Draft as of March 20, 2003

Resolving Conflicts Between Trade Secrets and the First Amendment

by
Pamela Samuelson[*]

I. Introduction

Preliminary and permanent injunctions are routinely granted in trade secret cases without offending the First Amendment, and this is as it should be. In the ordinary trade secret case, the misappropriator of trade secrets is an errant licensee,[1] a faithless employee or former employee,[2] an abuser of confidences,[3] a trickster who uses deceit or other wrongful means to obtain the secrets,[4] or a knowing recipient of misappropriated information trying to free-ride on the trade secret developer's investment.[5] In such cases, injunctions merely require parties to abide by express or implicit agreements they have made, to respect the confidences under which they acquired secrets, and to refrain from wrongful acts vis-à-vis the secrets.

Trade secrecy law is not, however, categorically immune from First Amendment scrutiny, as some commentators seem to think.[6] Section II will explain why conflicts between trade secrecy law and the First Amendment have thus far been relatively rare.

---

[*] Chancellor's Professor of Law and Information Management, University of California at Berkeley. The author wishes to thank Arizona State University for the opportunity to give the Hogan & Hartson Lecture in honor of Lee Lovinger based on this article. This paper was supported by NSF Grant No. SES-9979852.

[1] See, e.g., Tracer Research Corp. v. National Environmental Services Co., 42 F.3d 1292 (9th Cir. 1994); Union Carbide Corp. v. Exxon Corp., 77 F.3d 677 (2nd Cir. 1996); Imperial Chemical Industries Limited v. National Distillers & Chemical Corp., 342 F.2d 737 (2d Cir. 1965).

[2] See, e.g., SI Handling Systems v. Heisley, 753 F.2d 1244 (3d Cir. 1985); Comprehensive Technologies Intl. v. Software Artisans, Inc., 3 F.3d 730 (4th Cir. 1993); Lear Siegler, Inc. v. Ark-Ell Springs, Inc., 569 F.2d 286 (5th Cir. 1978).

[3] See, e.g., Smith v. Snap-On Tools Corp., 833 F.2d 578 (5th Cir. 1987); Roberts v. Sears, Roebuck and Co., 573 F.2d 976 (7th Cir. 1978); Hurst v. Hughes Tool Co., 634 F.2d 895 (5th Cir. 1981).

[4] See, e.g., E.I. duPont de Nemours & Co. v. Christopher, 431 F.2d 1012 (5th Cir. 1970); University Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518 (5th Cir. 1974); Telex Corp. v. Int'l. Business Machines Corp., 510 F.2d 894 (10th Cir. 1975)

[5] See, e.g., Data General Corp. v. Grumman Systems Support Corp., 834 F.Supp. 477 (D. Mass. 1992); Metallurgical Industries, Inc. v. Fourtek, Inc., 790 F.2d 1195 (5th Cir. 1986); Mixing Equipment Co. v. Philadelphia Gear, Inc., 436 F.2d 1308 (C.A. Pa. 1971).

[6] See, e.g., Andrew Beckerman-Rodau, *Prior Restraints and Intellectual Property: The Clash Between Intellectual Property and the First Amendment from an Economic Perspective*, 12 Fordham Intell. Prop., Media, & Ent. L.J. 1 (2001). See also Richard A. Epstein, *Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalism*, 52 Stan. L. Rev. 1003 (2000); Franklin B. Goldberg, *Recent Developments*: Ford Motor Co. v. Lane, 16 Berkeley Tech. L.J. 271 (2001)(questioning decisions applying the prior restraint doctrine of the First Amendment in trade secret cases). In connection with the categorical immunity concept, it worth noting that the U.S. Supreme Court recently repudiated dicta from a D.C. Circuit Court of Appeals decision in Eldred v. Ashcroft, 123 S. Ct. 769, 790 (2003)("the D.C. Circuit spoke too broadly when it declared copyrights 'categorically immune from challenges under the First Amendment.' 239 F.3d at 375.")

