Introducing A Take-Down for Trade Secrets on the Internet

Elizabeth A Rowe, University of Florida
INTRODUCING A TAKE-DOWN FOR TRADE SECRETS ON THE INTERNET

ELIZABETH A. ROWE

I. INTRODUCTION

II. BACKGROUND: TRADE SECRETS ON THE INTERNET

III. A TAKE-DOWN FOR TRADE SECRETS MERITS CONSIDERATION

IV. SECTION 512 OF THE DMCA

A. THE FORMATION OF THE DIGITAL MILLENNIUM COPYRIGHT ACT
B. DETAILS OF THE DMCA SAFE HARBOR PROVISION
C. SECTION 512 PROTECTION IN A NUTSHELL
D. SUMMARY OF DMCA CRITICISMS

V. ANATOMY OF THE LEGISLATION

A. SAFE HARBOR
B. DEALING WITH FRIVOLOUS REQUESTS
C. CARVE-OUT FOR MERE CONDUITS
D. CARVE-OUT FOR THE PRESS
E. SUBPOENA PROVISION
F. COUNTER-NOTICE NOT REQUIRED
G. STRICT COMPLIANCE REQUIRED
H. PROSPECTIVE APPLICATION

VI. OTHER POTENTIAL CONCERNS

A. FIRST AMENDMENT OBJECTIONS
1. The Statute Operates As a Prior Restraint on Speech
2. The Statute Acts As a Punishment for Lawfully Obtained Truthful Information about a Matter of Public Significance
B. TRADE SECRET IDENTIFICATION ISSUES
C. TECHNOLOGICAL PUZZLES
D. INTERNATIONAL MATERIALS

VII. CONCLUSION

* 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.
INTRODUCING A TAKE-DOWN

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, including their closely guarded sale prices, have just been posted on the bargain shoppers’ discussion forum, Fatwallet.com. Fearing that competitors may use knowledge of this valuable pricing information to compete unfairly, Wal-Mart’s attorneys immediately contact the operators of the website to request that its trade secret information be removed. 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.¹

This paper attempts to explore, for the first time, an existing void in trade secret law. This gap has not previously received attention in the legal scholarship. When a trade secret owner discovers 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.² In a previous paper I explored the implications of trade secrets appearing on the Internet, and the vast potential danger that could result in destruction of the trade secret.³ Accordingly, trade secret owners bear the burden of being


² See, e.g., DVD Copy Control Ass’n v. Bunner, 75 P.3d 1, 7-8 (Cal. 2003) (plaintiff was required to file suit against website operators after they ignored its request to remove its allegedly trade secret information from their websites). Another procedural approach might be to file an in rem action seeking removal of the posting. See Victoria 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. 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
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 take-down is not only costly, but is too slow for trade secret owners, given the speed with which information can be distributed over the Internet. Obtaining a temporary order from a court would likely take no fewer than several days.\(^4\)

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 an attempt to address this time lapse problem, this Article explores a proposal for trade secret take-down legislation, similar to that provided for the immediate removal of suspected copyright violations under the Digital Millennium Copyright Act (DMCA). A take-down provision for trade secrets would, like the DMCA, provide self-regulation and privatized enforcement in an effort to permit trade secret owners to save their trade secrets from a near certain death on the Internet. It 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\(^5\) and potentially poses such grave threats to trade secret

---

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

owners and to the functioning of our economy to merit action, or, at the
very least, an open discussion. The fact that no less than forty-two amicus
briefs supporting the trade secret owner were filed when the DVD v.
Bunner case was pending before the California Supreme Court is but one
salient indication of the importance of this issue to industry. 6

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
very lack of a take-down mechanism addressed in this Article. Unlike
copyright law which has yielded many instances of reported and unreported
cases involving copyright infringement on the Internet, 7 trade secret owners
who suffered from trade secrets posted on the Internet may have had to
disguise the claim in copyright clothing in order to try to utilize a take-down
under the DMCA. 8 Moreover, because the value of a trade secret lies in its

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.,

7 In the last three years approximately 70 reported decisions were issued addressing
copyright infringement and the DMCA. A search of the Westlaw Allfeds database for
“DMCA D.M.C.A. ‘Digital Millennium Copyright Act’ & ‘copyright infrig!’ & da (last 3
years) yielded 64 cases. The same search conducted in the Lexis Nexis Federal Court
Cases database yielded 73 cases.
The Chilling Effects database contained 1245 take-down notices related to the DMCA

8 See infra Part V for discussion of studies.

Indeed, attempting to use the DMCA take-down to address trade secret harm, may
have led to liability for misrepresentation. See, e.g., Online Policy Group v. Diebold, 337
F. Supp. 2d 1195, 1205 (N.D. Cal. 2004) (finding defendant liable under section 512(f) for
misrepresenting potentially trade secret protectable information as entitled to copyright
protection). Because the take-down provision under the DMCA applies exclusively to
copyright law, it may have had the unintended consequence of an over-reporting of
instances of alleged copyright infringement, and a corresponding under reporting 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 take-down legislation might be that it alleviates some of the misuse
of the DMCA’s take-down notices whereby claimants disguise what really are trade secret
claims as copyright infringement in order to make use of section 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
TECHNOLOGY. L. J. 621, 678, 684 (2006) (discussing use of section 512 notices for unfair
competition and privacy type claims and the extent to which the notices appeared to be
used against competitors).
secrecy, most misappropriators who have acquired another’s trade secrets and plan to use it for their own competitive advantage, have no incentive to publicize the secret.\textsuperscript{9} Thus, historically, trade secret misappropriation cases do not implicate disclosure of the secret, other than in a very limited fashion, such as to a new employer.

The rise of the Internet, however, has spawned a new motivation to acquire trade secrets for a reason other than competitive advantage: revenge. The great ease with which virtually anyone can post information on the Internet coupled with its “disinhibiting effect”\textsuperscript{10} and a general decline in employee loyalty in the workplace,\textsuperscript{11} have allowed disgruntled employees to achieve the ultimate revenge against their former employers by destroying trade secrets. One court captured the shift in balance of power made possible by the Internet in the following words: “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.”\textsuperscript{12} Accordingly, Internet disclosures are likely to become a greater problem than they have been in the past. Trade secret owners can also be deterred from filing suit fearing that such law suits will incite even greater discussion or disclosure of the trade secret online. One trade secret owner resorted to filing suit as an anonymous plaintiff in order to avoid further economic harm from the publicity, but was ultimately not permitted to proceed anonymously.\textsuperscript{13}

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

\textsuperscript{9} See, e.g., DVD v. Bunner, 10 Cal. Rptr. 3d 185, 195 (Court. App. 2004) (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.”)

\textsuperscript{10} Lyrissa Barnett Lidsky & Thomas 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).


\textsuperscript{13} America On Line, Inc. v. Anonymously Traded Public Company, 261 Va. 350 (2001) (the court granted the Internet Service Provider’s motion to quash finding that the plaintiff had not carried its burden of showing special circumstances to justify anonymity).
right of the public to free expression and to use of information in the public domain on the other. Ultimately, the objective would be for policy makers to create legislation that a trade secret owner can use as a shield to protect its intellectual property rather than a sword to suppress publication of embarrassing content. It is also important that any legislation be tailored to fit existing trade secret law principles in order to ensure consistency in implementation and application by courts. The proposed legislation in this Article is crafted with these objectives in mind.

The next section of this paper provides relevant background on the law pertaining to trade secrets on the Internet. Part III explains why a take-down provision for trade secret law merits consideration. Part IV summarizes the DMCA safe harbor provision. Part introduces components of trade secret take-down legislation, while Part VI addresses potential areas of concern such as the First Amendment and technological challenges. Finally, the Article concludes in Part VII.

---

II. BACKGROUND: TRADE SECRETS ON THE INTERNET

Trade secret law only protects secret information. The Internet makes information publicly available. Naturally, these opposing functions set the stage for conflict. Thus, many courts assume that a trade secret posted on the Internet has become generally known and consequently lost its trade secret status. Even when a party posting trade secret information may not have intended to cause harm to the trade secret owner, the nature of the Internet is such that the secret nonetheless could be destroyed. Unlike other mass media, the Internet has no editors who scrutinize submissions and decide what materials will be published. Any person sitting at a computer can post information onto the Internet, resulting in immediate and irreparable harm. One judge captured the problem in these words:

15 Parts of this section are derived from my earlier article which more fully addresses these issues. See Rowe, supra note 3, at 7-10.

16. 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.”).

