* 1964 SUP. CT. REV. 191, 208. Merely because speech concerns a commercial subject does not necessarily make it commercial speech for First Amendment purposes. *City of Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 420 (1993). However, the speech must be evaluated as a whole, in context, and considering the discloser's motives. *See generally* Margreth Barrett, *Domain Names, Trademarks and the First Amendment: Searching for Meaningful Boundaries*, 39 CONN. L. REV. 973, 988 (2007) (discussing commercial and noncommercial speech in trademark law).

213. *See Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n*, 447 U.S. 557, 562–64 (1980).

214. *See id.* at 562–63; *Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc.*, 425 U.S. 748, 771–72 n.24.

215. Some scholars may take issue with a direct comparison of trade-secret law to copyright, patent, and trademark law given the debate about whether trade secrets are property. However, for the reasons expressed in the next Section, they are close enough to be considered apples (even if some are green and others are red).

216. *See supra* note 190 and accompanying text.

2007:5 *Takedown for Trade Secrets on the Internet* 1079

*v. Vopper*.<sup>217</sup> While *Bartnicki* was not a trade-secret case, the question before the Court was whether under the First Amendment the media could be liable for disclosing the contents of communications illegally intercepted by wiretapping.<sup>218</sup> A plurality of the Supreme Court reasoned that “if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need . . . of the highest order.”<sup>219</sup> The important considerations for *Bartnicki* appeared to be that the media respondents did not play a part in the illegal interception of the information, that they obtained the tapes lawfully, and that the information<sup>220</sup> was of public concern.<sup>221</sup>

To the extent the proposed statute punishes the media for posting lawfully obtained trade-secret information about matters of public significance, it could run afoul of *Bartnicki*. It does not, however. First, and most importantly, the carveout for established news organizations would render this argument essentially moot. Indeed, the takedown requests would not apply to information posted by exempted media organizations (the very kind of media outlets directly covered by *Bartnicki*). Even under an extremely liberal interpretation of *Bartnicki*, which reaches persons not covered under the carveout, the “lawfully obtained” and “public significance” factors are unlikely fatal to the statute.

*a. Unlawfully obtained*

The trade secrets subject to takedown under the statute would necessarily be unlawfully obtained; misappropriation of a trade secret requires a wrongful acquisition of the secret.<sup>222</sup> Mere acquisition of another’s trade secret (without use or disclosure) is actionable as long as the person knows or has reason to know that the trade secret was wrongfully acquired.<sup>223</sup> *Bartnicki* is distinguishable because Vopper, the radio commentator who obtained the tape, acquired the tape from

217. 532 U.S. 514 (2001).

218. *Id.* at 525.

219. *Id.* at 528 (quoting *Smith v. Daily Mail Publ’g Co.*, 443 U.S. 97, 103 (1979)).

220. The intercepted conversation included discussion of blowing up the front porches of the homes of adversaries of the union. *Id.* at 518–19.

221. *Id.* at 525.

222. See RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 cmt. a (1995) (“Protection is available only against a wrongful acquisition, use, or disclosure of the trade secret.”).

223. See *id.* § 40 cmt. b (1995); UNIF. TRADE SECRETS ACT § 1(2)(i) (amended 1985), 14 U.L.A. 537 (2005).

someone else who claimed that it had been left anonymously in his mailbox.<sup>224</sup> Thus, Vopper did not obtain the tape illegally.<sup>225</sup> A person who acquires a trade secret under similar circumstances would, however, unlawfully obtain it because the circumstances would suggest that the person had reason to know that the trade secret was wrongfully acquired.<sup>226</sup> Such acquisition in itself would constitute misappropriation. Thus, consistent with trade-secret law, the intent of the takedown statute would be to capture and require removal of precisely this kind of unlawfully obtained information and could be squared with *Bartnicki*.