Section III argues that such conflicts may become more common in the future, and will discuss at some length DVD Copy Control Association v. Bunner[7] as an example of emergent tensions between trade secrets and the First Amendment. Section IV will consider the implications for trade secrecy injunctions and other remedies of various Supreme Court decisions on prior restraints and penalties for disclosure of non-public information.[8] It concludes that trade secrecy remedies should be subject to closer First Amendment scrutiny than they generally have in the past. It proposes several principles to assist courts in grappling with First Amendment defenses in trade secrecy cases.[9]

II. Why Conflicts Between Trade Secrets and the First Amendment Have Been So Rare

Courts rarely consider the First Amendment in deciding whether to issue a preliminary or permanent injunction against disclosure of trade secrets, or to award damages for trade secret misappropriation. There are several reasons for this. First, trade secret injunctions often aim to regulate conduct, not speech,[10] such as uses of the trade secrets to make products in competition with the trade secret owner, that are beyond the scope of First Amendment scrutiny.[11] Moreover, many trade secrets are, in fact, "things," not information.[12] Firms may claim as trade secrets, for example, the molds they use to cast their products or precision tools for refining products within the factory. Injunctions to stop disclosure of "thing"-secrets typically do not implicate First Amendment free speech interests.

Second, courts considering whether to issue injunctions against disclosure of informational trade secrets are typically trying to prevent disclosure of such secrets to particular individuals or firms, such as a former employee's private disclosure of a previous firm's trade secret information to a new employer, rather than to stop disclosure

---

[7] DVD Copy Control Association v. McLaughlin, 2000 WL 48512 (Cal. Super. Ct. 2000), rev'd sub nom., DVD Copy Control Ass'n v. Bunner, 93 Cal. App.4th 648, 113 Cal. Rptr.2d 338 (2001), appeal granted, 117 Cal. Rptr.2d 167, 41 P.3d 2 (2002). For the sake of simplicity and because the reported decisions focus on Bunner as a defendant, textual references to the case, including the trial court decision, will be designated as *Bunner*.

[8] 532 U.S. 514 (2000).

[9] Other articles suggesting that trade secret injunctions pose serious First Amendment problems include: 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 and Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 Duke L.J. 147, 229-31 (1998) (discussing preliminary injunctions in trade secret cases that raise serious First Amendment concerns); Eugene Volokh, *Freedom of Speech and Information Privacy*, 52 Stan. L. Rev. 1049 (2000).

[10] Conduct such as flag burning can, of course, be First Amendment protected (e.g., when done in protest of governmental policies). See, e.g., Texas v. Johnson, 491 U.S. 397 (1989). However, the kinds of conduct typically regulated by trade secret injunctions (e.g., against use of a particular chemical in a production process) are not expressive in a First Amendment sense.

[11] See, e.g., Comprehensive Technologies Int'l, Inc. v. Software Artisans, Inc., 3 F.3d 730 (4th Cir. 1993) (trade secret claim to stop disclosure and use of trade secrets by former employees to new firm).

[12] Flags and draft cards are, of course, "things," conduct as to which can in some contexts be protected by the First Amendment, as when they are burned in protest against government policies. See, e.g., Texas v. Johnson, 491 U.S. 397 (1989)(reversing conviction for flag desecration in protest of government policies on First Amendment grounds).

of the secrets to a broader public, as First Amendment speakers would typically wish to do.[13] Trade secret misappropriators generally have the same interest as the trade secret's developer in maintenance of the secret as against the public and as against other industry participants. They simply want to reuse the other firm's secrets in their own commercial enterprises without paying appropriate license fees. Revealing the secrets to the public would be nearly as disastrous for misappropriators as for the trade secret's developer, and would, moreover, facilitate detection of the misappropriation and increase the likelihood of the trade secret developer's taking action against the misappropriator.[14]

Third, trade secrets are generally matters of private, not of public, concern.[15] The internal design of a software product, the polishing processes a firm uses to refine ball-bearings, the secret ingredient that distinguishes one firm's product from its competitors', training manuals for salespeople, plans for future products, lists of a particular firm's customers are matters in which the public usually has little or no interest. Disclosure of such private information to the public would rarely provide information pertinent to the formation of sound public policy or otherwise advance a significant public interest. If anything, a misguided First Amendment-inspired policy that favored general publication of trade secrets would likely be harmful to the public because firms might be less willing to invest in further product development, might restrict licensing opportunities, or might adopt expensive security measures, the costs of which would be born by the consuming public in higher prices, if the firms lacked confidence that courts would enjoin disclosure of misappropriated trade secrets.[16]

Fourth, trade secrecy law is grounded in unfair competition, focusing on protecting legitimate expectations of parties who have confidential or contractual relationships with one another and steering second comers away from acquiring secrets