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


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

20. See, e.g., Jerome Stevens Pharm., 402 F.3d at 1254 (reversing district court dismissal, holding that FDA could be liable for misappropriation of trade secrets where it posted plaintiff’s trade secrets on its website for five months, and remanding).
The court is troubled by the notion that any Internet user . . . can destroy valuable intellectual property rights by posting them over the Internet, especially given the fact that there is little opportunity to screen postings before they are made. Nonetheless, one of the Internet’s virtues, that it gives even the poorest individuals the power to publish to millions of readers can also be a detriment to the value of intellectual property rights. The anonymous (or judgment proof) defendant can permanently destroy valuable trade secrets, leaving no one to hold liable for the misappropriation.21

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.

In an earlier paper I proposed that under very limited circumstances a trade secret owner might be able to save its trade secrets from the near certain death sentence imposed by the Internet.22 Critical to that preservation model, however, is how long the trade secret is exposed and how quickly the trade secret owner acts to prevent further dissemination of the trade secret. The rate at which information moves through the Internet dictates that a trade secret owner’s actions should be correspondingly rapid. Information that has been posted for more than a day or two is much more likely to have become “generally known” and deemed to have lost its status as a trade secret.23

Accordingly, a trade secret owner who discovers its information on the Internet must respond immediately and show that it took prompt action to remove the information or stem its further dissemination.24 In seeking to retain trade secret protection on information that has been posted, the goal is to separate those trade secret owners who have “slept on their rights” upon discovering the potentially fatal disclosure from those who have responded promptly. Unfortunately, the tools currently in place for addressing removals from websites are not satisfactory given the special concerns these kinds of cases pose. If trade secret owners are to bear the

21 Netcom, 923 F. Supp. at 1256 (citations omitted).

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

23 Id. at 32-33.

24 The appropriate strategy must be carefully tailored in light of the circumstances. See Cundiff, supra note 2, at 409-13 (discussing considerations in litigating to remove trade secrets from the Internet).
burden of acting swiftly to remove trade secrets from websites, then our legal system should provide the appropriate, efficient, and effective mechanisms to do so. Therein lays the inspiration for this Article.

III. A TAKE-DOWN FOR TRADE SECRETS MERITS CONSIDERATION

A trade secret can be any information of value used in one’s business that has been kept secret and provides an economic advantage over competitors. The wide range of information that can be entitled to trade secret protection include customer lists, costs, sales records, customer information, marketing strategies, secret contract terms, unpublished pricing information, and chemical formulas. Trade secrets encompass approximately 80% of the assets of some companies, and prior to obtaining patent protection, virtually all inventions are covered by trade secret protection.

From an efficiency perspective, trade secrets deserve strong protection because of their importance to industry and the economy. Trade secrets are integral to the economy in that they protect and encourage innovation. United States publicly traded companies own an estimated $5 trillion in trade secret information. Trade secrets are important to

---


31 See Hutchins, supra note 29, at 292.
businesses of all sizes, from the smallest mom and pop shops to the largest multi-national entities. They often form the most valuable of companies’ intangible assets, 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 once a trade secret has been disclosed, even if inadvertently, it ceases to be a trade secret.

Part of the appeal of choosing trade secret protection over other kinds of intellectual property protection, is the broad scope of information that is protectable and the relative ease with which a business can claim such protection. A business can, for example, protect trade secrets without complying with a government registration system. Unlike copyright law, trade secret law by definition protects only economically valuable information. Copyright law covers “original works of authorship fixed in


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-Rodeau, The Choice Between Patent Protection and Trade Secret Protection: a Legal and Business Decision, 84 J. PAT. & TRADEMARK OFF. SOC’y 371 (2002). Accordingly, one who chooses trade secret protection over patent protection has not necessarily foregone 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, § 3.01[1] [a].


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 to 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. See Bibbero Systems, Inc. v. Colwell Systems, Inc., 893 F.2d 1104, 1106 (9th Cir. 1990).

37 See Roger M. Milgrim, Commission Proposed Capital Punishment – By Definition – For Trade Secrets, A Uniquely Valuable IP Right, 88 J. PAT. & TRADEMARK OFF. SOC’y
any tangible medium of expression,"38 whereas trade secret law protects invention and information, 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.”39 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.40

If, similar to copyrights, trade secret information is of such importance that it warrants special protections 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 the impetus for providing a “safe harbor” to Internet Service Providers in the form of a take-down was to address any potential liability for copyright infringement, the same concerns also apply to trade secret law.41 An Internet Service Provider may be liable for trade secret misappropriation if it knows or has reason to know that a subscriber is misappropriating a trade secret.42 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, since 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 the fair use doctrine in copyright law.43 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 might

---

40 See Marina Lao, supra note 32, at 1634.
41 Some commentators question whether ISPs should ever be liable for copyright infringement. See, e.g., Marjorie Heins and Tricia Beckles, Will Fair Use Survive? Policy Report by Brennan Center for Justice, pg. 5 (2005). However, this Article does not enter that debate.
42 See UNIF. TRADE SECRETS ACT § 1(20(ii). The Restatement of Torts and Restatement of Unfair Competition definitions are consistent with the UTSA.
suggest that trade secret law more clearly defines whether the use of material is inappropriate and that, consequently, take-down notices for trade secrets will rarely lack a legitimate basis. However, trade secret law suffers from its own gray areas involving the fluid nature of identifying trade secrets and the fact that unlike copyright law, trade secret law must confront First Amendment principles. Nevertheless, the damage from unauthorized copyright infringement is likely to be less than the damage from the posting of a trade secret.

IV. SECTION 512 OF THE DMCA

A. The Formation of the Digital Millennium Copyright Act

With the rise of the Internet came many changes to everyday life, but arguably one of the greatest transformations was the way the world adapted its protection of intellectual property (IP). Recognizing that the need to defend copyrights in the digital realm was particularly dire, as was the need to “facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age,” Congress developed the Digital Millennium Copyright Act (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.

Among the many areas of contention between copyright law and the Internet, Congress noted that without a strong form of protection from copyright infringement liability, the incentive of Internet service providers (ISPs) to increase efficiency and improve existing technology faced significant roadblocks from IP owners. In order to address these competing interests, Congress stated one of its objectives in creating the DMCA simultaneously to clarify liability facing ISPs and yet promote the

44 See notes 125 and 131 infra and accompanying discussion.

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

46 See infra Parts VII.A and VII.B.


online environment as a place to disperse copyrighted works. Indeed, Congress was all too cognizant of the fact that copyright owners would be justifiably hesitant to place their works on the Internet should there be no ready method of protecting them against the potential “massive piracy” Internet distribution entailed.

While there was a general consensus about the desired effect of the DMCA there was great disagreement about how to accomplish it. One of the developmental reports created by the Working Group on Intellectual Property Rights, called the “White Paper,” advocated making ISPs strictly liable for their users’ copyright infringement. Among the numerous reasons the White Paper held this view was that ISPs are more aware than copyright owners of the identities and actions of their users, and thus are more capable of detecting and preventing infringing uses. Further, in rejecting the notion that knowledge was a necessary element for ISP liability, the White Paper noted that copyright infringement can be accomplished without intent or inquiry into the infringer’s state of mind. The White Paper concluded that ISPs could then mitigate their copyright liability by declining to provide infringing users service, requiring proof of licensing, and requiring indemnification and warranty agreements from all users.

While the White Paper promoted the strict liability avenue for ISPs, it also acknowledged the many viable arguments against it. Most notably, the report recognized the strong ISP contention that, given the volume of information it would be responsible for, it would be impossible for it to be able to monitor and identify infringing material. Also, ISPs argued that

---

50 Id. at 8.

51 Id. at 2.

52 See Zarins, supra note 48, at 264-66.


54 Id. at 124.


56 Id. at 129-30.

57 Id. at 122.

58 Id.
even if they were capable of such a feat, they would be statutorily prohibited by the Electronic Communications Privacy Act from accessing any stored communications without authorization.\(^5^9\)

Moreover, critics of the White Paper questioned why it neglected to consider other arguably analogous case law regarding landlord and tenant relationships.\(^6^0\) Likening the landlord to an ISP, these cases implied that liability should not flow to the ISP given the limited capacity it has to supervise and inspect its respective digital premises.\(^5^1\) 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, thus impeding information dissemination, increasing the costs of ISP services, and chilling free exchange.\(^6^2\) Ultimately, these arguments carried the day for ISPs. Congress rejected many of the White Paper’s ideas by refusing to enact them.\(^6^3\)

Into this controversial environment came the California district court decision in \textit{Religious Technology Center v. Netcom On-Line Communication Services, Inc. (RTC)}, which inadvertently helped dictate the direction of ISPs’ liability under the DMCA.\(^6^4\) The Church of Scientology sued a former member, Dennis Erlich, who was allegedly posting its copyrighted information on the Internet using a bulletin board service (BBS) that utilized Netcom On-Line Communications (Netcom) as an ISP.\(^6^5\) When RTC petitioned the BBS and Netcom to cease allowing Erlich to


\(^5^1\) See Zarins, \textit{supra} note 48, at 266; Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 261 (9th Cir. 1996).