*b. Public significance*

Keeping in mind the carveout for established news organizations, the remainder of the information implicated under the statute would not likely be information of public significance and not such that it would be shielded under *Bartnicki*. In fact, the plurality in *Bartnicki* specifically asserted that “[w]e need not decide whether [the interest in preserving privacy] is strong enough to justify the application of § 2511(c) to disclosures of *trade secrets* . . . or other information of *purely private concern*.”<sup>227</sup> This, at the very least, suggests that the Court considers trade secrets not to be at the level of public significance on which the *Bartnicki* decision turned. Two of the six justices (Justices Stephen Breyer and Sandra Day O’Connor) made clear in their concurrence that their vote relied on the fact that the speech involved was of “unusual public concern, namely, a threat of potential physical harm to others.”<sup>228</sup> Even though trade secrets might involve issues of public concern, it is very unlikely that a trade secret removed under the statutory scheme proposed here would meet the “unusual public concern” standard as articulated by Breyer and O’Connor.

Moreover, even if the removed trade-secret information were newsworthy, it is unclear whether the disclosure would be permissible under current trade-secret law.<sup>229</sup> Under the proposed legislation,

---

224. *Bartnicki*, 532 U.S. at 519.

225. The federal wiretap law at issue in the case made it illegal to “intentionally *disclose* . . . to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication.” 18 U.S.C. § 2511(1)(c) (2000) (emphasis added).

226. See discussion *supra* note 223.

227. *Bartnicki*, 532 U.S. at 533 (emphasis added).

228. *Id.* at 535–36 (Breyer, J. concurring).

229. In general, the trade-secret cases where First Amendment defenses have successfully shielded disclosures of allegedly newsworthy trade secrets have involved defendants who are journalists or news organizations. See, e.g., *CBS Inc. v. Davis*,

2007:5 *Takedown for Trade Secrets on the Internet* 1081

however, newsworthy trade-secret information could be posted in certain circumstances. For example, suppose the *Wall Street Journal* broke a story on its Web site based on leaked trade-secret information.<sup>230</sup> The takedown would not apply. If, however, the employee who obtained the trade-secret information posted it onto a chat site instead of sending it to the newspaper, the employee may be liable based for a breach of duty of confidence, regardless of the First Amendment.<sup>231</sup> Accordingly, the mere fact that the statute would cover information that may be of public significance would not, without more, offend the First Amendment. Indeed, the statute provides a built-in alternative to the individual who wishes to disclose a genuinely newsworthy trade secret of public significance: provide it to a news organization rather than posting it directly and subjecting it to a takedown request.

*c. An observation on the public-versus-private-concern labels*

The public-versus-private-concern distinction, though firmly rooted in First Amendment jurisprudence, is not, however, blessed with clarity or consistency.<sup>232</sup> Indeed, the boundary is blurry between that which is considered of “public concern”—and thus worthy of greater First Amendment protection—and that which is of private concern.<sup>233</sup> The highly subjective nature of the public-versus-private-concern

---

510 U.S. 1315, 1317 (1994) (involving CBS television network); *Procter & Gamble Co. v. Bankers Trust Co.*, 78 F.3d 219, 221 (6th Cir. 1996) (involving *Business Week* magazine); *Religious Tech. Ctr. v. Lerma*, 897 F. Supp. 260, 262 (E.D. Va. 1995) (involving the *Washington Post*).

230. One recent example of a similar event occurred in the spring of 2007 when a former Wal-Mart employee was sued by the company for, among other things, leaking trade secrets to the *Wall Street Journal*. Ann Zimmerman & Gary McWilliams, *Wal-Mart's Firing of a Security Aide Bites the Firm Back*, WALL ST. J., Apr. 9, 2007, at A1.