---

[13] See, e.g., Cybertek Computer Products, Inc. v. Whitfield, 203 U.S.P.Q. 1020 (Ca. Super. Ct. 1977)(former employee enjoined from disclosure of previous employer's trade secrets to new employer); Flotec, Inc. v. Southern Research, Inc., 16 F.Supp.2d 992 (S.D.Ind. 1998); Micro Data Base Systems, Inc. v. Dharma Systems, Inc., 148 F.3d 649 (C.A.7 Ind. 1998); Mangren Research and Development Corp. v. National Chemical Co., Inc., 87 F.3d 937 (C.A.7.Ill. 1996). Injunctions to forbid former employees from disclosing trade secrets of their former employers to new ones are untroublesome from a First Amendment standpoint, particularly when evidence shows that this has already occurred to some degree. Professors Lemley and Volokh assert that the "inevitable disclosure" doctrine of trade secret law is difficult to justify on First Amendment grounds, particularly at a preliminary injunction stage. See Lemley & Volokh, supra note xx, at 232. I question this conclusion given that such cases typically involve injunctions against private disclosures, not public ones, that courts generally use this doctrine sparingly (only in cases where circumstantial evidence indicates a high degree of likelihood of misappropriation), and that successful plaintiffs typically have to subsidize former employees during the period in which the injunction operates.

[14] See, e.g., Epstein, supra note xx, at 1036 ("The usual case of industrial espionage is *not* followed by widespread publication of the information so obtained. Rather, the thief usually wishes to keep its theft private so as to avoid detection by the owner of the trade secret and to prevent the dissemination of that secret to any *other* firms in the industry….")(emphasis in the original).

[15] See Bartnicki v. Vopper, 532 U.S. 514, 533 (2000)(characterizing trade secrets as matters of private concern).

[16] See Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 485-87 (1974)(discussing the socially harmful consequences that would flow from ruling that trade secret law was preempted by federal patent law, a result resembling the consequences of a policy of not enjoining disclosure of trade secrets on First Amendment grounds).

by wrongful means.[17] Various limiting doctrines of trade secrecy law generally make resort to free speech principles unnecessary in trade secrecy cases. Consider, for example, the reverse engineering defense in Chicago Lock Co. v. Fanberg.[18] Chicago Lock alleged that the Fanbergs misappropriated its trade secret key codes when they published a compilation of key code information and offered the compilation for sale. The Fanbergs obtained much of this information by reverse engineering Chicago locks for their customers, and the rest from other locksmiths. Because the Fanbergs had obtained the key code information by reverse engineering or from other reverse engineers, and because trade secrecy law considers reverse engineering to be a fair means of acquiring trade secrets, the Ninth Circuit Court of Appeals ruled against enjoining publication of the Fanberg book. The Ninth Circuit did not invoke the First Amendment in support of this ruling, although it could obviously have done so. Its constitutional concern was that if state trade secret law did not allow reverse engineering, it "would, in effect, convert the Company's trade secret into a state-conferred monopoly akin to the absolute protection that a federal patent affords. Such an extension of California trade secrets law would certainly be preempted by the federal scheme of patent regulation."[19]

Trade secret law is also limited by rules that limit secondary liability for misappropriation. A person who has not directly engaged in acts of misappropriation (e.g., has not breached a confidence or engaged in misconduct to obtain the secret) can only be held liable if he or she knew comes into possession of the secret knowing or having reason to know of its misappropriation, and cannot be held liable at all if the misappropriated information has become public through no fault by him or her. In Religious Technology Center, Inc. v. Lerma,[20] for example, the Washington Post and Lerma were charged with copyright infringement and trade secret misappropriation as to certain texts that the Church of Scientology used in its religious practices. The case against the Washington Post was based on the Post's duplication of documents containing the alleged trade secrets and publication of portions of the RTC texts in its newspaper. The Washington Post knew that RTC claimed the documents as trade secrets. Yet, the documents were available in unsealed court records in a California courthouse, and had also been posted on the Internet for ten days.[21] RTC tried to preserve the trade secret status of these documents by sending agents to the courthouse to block outsiders from getting access to the documents. However, the Post was able to obtain a copy of the documents from a court clerk. "Although the Post was on notice that the RTC had made certain proprietary claims about these documents, there was nothing illegal," said the court, "about The Post going to the Clerk's Office for a copy of the documents or downloading them from the Internet."[22]

---

[17] See, e.g., Lemley & Volokh, supra note xx, at 230 (restricting disclosure of a trade secret may be consistent with the First Amendment because of contractual relationships).
[18] 676 F.2d 400 (9th Cir. 1981).
[19] Id. at 404.
[20] 908 F. Supp. 1362 (E.D. Va. 1995).
[21] Id. at 1368.
[22] Id. at 1369. See also Cabot Corp. v. Thai Tantalum, Inc., 25 U.S.P.Q.2d (BNA) 1619 (Del. Ch. 1992)(denying preliminary injunction where the plaintiff sought to impute knowledge of misappropriation to non-misappropriating defendant based upon its knowledge of a lawsuit initiated against alleged misappropriator).