\(^6^3\) Zarins, \textit{supra} note 48, at 267.


post, both companies refused its request and were consequently added as defendants under a direct copyright infringement theory.\textsuperscript{66}

Even though the RTC court recognized that direct copyright infringement did not normally "require intent or any particular state of mind,"\textsuperscript{67} it still held that RTC had not shown the requisite likelihood of success on the merits for a preliminary injunction against the BBS and Netcom.\textsuperscript{68} Directly contradicting the theories espoused in the White Paper, the RTC court 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.”\textsuperscript{69} Moreover, RTC 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.\textsuperscript{70}

The RTC court left open whether or not Netcom could be liable as a contributory infringer,\textsuperscript{71} but noted that “a mere unsupported allegation of infringement by a copyright owner” may not be adequate for the knowledge requisite for contributory liability.\textsuperscript{72} In advocating what can best be described as a balancing of the burdens analysis for the knowledge requirement, the court stated that “[w]here 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 . . . .”\textsuperscript{73}

Thus, because Netcom acknowledged that had it actually looked at Erlich’s posting after receiving the notice it would have initiated an investigation for possible copyright infringement, the court left open whether Netcom could be subject to contributory liability.\textsuperscript{74} The court

\textsuperscript{66} \textit{Id.} at 1366.

\textsuperscript{67} \textit{Id.} at 1367.

\textsuperscript{68} \textit{Id.} at 1383.

\textsuperscript{69} \textit{Id.} at 1370.

\textsuperscript{70} \textit{Id.}

\textsuperscript{71} \textit{Id.} at 1374.

\textsuperscript{72} \textit{Id.}

\textsuperscript{73} \textit{Id.}

\textsuperscript{74} \textit{Id.} at 1374-75.
opined that Netcom had a duty to “take simple measures to prevent further damage to plaintiffs’ copyrighted works” once it had knowledge of Erlich’s infringing use of its services.\(^\text{75}\) Still, the court equitably balanced this obligation against the recognition that making ISPs responsible for monitoring all messages going through their system could “have a serious chilling effect on what some say may turn out to be the best public forum for free speech yet devised.”\(^\text{76}\)

Congress evidently was more impressed with the reasoning of the RTC court than it was with the White Paper. RTC was explicitly endorsed in the House Report for enactment of the On-Line Copyright Infringement Liability Limitation Act,\(^\text{77}\) which in turn eventually became the predicate for the DMCA’s Safe Harbor provisions.\(^\text{78}\) Indeed, in its discussion of the necessity to narrow and clarify the liability of service providers, the House Report referred to RTC as “the leading and most thoughtful judicial decision to date.”\(^\text{79}\) While being tentative not to “embark[ ] upon a wholesale clarification” of the doctrines of contributory and vicarious liability, the Senate Report also tacitly endorsed RTC 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.”\(^\text{80}\) Hence, through this relative codification of RTC’s principles, the so-called Safe Harbor Provision enumerated in 17 U.S.C. § 512 of the DMCA came to be.\(^\text{81}\)

---

\(^{75}\) Id. at 1375.

\(^{76}\) Id. at 1377-78.


\(^{78}\) Mike Scott, Safe Harbors under the Digital Millennium Copyright Act, 9 N.Y.U. J. LEGAL & PUB. POL’Y 99, 116 (2006)


\(^{80}\) S. REP. NO. 105-190, at 19 (1998).

\(^{81}\) Scott, supra note 78, at 116.
B. Details of the DMCA Safe Harbor Provision

In order for a service provider to qualify for the safe harbor, the alleged infringement generally has to occur during one of four basic activities: (i) transitory digital network communications, (ii) system caching, (iii) storing information at the direction of the user, or (iv) providing an information location tool. Furthermore, to protect service providers’ good faith actions to help mitigate infringement the provision additionally allows 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 to the affected service providers; including costs attorney’s fees. These limitations were designed to immunize service providers from liability for contributory infringement and provide “strong incentives” to foster cooperation between service providers and copyright owners in the fight against copyright infringement on the Internet.

In order to qualify for this relief from liability, service providers have to comply with certain stipulations set forth in 17 U.S.C. § 512(i). Among these conditions are the requirements that service providers not only adopt and implement procedures that allow for termination of repeat infringers, but also inform users of the policy’s existence. The provision also imposes an obligation on service providers 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.”

---

While these prerequisites apply to service providers seeking the limited liability under any of the subsections, service providers that provide services other than transitory digital communications must also satisfy the notice and take-down provision of 17 U.S.C. § 512(c). The take-down provision places an affirmative duty on service providers to “act expeditiously to remove, or disable access to, the material that is claimed to be infringing,” but only “upon obtaining actual knowledge” of infringement or “aware[ness] of facts or circumstances from which infringing activity is apparent.” The take-down provision is thus predicated on the fact that the service provider does not have control or receive financial benefit from the infringing activity.

Although the statute places no duty on service providers performing certain services to monitor its service for activity, it does create what the House Report referred to as a “red flag test” to determine when a service provider has a duty to act. In order to pass this test and maintain their limited liability, service providers 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. This test is thus comprised of both an objective and subjective portion, in that a service provider must not subjectively be aware of infringing activity that, objectively speaking, “would have been apparent to a reasonable person operating under the same or similar circumstances.”

Indeed, this red flag can be raised, for example, when a user gives the service provider a notification in compliance with the take-down provision. To permit this sort of notification, the service provider must designate and list with the Register of Copyrights an agent specifically designed to receive it. Among various other procedural requirements such as providing contact information and identifying the alleged infringing activity, this notice must include a statement “that the complaining party

---


92 Id.

93 Id.


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."96

The statute further requires that the copyright owner “substantially comply” with certain provisions of the take-down provision in order to ascribe sufficient knowledge to the ISP.97 However, as long as the complaining party substantially identifies the copyrighted material and infringing activity and provides contact information, the service provider must contact the complaining party or take other reasonable steps to bring the notification into compliance.98

Once the service provider receives a substantially compliant take-down notice and “acts expeditiously” to remove or disable access to the material99 it then must notify the subscriber that the material has been removed.100 The subscriber is subsequently permitted to provide a counter-notification 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.”101 Should the alleged infringer take advantage of this procedure, the service provider then must inform the copyright owner that it will replace or “cease disabling access to” the contested material within ten business days after receipt of the counter notification.102

To prevent the service provider 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.103 To facilitate this process and 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 a service provider to disclose the

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 their misrepresentation. See 17 U.S.C. § 512(f)(1)-(2) (1999).


identification of the alleged infringer “to the extent such information is available to the service provider.”

C. Section 512 Protection In A Nutshell

Section 512(a) provides the broadest protection for service providers who provide transmission and routing services and are thus a “mere conduit” of information. 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. The only condition of their safe harbor is that they adopt a policy for terminating repeat infringers and accommodate technical protection measures.

Sections 512 (c) and (d) apply to service providers providing hosting services and search engines. It is mainly to these providers that the take-down provision I discuss here applies. In order to receive the safe harbor from liability, these providers are required to remove allegedly infringing content, upon receipt of notice from the copyright holder. The 512(c) process requires that the service provider (i) “expeditiously” take down the information; (ii) notify the alleged infringer that the material has been removed; and (iii) forward any counter-notices from alleged infringers back to the original complainant. If, after 10-14 days, the complainant does not notify the service provider that it has filed an action against the alleged infringer, then the service provider may put-back the material.

---

106 Id.
107 Id.
108 Hosting services include, for instance, websites, forums, blogs, and social networking sites.
110 Search engines are not required to provide notice to the alleged infringer. See 17 U.S.C. § 512(d) (1999).
111 Id.
112 Id.
A brief mention of the anticircumvention provision and section 512 may also be of interest. Section 1201 of the DMCA makes it illegal to make available “anticircumvention” devices, or links to anticircumvention devices.\(^{113}\) However, it is interesting that illegal circumvention, by itself, at least in the view of one court, cannot be the subject of a section 512 notice, as it is separate and distinct from copyright infringement.\(^{114}\) It thus appears that the safe harbor provisions arguably do not apply to this section.\(^{115}\) I will note in passing that this provision seems to offer quasi trade-secret-like protection in that it essentially prohibits one from obtaining or accessing something which is being kept secret, i.e. the technological measures that protect the copyrighted work.\(^{116}\) Thus, favorable rulings upholding the validity of the anticircumvention provision may offer promise to a trade secret take down statute.\(^{117}\)

\(^{113}\) 17 U.S.C. § 1201 (1998);

\(^{114}\) 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 Section 1201 (a)(2), which applies only to circumvention products and technologies.") (internal citations omitted).