231. *Cf. Ford Motor Co. v. Lane*, 67 F. Supp. 2d 745, 753 (E.D. Mich. 1999) (holding that the First Amendment protects a third party from liability for disclosing trade-secret information because the third party was not under any duty not to disclose). This case suggests that the outcome would be different if the person posting were himself under a duty of confidence, such as an employee would be. *Id.*; *Snapp v. United States*, 444 U.S. 507, 509 (1980) (finding that a contract requiring a former Central Intelligence Agency agent to submit his memoirs for prepublication review was enforceable and not a prior restraint); *Boehner v. McDermott*, 484 F.3d 573, 580–81 (D.C. Cir. 2007) (holding that the First Amendment did not shield a congressman under duty of confidentiality when he disclosed an unlawfully intercepted taped conversation to the media).

232. *See generally* Cynthia L. Estlund, *Speech on Matters of Public Concern: The Perils of an Emerging First Amendment Category*, 59 GEO. WASH. L. REV. 1 (1990); Volokh, *supra* note 43, at 747.

233. *See* Volokh, *supra* note 43, at 747.

analysis may provide at least a partial explanation for this phenomenon.<sup>234</sup> There is a further danger from the First Amendment perspective in having courts decide what disclosures are newsworthy.<sup>235</sup> Yet, under trade-secret law courts routinely make similar discretionary decisions as they ultimately decide whether a protectable trade secret exists. Nevertheless, projecting that mold onto trade-secret law would appear to lead to the inexorable conclusion in virtually every case that the subject of the trade secret could be a matter of public concern. That is because, by definition, trade secrets would be valuable to competitors and, not surprisingly, of interest to them.

Accordingly, it would follow that if the formula to Coca-Cola (hailed as the quintessential trade secret)<sup>236</sup> were stolen and disclosed on the Internet, it would be considered of public concern because such a disclosure would be met with great interest from beverage competitors and consumers. This analysis is misplaced and ill-suited for trade-secret law, which even the *Bartnicki* court recognized.<sup>237</sup> It would swallow the protections granted under trade-secret law and concomitantly have the effect of creating a categorical rule that the First Amendment always trumps trade-secret law.

Trade-secret law recognizes limited circumstances in which an individual will be privileged to divulge trade-secret information because such information is in the public interest.<sup>238</sup> Using those exceptions as a guide, it would seem wise to modify the discourse by introducing more relevant and less ambiguous categorization. Namely, those trade secrets of “substantial public concern” will be privileged, as they arguably already are. But the vast remainder would concern private-business matters and either fall outside the purview of or be subject to a lower

---

234. *See id.* at 747–48 (criticizing courts’ public concern analyses and conclusions).

235. *See O’Grady v. Superior Court*, 44 Cal. Rptr. 3d 72, 114 (Ct. App. 2006) (noting the concern in having courts decide what technological disclosures are newsworthy).

236. *See, e.g., Coca-Cola Bottling Co. v. Coca-Cola Co.*, 107 F.R.D. 288, 289 (D. Del. 1985) (“The complete formula for Coca-Cola is one of the best-kept trade secrets in the world.”).

237. *See Bartnicki v. Vopper*, 532 U.S. 514, 533 (2001) (suggesting that trade secrets are matters of purely private concern); *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 762 (1985) (holding that a report about a company’s bankruptcy is not a matter of public concern); *DVD Copy Control Ass’n, Inc. v. Bunner*, 75 P.3d 1, 16 (Cal. 2003) (holding that the posting of source code is not substantially related to a legitimate matter of public concern).

238. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. c (1995). Some whistleblowing statutes also privilege disclosures of trade secrets. *See, e.g.,* 5 U.S.C.A. § 2302(b)(8) (West 2007); N.Y. Lab. Law § 740 (McKinney 2002 & Supp. 2007).