Because the information had been available in open court records and posted on the Internet, the court ruled that it was no longer a trade secret, saying: "Once a trade secret is posted on the Internet, it is effectively part of the public domain, impossible to retrieve. Although the person who originally posted a trade secret on the Internet may be liable for trade secret misappropriation, the party who merely downloads Internet information cannot be liable for misappropriation because there is no misconduct involved in interacting with the Internet."[23] Although the court in *Lerma* did not expressly invoke the First Amendment in support of its ruling, its application of limiting principles of trade secrecy law was consistent with the First Amendment interests of the Washington Post, its reporters, and readers eager to know about Scientology practices.

First Amendment/free speech defenses are unusual in trade secret cases, although they are not unknown.[24] On occasion, they have even been successful.[25] For example, CBS was charged with trade secret misappropriation, among other misdeeds, and preliminarily enjoined by a state court from broadcasting as part of a news program videotape footage of meat-packing factory operations which was said to reveal "confidential and proprietary practices and processes."[26] Supreme Court Justice Blackmun stayed the injunction as an unconstitutional prior restraint on speech, allowing CBS to go forward with the broadcast.[27]

On similar grounds, the Oregon Supreme Court overturned a preliminary injunction Adidas had persuaded a lower court to issue to prevent Sports Management News (SMN) from publishing reports about a new shoe design which Adidas claimed as a trade secret.[28] The Oregon court accepted that the design was an Adidas trade secret and that Adidas had only made this information available to select employees who were bound by confidentiality agreements not to reveal such information. Yet the court characterized as a "classic prior restraint" a lower court order that SMN refrain from publishing any

---

[23] *Lerma*, 908 F. Supp. at 1368. See also Religious Technology Center v. F.A.C.T.NET, 901 F. Supp. 1519, 1526 (D. Colo. 1995)(rejecting similar trade secret misappropriation claims against a website critical of the Church of Scientology because information from these texts had already been "made available on the Internet through persons other than Lerma, with the potential for downloading by countless users"); Religious Technology Center v. Netcom On-line Comm. Services, Inc., 923 F. Supp. 1231, 1256 (N.D. Cal. 1995)("Although Ehrlich cannot rely on his own improper postings to support the argument that the Church's documents are no longer secrets…, evidence that another has put the alleged trade secrets in the public domain prevents RTC from further enforcing its trade secret rights in those materials.").

[24] See, e.g., ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS, [Sec.] 12.06 (2002). (First Amendment defenses rare).

[25] See also Proctor & Gamble Co. v. Bankers Trust Co., 78 F.3d 219 (6th Cir. 1996)(injunction against disclosure by magazine of information leaked to it in violation of discovery order violated the First Amendment). But see Garth v. Staktek Corp., 876 S.W.2d 545 (Tex. App. 1994)(upholding constitutionality of preliminary injunction in trade secret case).

[26] CBS, Inc. v. Davis, 510 U.S. 1315 (1994).

[27] Id.

[28] Oregon ex rel. Sports Management News v. Nachtigal, 324 Ore. 80, 921 P.2d 1304 (1996). The Oregon Supreme Court overturned the lower court's order based on its interpreted the free speech clause of the Oregon Constitution; it did not consider whether it would have reached the same result under the First Amendment to the U.S. Constitution. Id., 921 P.2d at 1307-08.

information derived from Adidas proprietary information and that SMN submit to the court for its approval any reports about Adidas products before publishing them.[29]

Similarly, Ford Motor Co. lost a motion for a preliminary injunction on First Amendment grounds against Internet postings about unreleased new automobile designs that Ford claimed as trade secrets.[30] Ford claimed that Lane knew or should have known that employees who leaked the information had misappropriated it, and hence that Lane was secondarily liable for the misappropriation.[31] The trial court was persuaded that because Lane did not have a confidential relationship with Ford and did not himself misappropriate the information, "Ford's commercial interest in its trade secret and Lane's alleged improper conduct in obtaining the trade secrets are not grounds for issuing a prior restraint."[32]

III. Why Conflicts Between Trade Secrets and the First Amendment May Become More Common

A. Factors Contributing to Greater Potential For Clashes

Clashes between the First Amendment and trade secret law may become more common in the future, particularly as to issuance of preliminary injunctions, for several reasons. For one thing, the proportion of informational trade secrets, as compared with "thing" secrets, has grown as the economy has become increasingly information-based.[33] Second, the past few decades has brought a heightened awareness of the benefits of vigorous protection of intellectual property assets which seems to have induced firms to claim a broader range of non-public information as trade secrets.[34] Third, trade secrecy law, like other forms of intellectual property law, has been getting stronger over time. Some years ago, trade secret law was considered a relatively weak form of protection

---

[29] Id. at 1308.