\(^{116}\) It provides even greater protection than that afforded under trade secret law, however, in that it appears to prevent reverse engineering. It prohibits trafficking in technology that can circumvent technological measures employed by the copyright owner. 17 U.S.C. § 1201 (1998).

\(^{117}\) See Universal City Studios 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 take-down provision. Many commentators believe that its implementation has been laden with abuses by copyright holders, and that it could be improved by better balancing the benefits to copyright owners with protections for posters of allegedly infringing material. However, despite its weaknesses (perceived or actual), the DMCA safe harbor provision has achieved the intended purposes which spurred the legislation; namely, it clarifies ISP liability for contributory copyright infringement and promotes the distribution of copyrighted works over the Internet. This Article does not undertake to address changes to the safe harbor provision of the DMCA. Rather, it simply uses it as a jumping off point from which to design a take-down for trade secrets, 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 take-down notices collected by the Chilling Effects project. The

118 See, e.g., Michael Driscoll, Will Youtube Sail into the Dmca’s Safe Harbor or Sink for Internet Piracy?, 6 J. Marshall Rev. Intell. Prop. L. 550, 566-568 (2007); Heins & Beckles, supra note 41, at 8; 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 (2006); Scott, supra note 80 passim; Urban & Quilter, supra note 8, at 640.

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

120 See id.

121 See supra note 50.

122 From its inception in 2002, the Chilling Effects Web site invites the public and
authors, Professor Jennifer Urban and Laura Quilter, noted several problematic concerns in the take-down notices identified by the study including (i) serious legal questions relating to the merits of the underlying copyright claims, (ii) failure to comply with statutory requirements in the written notice, and (iii) use of the notices to address claims other than copyright infringement.  

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

ISPs to submit cease and desist and take-down letters that they have received from copyright holders. http://www.chillingeffects.org/dmca512 (last visited August 10, 2007).

123 Urban & Quilter, supra note 8, at 640.
124 Id. at 667-78.
125 Heins & Beckles, supra note 41, at 8.
126 Id. at 8.
127 Section 512’s safe harbor provision does not apply to trademark infringement. § 512(c) (1999). See also Gucci America, Inc. v. Hall & Associates, 135 F. Supp.2d 409 (S.D.N.Y. 2001) (refusing to grant Internet Service Provider’s (“ISP”) motion to dismiss where trademark infringement allegedly occurred on a website hosted by the ISP).
128 Id. at 36.
129 Id. at 32. They reported that another twenty-seven percent of the sample covered material that by their assessment was possibly protected under fair use or the First Amendment. Id.
V. ANATOMY OF THE LEGISLATION

Admittedly, I will not assume the intricate task of drafting trade secret take-down legislation. However, in this part I offer some points for consideration, identifying some of the potentially thorny issues that may arise from this kind of regulation, and being mindful of existing trade secret law principles in suggesting prospective solutions. The lessons learned from implementation of section 512 of the DMCA are certainly helpful, and provide guidance on the direction of the 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 take-down could be either an expansion of the DMCA, an expansion of the Economic Espionage Act, or 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, notice of the alleged inappropriate posting of the trade secret would be provided by the complainant to the ISP. Upon receipt of the notice the ISP would need to remove the material within a very short period (probably within 5 hours). The trade secret owner must then file a complaint in court within a certain number of days (probably 10 days), or provide proof to the ISP of an agreement with the alleged misappropriator. Failure to take this step would result in automatic put-back of the information. A notice provision to alert the subscriber of the take-down could be required, but the nature of a counter-notice requirement is not as clear.

A. Safe Harbor

It is worth considering whether the framework of a “safe harbor” is the best approach for this kind of legislation. It probably is the better context in which to place a take-down requirement, because it is difficult to find other workable incentives to encourage service providers to be observant, or another rubric that could legitimately compel their compliance. An important component of misappropriation under trade

---


131 See supra notes 22 and 23 and accompanying discussion explaining the need for promptness.

132 Professor Mark Lemley proposes a uniform safe harbor provision for internet service providers that covers all of the areas of intellectual property. See Mark A. Lemley, Rationalizing Internet Safe Harbors (Aug. 2007) (unpublished draft manuscript). This would be an interesting alternative to the current piece meal approach to safe harbors. His
secret law, particularly in the context of intermediary liability, is knowledge that the information is another’s trade secret. One is liable for misappropriation if he turns a blind eye to or ignores the use of another’s trade secret. Accordingly, service providers could be liable for misappropriation when they transmit information in violation of trade secret law, with knowledge that the information is protectable. Weighed against the realities of the tremendous burden that it would (at least with today’s technology) impose upon them to police their users’ content, a safe harbor appears to be a fair balance. The trade secret owner bears the burden of monitoring the Internet, but the service provider 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 by the kind of service offered to the safe harbors. Otherwise, being over-inclusive increases the chances of take-down notices being sent to virtually every kind of service provider, even if liability would be extremely unlikely based on the kind of services offered. Not only does it create a high compliance burden on service providers, but it also magnifies the potential for a chilling effect on speech, as service providers acting in their best interest comply with notices to preserve their immunity even if liability would be remote. It is for this reason that service providers who are mere conduits are exempted under this proposal.

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. 93C1601, 1998 U.S. Dist. LEXIS 3221, at *19 (N. D. Ill. Mar. 16, 1998) (explaining that constructive notice that information was a trade secret is sufficient).


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.
B. Dealing with Frivolous Requests

Recognizing the potential for misuse of a take-down for trade secrets, a complaining trade secret owner’s take-down 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 take-down.\(^\text{139}\) 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 is 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.\(^\text{140}\) Alternatively, it could be a fee to the ISP as compensation for its having to divert resources to removing or disabling information within hours of receiving a take-down request.

In addition, there ought to be a statutory remedy for a frivolous take-down request.\(^\text{141}\) An alleged infringer whose material is improperly subject to a take-down under the DMCA has a remedy against the copyright owner if a “knowing material misrepresentation” was made in the notice to the service provider.\(^\text{142}\) In *Online Policy Group v. Diebold*,\(^\text{143}\) a federal district court in California concluded as a matter of law that Diebold had “knowingly materially misrepresented” that publication of its email archive exposing weaknesses in its voting machines was protected by copyright law, and this misrepresentation was material because the take down notice caused the websites to remove the email archives.\(^\text{144}\) Ironically, the contents of the emails might have been protectable under trade secret law.

An analogous bad faith-type standard seems appropriate for a trade secret take-down provision. While the standard may be difficult to meet depending on the particular circumstances of a case, it should not

---

\(^{139}\) See *Rossi v. Motion Picture Ass’n*, 391 F.3d 1000, 1002 (9th Cir. 2004).

\(^{140}\) See *Fed. R. Civ. P.* 65(c).

\(^{141}\) Under the DMCA, if one misrepresented her claim in the take-down notice, then she is liable to the service provider for any damages resulting from an improper removal of material. § 512(f).

\(^{142}\) § 512(f). Under subsection 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 counter-notice. *Id.*

\(^{143}\) 337 F. Supp. 2d 1195 (N.D. Cal. 2004).

\(^{144}\) *Id.* at 1204 (interpreting section 512(f)).
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 the Diebold case, one would expect that if a trade secret owner submits a take-down notice for material that a court determines the trade secret owner should have known was not protectable as a trade secret \(^{145}\) (because, for instance, it had not taken adequate steps to protect the information) then liability under a “knowing material misrepresentation” standard could be satisfied. Indeed, trade secret law precedent provides support for penalizing a trade secret owner for asserting a trade secret claim in bad faith, and an extension of this principle to this context would be entirely consistent. \(^{146}\) 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. \(^{147}\)

**C. Carve-Out for Mere Conduits**

Service providers that are merely conduits of alleged trade secrets, providing only transmission and routing services, should probably be exempt from the take-down notice procedure for two main reasons. \(^{148}\) First, as a practical matter, because material resides on their users’ computers rather than on the service provider’s servers, the service provider has no ability to remove material from its system. \(^{149}\) Second, it is highly unlikely that the mere transmission of trade secret information under these circumstances would constitute actionable trade secret misappropriation.