2007:5 *Takedown for Trade Secrets on the Internet* 1083

level of scrutiny under the First Amendment.<sup>239</sup> If the secret Coca-Cola formula contained a poisonous substance that company officials had been aware was causing cancer, then the person who posted that revelation on the Internet would have a stronger First Amendment defense than if the disclosure were merely to reveal nonharmful ingredients.<sup>240</sup>

Consider again the hypothetical involving Dave and the Microsoft source code. Dave is not likely to prevail on his First Amendment challenge for a host of reasons. First, Dave disclosed the trade secret in breach of his agreement with Microsoft, and a court is likely to find that the First Amendment will not sanction his conduct.<sup>241</sup> Second, to the extent Dave claims to have been merely expressing his dislike of Microsoft, Dave was not acting as a journalist but as a salesperson.<sup>242</sup> Third, if Dave or the Web-site operator were to attempt an argument under *Bartnicki* (even though the kind of media organization present in *Bartnicki* is absent here) it would likely fail<sup>243</sup> because the source code was unlawfully obtained—Dave knew that it was a Microsoft trade secret and that he was disclosing it in breach of his agreement with the company<sup>244</sup>—and because the source code does not implicate the kind of “unusual public concern” contemplated in *Bartnicki*.<sup>245</sup>

d. *Trade secrets as quasi-property*

Another factor that often touches on the debate about the role of the First Amendment in trade-secret law is the significance of viewing trade-secret protection as a property right. Courts tend to lend greater weight to interests that can be characterized as property rights when

---

239. This kind of test would, at least to some degree, include consideration of the discloser’s motives for posting the information. *See Bunner*, 75 P.3d at 15–16 (characterizing trade secrets that convey technical information as matters of private concern); Estlund, *supra* note 232, at 37 (suggesting that Supreme Court cases “strongly suggest that expression arising out of and motivated by a workplace dispute or other controversy in which the speaker has a personal stake is presumptively not of legitimate concern to the public”).

240. *See Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195, 1203 (N.D. Cal. 2004) (allowing postings of internal company e-mails regarding problems with voting machines under the fair-use rubric); *Dun & Bradstreet*, 472 U.S. at 761–62 (holding that distributing a credit report from a business declaring bankruptcy was not of public concern); *Connick v. Myers*, 461 U.S. 138, 147–48 (1983) (holding that a questionnaire concerning staff morale in a district attorney’s office in the context of an employee’s personal dissatisfaction with the office was not of public concern).

241. *See supra* notes 183–84 and accompanying text.

242. *See supra* Part VI.A.1.a.

243. *See supra* Part VI.A.2.

244. *See supra* Part VI.A.2.a.

245. *See supra* Part VI.A.2.b.

balancing against First Amendment concerns.<sup>246</sup> The question of whether trade-secret law confers a “property” right or merely protects against breaches of confidence has been subject to debate and supported by arguments on both sides.<sup>247</sup> However, analysis of contemporary trade-secret law may better recognize a hybrid-like nature of trade-secret law that is grounded in theories of both property and confidence, rather than in a mutually exclusive struggle.<sup>248</sup>

Thus, there is ample support for the position that despite the lack of exclusive rights to a trade-secret owner, trade-secret law confers sufficient property-like rights to at least require a thoughtful analysis under the First Amendment (rather than a categorical trumping by the First Amendment) and to grant it the same kind of deference as its intellectual property siblings.<sup>249</sup> This is not to suggest that treating trade secrets as property makes them immune to First Amendment concerns but rather that a lower level of scrutiny might be appropriate.

---

246. See, e.g., *DVD Copy Control Ass’n, Inc. v. Bunner*, 75 P.3d 1, 14 (Cal. 2003) (“[P]rohibiting the disclosure of trade secrets acquired by improper means is the only way to preserve the property interest created by trade secret law and its concomitant ability to encourage invention.”).