[30] Ford Motor Co. v. Lane, 67 F. Supp.2d 745 (E.D. Mich. 1999). This decision is criticized in Goldberg, supra note xx, at 271, and Epstein, supra note xx, at 1035-46. Both Goldberg and Epstein regard Lane as a non-media defendant whose First Amendment claim was undermined by the vindictive nature of Lane's posting of the Ford designs after a dispute between Ford and Lane over Lane's domain name. Goldberg, supra note xx, at xx; Epstein, supra note xx, at xx. While it does appear that Lane was angry at Ford over the domain name dispute, it is also true that Lane had been operating a website about Ford designs for a long time, and there was no evidence that Lane was inducing Ford employees to breach contracts or confidences with Ford or that Lane participated in any misappropriation of Ford secrets.

[31] Id. at 748. The same was apparently true in *Sports Management News*, although the Oregon Supreme Court did not expressly say so.

[32] Id. at 753. A similar theory underlies the trade secret claim in DVD Copy Control Association v. Bunner which will be discussed at length in the next section

[33] See, e.g., J.H. Reichman & Jonathan A. Franklin, *Privately Legislated Intellectual Property Rights,: Reconciling Freedom of Contract with Public Good Uses of Information*, 107 U. Penn. L. Rev. 875, 884-88 (1999). See also Rochelle Cooper Dreyfuss, *A* Wiseguy's *Approach to Information Products: Muscling Copyright and Patent Into a Unitary Theory of Intellectual Property*, 1992 Sup. Ct. Rev. 195 (1993); J.H. Reichman, *Computer Programs as Applied Scientific Know-How: Implications of Copyright Protection for Commercialized University Research*, 42 Vand. L. Rev. 639, 660 (1989).

[34] See, e.g., Robert P. Merges, *One Hundred Years of Solicitude: 1900-2000*, 88 Calif. L. Rev. 2187, 2233-40 (2000) (discussing expansions in intellectual property protection in recent decades).

against certain forms of unfair competition,[35] and courts were hostile to the notion that trade secret developers have "property" rights in their secrets.[36] Today, trade secrecy law is widely perceived of as a strong form of legal protection,[37] and courts have become more receptive to conceiving of trade secrets as "property."[38] The trend toward more expansive intellectual property protection may encourage trade secret developers, among others, to make bolder claims than in past decades.[39] Together, these developments contribute to an enhanced potential for conflicts between trade secrecy and free speech interests.

More significant, though, is the increasing use of mass market licenses to protect information secrets in ways that trade secrecy law would not do. For example, mass market software licenses often contain terms forbidding reverse engineering,[40] even though trade secret law would permit this. Other mass market license provisions forbid criticism of the product or disclosure of flaws which directly implicate free speech interests and aim to keep secret matters in which the public may have an interest.[41] Firms sometimes also use access controls and click-through licenses to claim publicly available information as trade secrets.[42] These efforts to plug "leaks" that trade secret law has long permitted have broad social implications that proponents of mass market licenses prefer to ignore.[43] Those who object to the "privacation" of information—that is, the use of mass-market licenses and/or access controls to claim as trade secrets information that would otherwise be public—will be inclined to make the information public to protest the privacation effort. This substantially enhances the potential for conflicts between trade secret and First Amendment interests.

---

[35] See, e.g., Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974).

[36] See, e.g., RESTATEMENT OF TORTS Sec. 757, comments a, b, c (1939). A more Restatement points out that "[t]he owner of a trade secret does not have an exclusive right to possession or use of the secret information. Protection is available only against a wrongful acquisition, use or disclosure of the trade secret," AMERICAN LAW INSTITUTE, RESTATEMENT OF THE LAW OF UNFAIR COMPETITION, comment a to Sec. 43 at 493 (1993), as when the use or disclosure breaches an implicit or explicit agreement between the parties or when improper means, such as trespass or deceit, are used to obtain the secret. AMERICAN LAW INSTITUTE, RESTATEMENT OF TORTS, sec. 757 (1939). See also Uniform Trade Secrets Act, sec. 1.