\(^{145}\) 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. CVD, Inc. v. Raytheon Co., 769 F.2d 842, 851 (1st Cir. 1985) (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 VII.B

\(^{148}\) Congress, in section 512(a), codifies the decision in RTC v. Netcom (“[i]t 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”). Religious Technology Center v. Netcom On-Line Communications Services, Inc., 907 F.Supp. 1361, 1372 (N.D. Cal. 1995). It thus preserves immunity for service providers who do no more than move packets of information on the Internet. See H.R. CONF. REP. NO. 105-796, at 19-20 (1998).

\(^{149}\) See Urban & Quilter, supra note 8, at 675 (discussing section 512(a) “take-down” notices to service providers acting as conduits).
Accordingly, since liability would not be well grounded in trade secret law, it appears to make little sense to include these transmitters as part of the take-down scheme, as it would merely unnecessarily impose costs and burdens to comply.\footnote{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.}

\section*{D. Carve-Out 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”\footnote{151}{This phrase is meant to capture traditional news organizations such as television stations, newspapers, and magazines that have editorial staff that review and make decisions about publication. It excludes bloggers, web site operators, and all non-traditional news persons. \textit{See also infra Part VII.A.1.a discussing such person’s legal status as publishers.}} from the take down statute. In particular, where members of such organizations played no part in illegally obtaining a trade secret that is a matter of public concern and accessed it lawfully, current Supreme Court jurisprudence would appear to shield them from liability for disclosure under the First Amendment.\footnote{152}{\textit{See} Bartnicki v. Vopper, 533 U.S. 514, 525 (2001). \textit{See also infra Part VII.A.2.}.} To be clear, providing a carve-out in this statute for the press does not provide immunity. Rather, where the trade secret appears on a website belonging to a covered organization, a trade secret owner could not utilize the take down statute to have the information removed. Instead, the currently existing process of filing suit and moving for a preliminary injunction would be required.

This carve-out 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 could serve as a filter for the intent of the poster: information that is newsworthy rather than information which is posted mainly to exact revenge or harm a trade secret owner is more likely to be protected.\footnote{153}{\textit{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 newsgathering process).} Furthermore, it would also 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 other matters of substantial concern.” 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 on-line editions which 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 of the alleged misappropriator might be of value. Nonetheless, recognizing that this kind of proviso could be fraught with hazards, a careful analysis, perhaps including an evaluation of the implementation of the DMCA’s corollary provision might be wise. For instance, the subpoena provision in section 512 does not appear to apply to service providers who are mere conduits, i.e. those who do not store material on their servers. 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, as is required under this proposal. However, it must be carefully tailored to avoid abuses. The


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

156 See section 512(h). 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. § 512(h)(2)(C).

157 See Recording Industry Ass’n of America, Inc. v. Verizon Internet Services, 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 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, as someone else could have used the computer. See, e.g., Emily Umbright, DMCA Proof Internet Law Still Evolving, St. Louis Daily Record, Aug. 29, 2003; http://findarticles.com/p/articles/mi_qn4185/is_20030829/ai_n10177627/print (last visited May 17, 2007)(discussing the music industry’s subpoenas to alleged copyright infringers).

159 See supra Part V.

160 See generally Lidsky & Cotter, supra note 10, at 1594-98 (discussing tort actions
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 take-down notice, perhaps additional safeguards should be required to help ensure, for instance, that (i) the subpoena is sought by a bona fide owner of a trade secret, (ii) it is intended to be used for the exclusive purpose of enforcing trade secret rights, and (iii) the alleged misappropriator has notice and an opportunity to object to its issuance. 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. Counter-Notice Not Required

Section 512 allows an ISP “subscriber” to submit a counter-notice contesting an allegation of copyright infringement. After receiving a counter-notice claiming that the targeted material is not infringing, the service provider must, within ten business days, notify the party providing the notice of the subscriber’s objection. If after receiving such notice, the copyright owner does not file suit within fourteen days, the material must then be re-posted or put back. While notice of the take-down to the subscriber is important, it is worth rethinking whether a counter-notice should be required and for what purpose.

---

161 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.

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

163 17 USC § 512(g)(3). The provisions do not require notice before the material has been removed, only after it has been removed. See 17 USC § 512 (g)(2)(A).

164 By way of defense, the counter-notice merely requires a statement under penalty of perjury that the material was removed by mistake or misidentification. Section 512 (g)(3)(C).

165 Section 512 (g)(2).

166 Section 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).
To some extent a counter-notice may not be an effective component for a trade secret take-down. First, the filing of a lawsuit under section 512 appears contingent upon the alleged misappropriator providing the counter-notice, in so far as unless the subscriber submits a counter-notice nothing in the statute requires the copyright owner to file an action.\(^{167}\) 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.\(^{168}\) The alleged misappropriator may request the put back after the requisite time has passed by providing notice to the service provider, with a copy to the complainant. Initiating a lawsuit may present practical difficulties for trade secret owners, but the requirement could serve as another safeguard against frivolous notices.

Although the ISP would be required to notify the subscriber that her material has been removed, and is the subject of a trade secret misappropriation allegation, it is unclear that a counter-notice procedure would be worthwhile.\(^{169}\) A trade secret owner is not likely to be swayed by an alleged misappropriator’s counter-notice stating that the information was removed by mistake or misidentification. Thus, the counter-notice would not appear to serve a substantive purpose. Perhaps the result may be different if a counter-notice (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 of the complainant’s claim. However, the nature of trade secret law 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.

\(^{167}\) See id.

\(^{168}\) See supra Part V.

\(^{169}\) While it seems unfair at some level to not allow a response from the person who posted the allegedly trade secret information, unless a substantively useful purpose for the counter notification can be identified, the end result would be a counter-notice process without a function, which serves no purpose other than to create paperwork or the appearance of providing due process.
G. Strict Compliance Required

Given the fluid nature in which trade secrets are identified as well as the drastic *ex ante* restraint which a take-down requirement imposes, it would appear that strict compliance with the notice provisions ought to be mandatory. Thus, a provider receiving an incomplete take-down notice may reject the notice for failure to comply with the statutory provisions, and need not proceed with the take-down until the notice has been corrected.170 One of the problems facing implementation of the DMCA’s take-down provision has been the failure to comply with the strict notice requirements.171 As a result, the question whether the service provider can be protected by the liability limitations when the take-down notice has, for instance, failed to identify the allegedly infringing material with sufficient specificity has met with mixed results.172

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.173 Moreover, given the inability to pre-certify a trade secret,174 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 take-down notice to be especially cautious about following the notice requirements. In addition, it would eliminate any uncertainty for providers who receive incomplete notices and are unsure about whether to proceed with the take-down, and of the status of their immunity resulting from such incomplete notices.

This requirement does not espouse that a complaining trade secret owner must disclose the details of the trade secret publicly in its take-down

---

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

171 See *supra* note 124.

172 See, e.g., ALS Scan, Inc. v. Remarq Communities, Inc., 239 F.3d 619 (4th Cir. 2001) (reversing dismissal where the notice required that news group 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, *inter alia*, failing to provide sufficient information to identify the allegedly infringing auction listings).


174 See *infra* Part VII.A.
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. Thus, the take-down 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

Returning to the Wal-Mart hypothetical presented at the beginning
of this paper, the scenario if this proposal were to be implemented, would
be different. Upon discovering the content of the sales circular on
fatwallet.com on Friday afternoon, Wal-Mart would immediately submit a
statutorily compliant take-down request to the operators of the website,
along with the required fee. 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
take-down 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, a far shorter period than the approximately
seven days that may have elapsed under the current regime, as described in
the hypothetical.

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

It may also be wise to submit a take-down to the search engines, which may have
already captured the information.

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 careful consideration of such factors as
whether the information retained trade secret protection despite having appeared on the
website 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
I will now use another well known company to illustrate the posting of a different kind of trade secret and in a different context. 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 offer it for sale on a website critical of Microsoft, Microsoftsucks.com. He posts it anonymously on the site, 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 website to have it removed. The operators refuse to do so. Post enactment of a trade secret take-down 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 take-down provision is unconstitutional because it violates his rights under the First Amendment. The next section provides a framework within which to address that argument.

VI. OTHER POTENTIAL CONCERNS

While the discussion above has attempted to suggest some ways to strengthen this kind of trade secret legislation there may also be other, more workable, solutions. Moreover, take-down legislation would be 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, which includes, for instance 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 section will highlight a few additional issues that deserve consideration.

---

178 This hypothetical is loosely based on United States v. Genovese, 409 F. Supp. 2d 253 (S.D.N.Y. 2005).
A. First Amendment Objections

One of the strongest potential challenges against a scheme which 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 publication of information already made public.” When weighing First Amendment rights against the commercial interests in protecting trade secrets, courts are often reluctant to enjoin disclosures of trade secrets. While the kind of speech restriction proposed here presents thorny issues, they are not insurmountable or fatal to trade secret take-down 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.