247. For those cases espousing a property view, see, *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1002 (1984); *Chicago Lock Co. v. Fanberg*, 676 F.2d 400, 404 (9th Cir. 1982); *E.I. du Pont de Nemours & Co. v. United States*, 288 F.2d 904, 912 (Ct. Cl. 1961); *Peabody v. Norfolk*, 98 Mass. 452, 458 (1868); *Den-Tal-Ez, Inc. v. Siemens Capital Corp.*, 566 A.2d 1214, 1228 (Pa. Super. Ct. 1989). For cases espousing a breach of confidence view, see, *E.I. du Pont de Nemours Powder Co. v. Masland*, 244 U.S. 100, 102 (1917); *Eastman Co. v. Reichenbach*, 20 N.Y.S. 110, 115–16 (1892); RESTATEMENT (FIRST) OF TORTS § 757 cmt. a (1939).

248. While it is true that trade-secret law protects against breaches of confidence, in order to succeed on a misappropriation claim, a trade-secret owner must prove that the information rises to protectable status as a trade secret. The breach alone, without the property-like protectable status, is insufficient. See *Lariscey v. United States*, 949 F.2d 1137, 1141 (Fed. Cir. 1991) (“The laws governing ownership and use of unpatented property and unpublished information thus derive from theories of property, adapted to achieve fairness in commercial relationships . . . .”) (internal citations omitted). For discussions on treating protection of information as property, see generally Andrew Beckerman-Rodau, *Are Ideas Within the Traditional Definition of Property?: A Jurisprudential Analysis*, 47 ARK. L. REV. 603, 624 (1994).

249. See, e.g., *Ruckelshaus*, 467 U.S. at 1003–04 (exposing a secret formula could be an unconstitutional taking); *Chicago Lock Co.*, 676 F.2d at 404; *E.I. du Pont de Nemours*, 288 F.2d at 912 (sale of secret process invoked capital-gains tax); *Bunner*, 75 P.3d at 13 (endorsing the property-rights view of trade-secret law); *Teller v. Teller*, 53 P.3d 240, 247–49 (Haw. 2002) (trade secrets are property for division in marital estate); *Peabody*, 98 Mass. at 458; *Den-Tal-Ez, Inc.*, 566 A.2d at 1228.

### B. Trade-Secret-Identification Issues

Unlike the other branches of intellectual property, an owner cannot register a trade secret and be granted a certificate or other proof of ownership.<sup>250</sup> Indeed, federal statutory law does not even govern trade-secret law; state law governs it.<sup>251</sup> An entity that has taken reasonable steps to protect valuable business information only knows with certainty whether a court will agree that the information is indeed a trade secret when the court actually makes the determination. With that in mind, permitting removal of materials that a trade-secret owner claims as trade secret before a court has had any opportunity to conduct a review can be problematic and subject to abuse.

This is not entirely unlike copyright law, however, which is itself highly nuanced, fact specific, and subject to the infamously uncertain fair-use defense. As a result, like § 512 notices, the trade-secret-takedown notices may be questionable. Even without bad faith, a notice may be deficient because of the legal difficulty in certifying a trade secret.<sup>252</sup> Accordingly, safeguards such as the bond/fee requirement, the required initiation of a misappropriation action, and the remedy for bad-faith takedown requests should be inserted at different stages of the takedown process help to address this concern.

### C. Technological Puzzles

Even with the best-laid legislation, technological advancement will continue to pose difficulties for trade-secret owners seeking to enforce their rights over the Internet. This is part of a larger problem where emerging technologies test the existing legal paradigms and create the ever-changing potential for users, with either good or bad intentions, to thwart the law.<sup>253</sup>

---

250. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. d (1995) (“It is not possible to state precise criteria for determining the existence of a trade secret. The status of information claimed as a trade secret must be ascertained through a comparative evaluation of all the relevant factors, including the value, secrecy, and definiteness of the information as well as the nature of the defendant’s misconduct.”); See MELVIN F. JAGER, 1 TRADE SECRETS LAW § 1:1 (2007).

251. Forty-five states and the District of Columbia have adopted the Uniform Trade Secrets Act (“UTSA”), which lends some uniformity in defining trade secrets and misappropriation. See Uniform Law Commissioners, A Few Facts About the Uniform Trade Secrets Act, [http://www.nccusl.org/update/uniformact\\_factsheets/uniformacts-fs-utsa.asp](http://www.nccusl.org/update/uniformact_factsheets/uniformacts-fs-utsa.asp) (last visited Nov. 9, 2007).

252. See Urban & Quilter, *supra* note 8, at 681 (discussing failure of some notice senders to understand the parameters of copyright law).

253. See generally Tomas A. Lipinski, *The Developing Legal Infrastructure and the Globalization of Information: Constructing a Framework for Critical Choices in*

Moreover, it would be remiss to overlook the cultural backlash that a trade-secret-takedown mechanism may engender, both generally and in specific cases. Indeed, there is always the risk that attempts to take down posted information may result in even more rapid spreading of the information.<sup>254</sup> At the very least, like the DMCA, Web sites or projects dedicated to collecting trade-secret owners' takedown notices are certain to emerge, giving even greater exposure to the alleged secrets.<sup>255</sup>

One approach would be to let the courts deal with these issues as they arise. Indeed, some commentators suggest that legislation constrains the courts who are better equipped to develop doctrine in a manner that is "fluid and responsive to changes in technology."<sup>256</sup> However, courts may often defer to policymakers to legislate these new challenges and simply find that certain technological advances are not contemplated in existing legislation.<sup>257</sup> As one court lamented:

It is not the province of the courts . . . to rewrite the DMCA in order to make it fit a new and unforeseen internet architecture, no matter how damaging that development has been . . . . The plight of copyright holders must be addressed in the first instance by the Congress . . . .<sup>258</sup>

In the end, there is no uncomplicated answer, and the solution probably lies in a multifaceted approach with built-in flexibility.

Even with legislation, it will continue to be possible for creative and motivated individuals to evade compliance. For example, a practical problem and potential loophole that may continue to plague

---

*the New Millennium Internet—Character, Content and Confusion*, 6 RICH. J.L. & TECH., 19, ¶¶ 22, 30 (Winter 1999–2000), <http://www.richmond.edu/jolt/v6i4article2.html> (discussing how copyright law and trademark law have had to adapt to new technologies); Richard H. Chused, *Rewrite Copyright: Protecting Creativity and Social Utility in the Digital Age*, ISRAEL L. REV., Fall 2005, at 80, 83 (discussing responses to new technological developments).

254. See *DVD Copy Control Ass'n, Inc. v. Bunner*, 10 Cal. Rptr. 3d 185, 190 (Cal. Ct. App. 2004) (discussing campaign to spread alleged trade-secret material in retaliation against plaintiff's lawsuit); Cundiff, *supra* note 2, at 410–11 (noting that filing a suit can lead to a "chatting frenzy on the Internet").

255. Cf. *supra* note 122 and accompanying text (discussing the Chilling Effects Project).

256. Daniel R. Cahoy, Comment, *New Legislation Regarding On-Line Service Provider Liability for Copyright Infringement: A Solution in Search of a Problem?*, 38 IDEA 335, 354 (1998).

257. See *In re Charter Commc'ns, Inc.*, 393 F.3d 771, 777 (8th Cir. 2005); *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229, 1238 (D.C. Cir. 2003).

258. *Verizon Internet Servs.*, 351 F.3d at 1238.