It is beyond the scope of this Article to enter the larger discussion about the role of the First Amendment in trade secret law, and many highly respected scholars have weighed in on the debate. Nevertheless, to the

179 Bunner, 31 Cal. 4th at 900 (Moreno, J., concurring).

180 See Procter & Gamble Co. v. Bankers Trust Co., 78 F.3d 219, 225 (6th Cir. 1996) (refusing to enjoin publication of trade secrets improperly obtained in violation of a protective order, noting, “[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.”

181 For instance, one 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 (1993). Some whistleblowing statutes also privilege disclosures of trade secrets. See, e.g., 5 U.S.C.A. § 2302(b)(8) (West 1996 & Supp. 2006); N.Y. Lab. Law § 740 (West 2002 & Supp. 2006).


For those advocating First Amendment rights over trade secret protection, see, for example, David Greene, Trade Secrets, the First Amendment, and the Challenges of the Internet Age, 23 HASTINGS COMM. & ENT. L.J. 537 (2001); Mark A. Lemley & Eugene Volokh, Freedom of Speech and Injunctions in Intellectual Property Cases, 48 DUKE L.J. 147, 229-31 (1998); Volokh, see 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
extent that an exposition of the kind undertaken in this Article necessitates an underlying belief about the place of the First Amendment, my peg would be closer to the middle of the debate. As an onlooker into the intricate world of First Amendment jurisprudence and its esteemed yet divergent commentators, I argue that, with limited exceptions, 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. As a result, First Amendment rights may trump trade secret protections in some circumstances, but not in most.

To the extent trade secret misappropriation often involves breaches of contract or breaches of confidence, the First Amendment would generally not be implicated by regulation of the illicit conduct. 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. Thus, one would expect that when an employee discloses her employer’s trade secrets on the Internet, the First Amendment would not sanction her conduct.

However, where the alleged misappropriator or the person posting the trade secret (a potentially relevant distinction on the Internet) was not bound by any such contract the potential for running afoul of the First Amendment may be greater. Thus, as to company outsiders who


183 Cf. Charter Comm’ns, 393 F.3d 771, 779-83 (8th Cir. 2005) (Murphy, J., dissenting) (reasoning that copyright infringement over the Internet is not protected expression).

184 See generally Cohen v. Cowles Media Co., 501 U.S. 663 (1991) (contracts not to speak are enforceable); see also Lidsky & Cotter, supra note 10, at 595 (exploring anonymous speakers and tortious speech).

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


The defendant operated a website 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 on his website relating to the quality of Ford’s products, thinking 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 reversed the order on First Amendment grounds, considering an injunction to prevent Lane from publishing trade secrets a prior restraint.
themselves are not bound by any duty of confidentiality, First Amendment concerns may be implicated. Accordingly, the First Amendment question is relevant here to the extent trade secret take-down legislation would cover these persons. In order to frame the issues in a succinct manner within the morass of First Amendment law, I will discuss below what I anticipate will be the two main First Amendment objections to a trade secret take-down statute.

In sum, however, as long as the enacted regulation provides sufficient safeguards to ensure that complainants are owners of protectable trade secrets, and that 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, take-down legislation should withstand First Amendment scrutiny. Moreover, the fact that the DMCA has withstood First Amendment challenges suggests that a trade secret take-down provision ought to fare at least as well.

187 The First Amendment may not protect one who tries to convert a trade secret for economic gain. See Genovese, 409 F. Supp. 2d at 256.

188 One interesting side note may be consideration of 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 take-down 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, thus assertion of a right to speak, where they are mere vessels or a medium to transmit the information, appears attenuated. They are therefore neither like the individual posting the trade secret nor like the press in the First Amendment analysis.

189 See supra note 178.

190 See In re Verizon Internet Servs., Inc., 257 F. Supp.2d 244, 258-64 (D.D.C. 2003), rev’d on other grounds, 351 F.3d 1229 (D.C. Cir. 2003) (finding that the DMCA provided sufficient safeguards).

191 See, e.g., In re Verizon Internet Servs., Inc., 257 F. Supp.2d 244, 258-64 (D.D.C. 2003), rev’d on other grounds, 351 F.3d 1229 (D.C. Cir. 2003) (finding that the DMCA provided sufficient safeguards); Universal City Studios 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). More generally, the Supreme Court has made clear that the First Amendment does not protect speech that infringes copyright. See Harper & Rowe, Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 55-60 (1985).
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.\textsuperscript{192} Injunctive orders are a staple of trade secret law, however, and generally do not offend the First Amendment.\textsuperscript{193} Injunctions in trade secret law serve the important purposes of encouraging innovation and helping to preserve standards of commercial morality.\textsuperscript{194} Indeed, trade secret law specifically provides for preliminary injunctive relief as a remedy for misappropriation.\textsuperscript{195} Accordingly, assuming that the majority of removals under the statute will involve persons who have posted information in violation of an agreement or duty not to disclose, or with knowledge that the trade secret was misappropriated by such a person, the prior restraint argument is likely to be without merit.\textsuperscript{196} Where the argument may carry greater weight, however, might be in circumstances involving journalists or news organizations publishing


\textsuperscript{193} See generally, Pamela Samuelson, supra note 181, at 780 (discussing why the First Amendment is often not applicable in trade secret cases).

\textsuperscript{194} See DVD Copy Control Ass’n v. Bunner, 75 P.3d 1, 13 (Cal. 2003).

\textsuperscript{195} See Unif. Trade Secrets Act § 2(a) (“Actual or threatened misappropriation may be enjoined.”). See also Restatement (Third) of Unfair Competition § 44.

\textsuperscript{196} For cases providing injunctive relief without implicating the First Amendment see, e.g., Comprehensive Technology. Int’l v. Software Artisans, Inc., 3 F.3d 730, 732 (4th Cir. 1993); SI Handling Sys. v. Heisley, 753 F.2d 1244, 1251 (3rd Cir. 1985); Smith v. Snap-On Tools Corp., 833 F.2d 578, 579 (5th Cir. 1987); Metallurgical Indus., Inc. v. Fourtek, Inc., 790 F.2d 1195, 1197-98 (5th Cir. 1986); Genovese, 409 F. Supp. 2d at 256.
arguably newsworthy trade secrets. However, the carve-out for established news organizations alleviates this concern.

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, the California Court of Appeal chose not to distinguish a person who published information on his website from “publishers who provide news to the public through traditional print and broadcast media.”

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 website.

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 would be treated as traditional publishers or journalists for First Amendment purposes.

Second, because even traditional publishers and journalists may not always be shielded under the First Amendment depending on the nature of their conduct, trade secret owners may prevail against First Amendment restrictions.

---


198 See supra Part IV.D.

199 44 Cal. Rptr. 3d 72 (Ct. App. 2006).

200 Id. at 106.

201 Id. at 76.

202 See, id. at 103, n. 21

203 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) (“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...
Amendment defenses. It is therefore important to realize that of all the possible conduct that may be captured by the statute, only a small sub-group (the quasi-journalist Internet posters) may possibly raise meritorious prior restraint concerns.

b. Adequate Safeguards

Regardless of whether the statute is deemed to be content-neutral or content based, prudence would direct that it should contain adequate safeguards to survive First Amendment scrutiny. Thus, provisions such as (a) the requirement of a bond to accompany a take down request, (b) the temporary nature of the removal prior to court intervention, (c) the requirement of court intervention (i.e. filing a lawsuit) and in a very short period, and (d) the remedy for a bad faith take down request serve to mitigate potential problems. 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 information.

Some Supreme Court cases also support the proposition that the conduct of a publisher may be taken into consideration in deciding whether to grant First Amendment protection. See, e.g., Cohen v. Cowles Media Co., 501 U.S. 663 (1991); Seattle Times Co. v. Rhinehart, 467 U.S. 20 (1984); see also Bartnicki v. Vopper, 532 U.S. 514 (2001) (addressing whether the media may be liable for using information unlawfully obtained by a third party); MARC A. FRANKLIN, DAVID A. ANDERSON, & LYRISDA BARNETT LIDSKY, MASS MEDIA LAW CASES AND MATERIALS 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).

This kind of regulation is likely to be deemed content neutral. See DVD v. Bunnner, 75 P.3d 1, 11 (Cal. 2003) (finding 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”).

See Kingsley Books, Inc. v. Brown, 354 U.S. 436, 440 (1957) (upholding a statute permitting pre-publication injunctions of allegedly obscene books where the legal standards for issuing the injunction were clear and there were procedural safeguards in place).