2007:5 *Takedown for Trade Secrets on the Internet* 1087

trade-secret owners is the ease with which alleged misappropriators can simply move the material to a different site after being subject to a takedown.<sup>259</sup> In other instances, they may also repost the information on the same site by altering their identities.<sup>260</sup> Moreover, even without human manipulation, a cached version of the information may remain on the search engine or on the hard drive of anyone who has viewed the information.<sup>261</sup> Once a search engine picks the information, it may also store the information on its own server, which makes it possible for multiple servers to store the material.<sup>262</sup> Finally, the information may also remain in archival form on the Internet.<sup>263</sup>

One glaring hole in enforcement of the DMCA has been peer-to-peer (P2P) file sharing, and it is worth considering how any trade-secret legislation should address this technological architecture (and others like it that are yet unanticipated). P2P-file-sharing services involve circumstances where users store files on their computers and send them directly to each other rather than having the material reside on a central server. Instead, the users' ISPs simply act as a conduit in the process. This kind of distribution system makes it difficult to identify the specific source of infringing material and to identify infringers.<sup>264</sup> Until the law in this area settles, proactive preemptive measures may be the best recourse for trade-secret owners.<sup>265</sup>

It is important to recognize that legislation alone may not be the best approach to this kind of problem, which in many ways seems ill-suited to the fluid and individualized nature of trade-secret law.

---

259. See, e.g., *Rossi v. Motion Picture Ass'n of Am. Inc.*, 391 F.3d 1000, 1002 (9th Cir. 2004) ("After receiving notice from his ISP that his website would be shut down, Rossi found a new ISP to host [the material]."); *Urban & Quilter, supra* note 8, at 679–80.

260. See, e.g., *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1097 (W.D. Wash. 2004) (discussing vendor whose account was terminated after a takedown notice but then who opened at least two different vendor accounts under slightly different names).

261. Cundiff, *supra* note 2, at 405.

262. See generally Matthew Fagan, Note, *Can You Do a Wayback on That? The Legal Community's Use of Cached Web Pages in and out of Trial*, 13 B.U.J. SCI. & TECH. L. 46, 50–55 (2007).

263. See, e.g., Internet Archive: Wayback Machine, <http://www.archive.org/web/web.php> (last visited Oct. 13, 2007).

264. Niva Elkin-Koren, *Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic*, 9 N.Y.U. J. LEGIS. & PUB. POL'Y 15, 17 (2006).

265. See, e.g., Larry Greenemeier, *Beware P2P Networks With a Tunnel To Confidential Data, Study Warns*, INFO. WK., Mar. 15, 2007, <http://www.informationweek.com/news/showArticle.jhtml?articleID=199600527> (discussing blocking company ports to prevent access to P2P networks and tracking potentially leaked data).

Ironically, in time, trade-secret owners may discover that technology proves the most successful way to combat other technology.<sup>266</sup> Imagine, for instance, a brave new world where Web crawlers search the Internet continuously for specially tagged trade-secret information and prevent its transmission or posting on any unauthorized site.<sup>267</sup> Until then, however, it would be imprudent for trade-secret owners to ignore the fact that the best defense is a good offense; vigilance in protecting<sup>268</sup> and monitoring trade secrets *before* they are posted on the Internet is critical. To that end, an assortment of technological tools is available to monitor employees and maintain better control of trade-secret information.<sup>269</sup>

#### D. International Materials

Some of the material targeted by a takedown notice may very well reside outside of the United States.<sup>270</sup> While foreign-owned material hosted on a U.S. server may be subject to U.S. laws, it is unclear whether material hosted outside the United States could be covered. The extent to which trade-secret misappropriation that occurs outside the United States may be redressed in U.S. courts is, to some degree, unsettled.<sup>271</sup> This could create practical and legal difficulties for a trade-

---

266. For instance, movie studios, frustrated by hackers discovering and posting passwords on the Internet to enable copying of DVDs, have a new strategy. If hackers post stolen passwords on the Web, the studios can change the passwords, disabling the ability to play the DVD unless the consumer downloads updated software with the new password. Keith Winstein, *Consumers May Get Caught in Piracy War—Strategy To Thwart Movie Copying Could Frustrate Innocent Users*, WALL ST. J., July 5, 2007, at B3.

267. Realization of such a scenario may be closer than one would think. *See, e.g.*, Kevin J. Delaney, Brooks Barnes & Matthew Karnitschnig, *Policing Web Video with ‘Fingerprints,’* WALL ST. J., Apr. 23, 2007, at B1 (reporting on policing web video with fingerprints to detect copyright infringement).

268. *See, e.g.*, *Four Seasons Hotels & Resorts v. Consorcio Barr*, 267 F. Supp. 2d 1268, 1301 (S.D. Fla. 2003) (discussing steps to protect plaintiff’s computer network); *Wrap-N-Pack, Inc. v. Eisenberg*, No. 04-cv-4887 (DRH)(JO), 2007 WL 952069, at \*9 (E.D.N.Y. Mar. 29, 2007) (illustrating plaintiff’s “significant safeguards” to protect its customer information).

269. For discussion of various technologies that are currently available, see Meir S. Hornung, *Think Before You Type: A Look at Email Privacy in the Workplace*, 11 FORDHAM J. CORP. & FIN. L. 115, 125–26 (2005); Cundiff, *supra* note 2, at 413–18; Daniel W. Park, *Trade Secrets, the First Amendment, and Patent Law: A Collision on the Information Superhighway*, STAN. J.L. BUS. & FIN., Autumn 2004, at 46, 60.

270. *See* Urban & Quilter, *supra* note 8, at 676 (reporting on the large number of § 512 notices that targeted material outside the United States).

271. *Compare* *Cisco Sys., Inc. v. Huawei Techs. Co.*, 266 F. Supp. 2d 551, 555 (E.D. Tex. 2003) (applying Texas trade-secret law in granting a worldwide preliminary injunction on a misappropriation claim but noting that Chinese trade-secret

2007:5 *Takedown for Trade Secrets on the Internet* 1089

secret owner, even with a takedown provision, since alleged infringers may simply move the information to a foreign server.

One answer involving possible criminal sanctions may lie with the Economic Espionage Act, which has a very broad territorial reach. This act covers conduct that occurs outside the United States as long as an “act in furtherance of the offense was committed in the United States.”<sup>272</sup> Furthermore, if the defendant is a U.S. corporation, citizen, or permanent resident, even acts of misappropriation that occur entirely on foreign soil violate the statute.<sup>273</sup> It might be advisable in this context to consider similar terms for trade-secret-takedown legislation that would operate independently or in conjunction with the Economic Espionage Act.

## VII. CONCLUSION

For trade-secret owners, the goal ought to be keeping trade secrets from leaking onto the Internet in the first instance. When a trade secret is revealed on the Internet despite the owner’s best efforts, however, as presented in the hypothetical at the beginning of this Article, any chance of saving the trade secret from destruction lies in the trade-secret owner’s acting with utmost urgency to prevent further dissemination of the secret. Currently, the only available judicial instrument to effectuate removal of a trade secret posted on the Internet is injunctive relief. The speed with which information can be circulated over the Internet, coupled with the time and expense involved in seeking injunctive relief, suggests that a more expedient and efficient mechanism is necessary to fill the gap until a court can intervene.

This Article has explored the possibility of legislation, using the safe-harbor provision of the DMCA as a starting point, that would offer a shield to trade-secret owners to protect their intellectual property while also providing a safe harbor to ISPs from trade-secret-misappropriation claims. From a trade-secret owner’s perspective, the ability to have trade-secret information removed from a Web site via a takedown provision is undoubtedly valuable. Accordingly, given the importance of trade secrets to American businesses, Congress should enact takedown legislation for trade secrets.

---

law may have been applicable), *with* BP Chems. Ltd. v. Formosa Chem. & Fibre Corp., 229 F.3d 254, 266 (3d Cir. 2000) (reversing grant of preliminary injunction on a trade-secret-misappropriation claim and finding that Taiwan, not the United States, would have a greater interest “in setting the standards that govern the conduct of its own citizens regarding intellectual property that is present within its borders.”)

272. 18 U.S.C. § 1837(2) (2000).

273. *Id.* § 1837(1).