See Thomas v. Chi. Park District., 534 U.S. 316, 321 (2002) (explaining that content based restraints must contain such safeguards as expeditious judicial review, brevity of the restraint, and censor bearing burden of proof in court). Content neutral regulations do not require such heightened procedural safeguards. Id. at 322.
the speech until a court can rule on the merits. While this fact, by itself, is not determinative in the analysis it may help to 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 not purely core speech, which is generally the focus of the prior restraint cases, but presumably commercial speech as well. Trade secret law protects business information, and as such, it is expected that business entities (including non-profit organizations) will be the beneficiaries of any take-down provision. Although commercial speech can be difficult to define, an argument can be made that trade secret law, and in particular the information that would be subject to the take-down,

---

207 The term prior restraint describes “administrative and judicial orders forbidding certain communications when used in advance of the time that such communications are to occur.” Alexander v. United States, 509 U.S. 544, 550 (1993) (emphasis added).

208 This is likely to be considered a “prior administrative restraint,” requiring similar procedural protections as traditional prior restraints. See Center For Democracy & Technology v. Pappert, 337 F. Supp.2d 606, 656-57 (E.D. Pa. 2004).


210 The Supreme Court has defined commercial speech as speech that does “no more than propose a commercial transaction.” Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 66 (1983). 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 id at 67-68.

211 Recent data suggests that business entities comprise the large majority of those utilizing the DMCA take-down notice provisions as well. Urban & Quilter, supra note 8, at 649-50.

implicates commercial speech rather than core First Amendment speech. While commercial speech is entitled to First Amendment protection, it is a lesser degree of protection than that which would apply to other kinds of speech, such as political speech. 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 we can compare apples to apples: whether trade secret restrictions are permissible in light of permissibility of restrictions in other areas of intellectual property, rather than, for instance, that effecting core speech. Moreover, given that similar speech restrictive regulations have passed constitutional muster in other areas of intellectual property, bodes well for this proposal.

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 v. Vopper. While Bartnicki was not a trade secret case, the question before the Court was whether under First Amendment the media could be liable for

---


Merely because speech concerns a commercial subject does not necessarily make it commercial speech for First Amendment purposes. See City of Cincinnati v. Discovery Network, 507 U.S. 410, 421(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 non-commercial speech in trademark law).


215 See, id; see also Virginia State Board. Of Pharmacy, 425 U.S. at 771-72 & n. 24.

216 Some 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 sub part, they are close enough to be considered apples (even if some are green and others are red).

217 See supra note 191 and accompanying text.

disclosing the contents of information illegally intercepted by wiretapping.\textsuperscript{219} 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.”\textsuperscript{220} The important considerations for the Bartnicki court appeared to be that the media respondents did not play a part in the illegal interception of the information, they obtained the tapes lawfully, and the information\textsuperscript{221} was of public concern.\textsuperscript{222}

To the extent the proposed statute was to punish the media for posting lawfully obtained trade secret information about matters of public significance, it could run afoul of Bartnicki. However, it does not. First, and most important, the carve-out for established news organizations would render this argument essentially moot. Indeed, the take-down requests would not apply to information posted by the exempted media organizations (the very kind of media outlets directly covered by Bartnicki). If one were to adopt an extremely liberal interpretation of Bartnicki to reach those persons not covered under the carve-out, it is still unlikely that the “lawfully obtained” and “public significance” factors would be fatal to the statute.

a. Unlawfully Obtained

The trade secrets subject to take-down under the statute would necessarily be unlawfully obtained. That is because misappropriation of a trade secret requires a wrongful acquisition of the secret.\textsuperscript{223} 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.\textsuperscript{224} Bartnicki is distinguishable because Vopper, the radio commentator who obtained the tape from someone else who claimed

\textsuperscript{219} \textit{Id.} at 525.

\textsuperscript{220} \textit{Id.} at 528 (internal citations omitted).

\textsuperscript{221} The intercepted conversation included discussion of blowing up the front porches of the homes of adversaries of the union. \textit{Id.} at 518-19.

\textsuperscript{222} \textit{Id.} at 525.

\textsuperscript{223} See \textit{RESTATEMENT (THIRD) OF UNFAIR COMPETITION} § 43, cmt. a (“Protection is available only against a wrongful acquisition, use, or disclosure of the trade secret.”)

\textsuperscript{224} See \textit{RESTATEMENT (THIRD) OF UNFAIR COMPETITION} § 40, cmt. b; \textit{UNIF. TRADE SECRETS ACT} § 1(2)(i).
the tape had been left anonymously in his mailbox.225 did not obtain it illegally.226 One who acquired a trade secret under similar circumstances, however, would be deemed to have “unlawfully obtained” it, as such acquisition in itself would constitute misappropriation. Thus, consistent with trade secret law the intent of the take-down 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 carve-out for the 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.”227 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 O’Connor and Breyer) 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.”228 Even if one were to accept that trade secrets may at times 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 these Justices.

Moreover, even if the removed trade secret information were newsworthy it is unclear whether the disclosure would be permissible under current trade secret law jurisprudence, even in light of the First Amendment.229 Thus, suppose the Wall Street Journal was to break a story

225 Bartnicki, 532 U.S. at 519.

226 The federal wiretap law at issue in the case made it illegal to “intentionally disclose . . . to any 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 (a)(c)(2000) (emphasis added).

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

228 Id. at 535 (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, 510
on its website based on leaked trade secret information, the take-down 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, he may be liable based on a breach of his duty of confidence regardless of the First Amendment. 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: she can provide it to a news organization rather than posting it directly and having it be the subject of a take-down request.

c. An Observation on the Public v. Private Concern Labels

The public versus private concern distinction, though firmly rooted in First Amendment jurisprudence, is not, however, blessed with clarity or consistency. Indeed, the boundaries of that which is considered of “public concern” and thus worthy of greater First Amendment protection versus that which is of private concern are blurry. The highly subjective public v. private concern distinction

---

230 One recent example of a similar event occurred this past spring when a former Wal-Mart employee was sued by the company for, among other things, leaking trade secrets to the Wall Street Journal. See Ann Zimmerman and Gary McWilliams, Wal-Mart’s Firing of a Security Aide Bites the Firm Back, THE WALL STREET JOURNAL, April 9, 2007 at A1.

231 Cf. Ford Motor Co v. Lane, 67 F. Supp. 2d 745, 753 (E.D. Mich. 1999) (First Amendment protects third party from liability for disclosing trade secret information because he 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.


233 See id.
nature of the public versus private concern analysis may provide at least a partial explanation for this phenomenon.\textsuperscript{234} There is a further danger from the First Amendment perspective in having courts decide what disclosures are newsworthy and which are not,\textsuperscript{235} 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 the formula to Coca-Cola (hailed as the quintessential trade secret)\textsuperscript{236} if stolen and disclosed on the Internet 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, as even the \textit{Bartnicki} court recognizes.\textsuperscript{237} 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 when an individual will be privileged to divulge trade secret information because such information is in the public interest.\textsuperscript{238} 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 that are deemed 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

\begin{enumerate}
\item \textsuperscript{234} See Volokh, supra note 43, at 747-48 (criticizing courts’ public concern analyses and conclusions).
\item \textsuperscript{235} See O’Grady, 44 Cal. Rptr. 3d at 114 (noting the concern in having courts decide what technological disclosures are newsworthy).
\item \textsuperscript{236} See, e.g., Coca-Cola Bottling Co. v. Coca-Cola Co., 107 F.R.D. 288 (D. Del. 1985) (noting that the complete formula for Coca-Cola is one of the best kept secrets in the world).
\item \textsuperscript{237} See Bartnicki, 532 U.S. at 533 (suggesting that trade secrets are matters of purely private concern); Dun & Bradstreet, Inc. v. Greenmoss Builders Inc., 472 U.S. 749, 789 (1985) (holding that a report about a company’s bankruptcy is not a matter of public concern); DVD Copy Control Ass’n v. Bunner, 75 P.3d 1, 16 (Cal. 2003) (posting of source code not substantially related to a legitimate matter of public concern).
\item \textsuperscript{238} See supra note 181.
\end{enumerate}
lower level of scrutiny under the First Amendment.\textsuperscript{239} Continuing on with the Coca-cola hypothetical, if the secret formula contained a poisonous substance which company officials had been aware were causing cancer, then one who posted that revelation on the Internet would have a stronger First Amendment defense than if the disclosure were to merely reveal non-harmful ingredients.\textsuperscript{240}

It is now time to revisit the First Amendment claim in the hypothetical involving Dave and the Microsoft source code, introduced in the preceding section. Dave is not likely to prevail on his First Amendment challenge for a host of reasons, including, among others: (i) 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;\textsuperscript{241} (ii) 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, and even the broadest reading of \textit{O'Grady} (if it were more widely accepted as a rule) would not likely save him;\textsuperscript{242} (iii) If Dave or the website operator were to attempt an argument under \textit{Bartnicki} (even though the kind of media organization present in \textit{Bartnicki} is absent here) they are not likely to be met with success.\textsuperscript{243} The source code was unlawfully obtained because Dave knew that it was a Microsoft trade secret and that he was disclosing it in breach of his agreement with the company.\textsuperscript{244}

---

\textsuperscript{239} This kind of test would, at least to some degree, include some consideration of the discloser’s motives for posting the information. See DVD v. Bunner, 75 P.3d 1, 15-16 (Cal. 2003) (characterizing trade secrets that convey technical information as matters of private concern); \textit{See also} Estlund, \textit{supra} note 227, at 37 (suggesting that supreme court cases “strongly suggest that expression arising out of and motivated by workplace dispute or other controversy in which the speaker has a personal stake is presumptively not of legitimate concern to the public.”)


\textit{See also} Dun & Bradstreet v. Greenmoss builders, 472 U.S. 749, 761 (1985) (holding that distributing credit report about business declaring bankruptcy was not of public concern); Connick v. Myers, 461 U.S. 138, 147-48 (1983) (holding that questionnaire concerning staff morale in district attorney’s office, in the context of an employee’s personal dissatisfaction with the office, not of public concern).

\textsuperscript{241} See notes 184 and 185 and accompanying text.

\textsuperscript{242} \textit{See supra} Part VI.A.1.a.

\textsuperscript{243} \textit{See supra} Part VI.2.

\textsuperscript{244} \textit{See supra} Part VII.2.a.
d. Trade Secrets as Quasi-Property

It is worth mentioning another factor that often touches on the debate about the role of the First Amendment in trade secret law; 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 balancing against First Amendment concerns.\textsuperscript{246} The question 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.\textsuperscript{247} However, analysis of contemporary trade secret law may do better to recognize a hybrid-like nature of trade secret law which is grounded in theories of both property and confidence, rather than in a mutually exclusive struggle.\textsuperscript{248}

Thus, for the purposes of this Article, 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

\textsuperscript{245} See supra Part VII.2.b.

\textsuperscript{246} See, e.g., Bunner, 75 P.3d at 14 (“prohibiting 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.”)


\textsuperscript{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 Lariscoy 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).
trumping by the First Amendment), and to grant it the same kind of deference as its other intellectual property siblings. 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.

B. Trade Secret Identification Issues

Unlike the other branches of intellectual property, one cannot “register” a trade secret and be granted a certificate or other proof of ownership. Indeed, there is not even federal statutory law governing trade secret law: it is governed by state law. An entity which has taken reasonable steps to protect valuable business information which it claims as a trade secret, only knows with certainty whether a court will agree that the information is indeed a trade secret when such a determination is made by the court in the course of trade secret litigation. 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.

However, this is not entirely unlike copyright law which is itself highly nuanced, fact specific, and subject to the infamously uncertain fair use defense. As a result, like section 512 notices, the trade secret take-down notices may suffer from questionable notices that, even without bad faith, are a result of the legal difficulty in certifying a trade secret.


250 “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.” RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39, cmt. d. See also MELVIN F. JAGER, 1 TRADE SECRETS LAW § 1:1, para. 2 (2003).

251 Forty-four states and the District of Columbia have adopted the Uniform Trade Secrets Act (“UTSA”), which lends some uniformity in defining trade secrets and misappropriation.

252 See Urban & Quilter, supra note 8, at 681 (discussing failure of some notice senders to understand the parameters of copyright law).
Accordingly, safeguards such as the bond/fee requirement, the required initiation of a misappropriation action, and the remedy for bad faith take-down requests inserted at different stages of the take-down 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.\(^{253}\)

Moreover, one would be remiss to overlook the cultural backlash that a trade secret take-down 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.\(^{254}\) At the very least, like the DMCA, websites or projects dedicated to collecting trade secret owners’ take-down notices are certain to emerge, giving even greater exposure to the alleged secrets.\(^{255}\)

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.”\(^{256}\) However, courts may often defer to the policy makers to legislate these new challenges, and simply find that certain technological advances were not contemplated in


\(^{254}\) See DVD Copy Control Ass’n Inc. v. Bunner, 10 Cal. Rptr. 3d 185, 190 (Ct. App. 2004) (discussing campaign to spread allegedly trade secret material in retaliation against plaintiff’s lawsuit). See also Cundiff, supra note 2, at 410-11 (noting that filing suit can lead to a “chatting frenzy on the Internet.”).

\(^{255}\) Cf. note 122 supra and accompanying text discussing the Chilling Effects Project.

existing legislation. 257 As one court lamented, “[i]t 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 . . . . [t]he plight of copyright holders must be addressed in the first instance by the Congress . . . .” 258 In the end, there is no uncomplicated answer and the solution probably lies in a multifaceted approach to these problems 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 which may continue to plague trade secret owners is the ease with which alleged misappropriators can simply move the material to a different site after being subject to a take-down on one site. 259 In other instances they may also re-post the information on the same site by altering their identities. 260 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. 261 Search engines may also store information on their own servers once it has been picked by their engine, making it possible for the material to be stored on multiple servers. Finally, the information may also remain in archival form on the Internet. 262

One glaring hole in enforcement of the DMCA has been peer-to-peer 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). Peer-to-peer (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

257 An example of this kind of bounce back is evident in the peer to peer file sharing cases brought under the DMCA take down provisions. See discussion infra at Part VIII.B.


259 See, e.g., Urban and Quilter, supra note 8, at 679-80; see also Rossi v. Motion Picture Ass’n of America, 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].”)

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

261 Cundiff, supra note 2, at 405.

262 See, e.g., http://www.archive.org/web/web.php
server. Instead, the users’ Internet Service Providers 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. Until the law becomes settled in this area, proactive preemptive measures may be the best recourse for trade secret owners.

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. Ironically, in time trade secret owners may discover that technology itself may prove the most successful way to combat technology. 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. 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 and monitoring trade secrets before they are posted on the Internet is critical. To that end, there are an assortment of


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. See Keith Winston, Consumers May Get Caught in Piracy War, Strategy to Thwart Movie Copying Could Frustrate Users, THE WALL STREET JOURNAL, 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 and Matthew Karnitschnig, Policing Web Video with ‘Fingerprints,’ THE WALL STREET JOURNAL, April 23, 2007, at B1 (reporting on policing web video with fingerprints to detect copyright infringement).

technological tools that may be used to monitor employees and maintain better control of trade secret information.269

D. International Materials

Some of the material targeted by a take-down notice may very well reside outside of the United States.270 While foreign owned material hosted on a United States server may be subject to United States laws, it is unclear, however, whether material hosted outside the United States could be covered. The extent to which trade secret misappropriation which occurs outside the United States may be redressed in United States courts is to some degree, unsettled.271 This could create practical and legal difficulties for a trade secret owner, even with a take-down provision, since alleged infringers may simply move the information to a foreign server.

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

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. OF CORPORATE AND FINANCIAL LAW 115, 125-26 (2005); Cundiff, supra note 2 at 363-64; Daniel W. Park, Trade Secrets, The First Amendment, and patent law: A Collision on the Information Superhighway, 10 STANFORD J. OF LAW, BUSINESS AND FINANCE 46, 60 (2004).

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

271 Compare, for example, Cisco Systems, Inc. v. Huawei Technologies Co. Ltd., 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 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 trade secret misappropriation claim and finding that Taiwan, not the United States, would have a greater interest “in setting the standards for the protection of intellectual property within its own border.”)


VII. CONCLUSION

For trade secret owners the goal ought to be keeping their trade secrets from leaking onto the Internet in the first instance. When, however, as presented in the hypothetical at the beginning of this Article, a trade secret is revealed on the Internet despite the owner’s best efforts, 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 in the form of injunctive relief from a Court. 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 expeditious and efficient mechanism is necessary to fill the gap until a court can intervene.

This Article has explored the possibility of legislation, similar to that provided for copyright law under the DMCA, which would offer a shield to trade secret owners while also providing a safe harbor to Internet Service Providers from trade secret misappropriation claims. From a trade secret owner’s perspective, the ability to have trade secret information removed from a website via a take-down provision is undoubtedly valuable. In addition to introducing some points for consideration regarding components of trade secret take-down legislation, I hope more generally to invite discussion and initiate deliberation of the propriety of this kind of regulation.