[37] See, e.g., Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 Calif. L. Rev. 241, 243 (1998).

[38] See, e.g., Ruckelshaus v. Monsanto Co., 467 U.S. 986 (1984) (holding trade secrets to be property for purposes of takings law); Beckerman-Rodau, supra note xx, at 20-23.

[39] See, e.g., IBP, Inc. v. Klumpe, 2001 WL 1456173 (Tex.App. 2001); Group One, Ltd. v. Hallmark Cards, Inc., 254 F.3d 1041 (Mo. 2001); DTM Research, L.L.C. v. AT & T Corp., 245 F.3d 327 (Md. 2001); Phillip Morris Inc. v. Reilly, 113 F.Supp.2d 129 (D.Mass. 2000).

[40] See, e.g., Mark A. Lemley, *Beyond Preemption: The Law and Policy of Intellectual Property Licensing*, 87 Calif. L. Rev. 111, 129 (1999); Dennis S. Karjala, *Federal Preemption of Shrinkwrap and Online Licenses*, 22 U. Dayton L. Rev. 511, 520 n. 28 (1997).

[41] See, e.g., State of New York v. Network Associates, Inc., Civil No. 400590/02 (N.Y. Supreme Court, Jan. 6, 2003) (on file with author).

[42] See, e.g., Julie E. Cohen, *Call It the Digital Millennium Censorship Act: Unfair Use*, New Republic Online (May 23, 2000), available at http://www.tnr.com/online/cohen052300.html (discussing Microsoft's efforts to keep Kerberos specification as a trade secret through access controls and license terms, even though the specification was published on a publicly accessible website)

[43] See, e.g., Rochelle Cooper Dreyfuss, *Do You Want to Know a Trade Secret? How Article 2B Will Make Licensing Trade Secrets Easier (But Innovation Harder)*, 87 Calif. L. Rev. 191, 241 (1998).

The medium that most readily facilitates the objectives of privaction-objectors is the Internet. In the past, a misappropriator who wanted to make trade secrets public would have had to persuade a traditional publisher to make the secrets public. This would have been quite difficult if the secrets were not really matters of public concern warranting publication or if the publisher decided it was too risky to publish the secrets because of potential liability for trade secret misappropriation. With the advent of the Internet, virtually anyone can become a publisher, and anything published on the Internet potentially has a global audience of many millions of people.[44] Misappropriators no longer need to convince traditional publishers to make trade secrets publicly available. They can do it themselves by posting the secrets on the Internet. The risk of destruction of trade secrets from Internet posting has induced some courts and commentators to adopt stronger trade secret rules.[45]

B. *DVD Copy Control Association v. Bunner*

A case that illustrates many of these trends is DVD Copy Control Association v. Bunner.[46] DVD Copy Control Association (DVD CCA) claims trade secret rights in the Content Scramble System (CSS), an encryption program, used to protect DVD movies. DVD CCA has leverage to impose stringent licensing terms on makers of DVD players because it controls key patents covering components of DVD players.[47] Among the license terms routinely imposed by DVD CCA are requirements that licensees install CSS in their systems, undertake various security measures to ensure that CSS remains secret, and include in end-user licenses provisions that forbid end-users from reverse engineering CSS.[48]

Notwithstanding these efforts to keep CSS secret, a teenager named Jon Johansen was alleged to have reverse engineered CSS in Norway.[49] Based upon what he learned in the course of this reverse engineering, Johansen wrote a program, DeCSS, that bypasses CSS. Johansen posted DeCSS in source and object code form on the Internet. In late October 1999, this program was the subject of intense discussion at various Internet sites,

---

[44] See, e.g., Reno v. American Civil Liberties Ass'n, 521 U.S. 844 (1997) (emphasizing the significance of the Internet in facilitating speech from a wide array of sources).

[45] See, e.g., Universal City Studios, Inc. v. Corley, 273 F.3d 429, 454 (2d Cir. 2001)(dangers of Internet as reason for lesser First Amendment protection for posting information on the Internet). See also Goldberg, supra note xx, at 292; Bruce T. Adkins, *Trading Secrets In the Information Age: Can Trade Secret Law Survive the Internet?*, 1996 U. Ill. L. Rev. 1151 (proposing stronger trade secret rules to protect secrets against Internet publication).

[46] DVD Copy Control Ass'n v. Bunner, 93 Cal. App.4th 648, 113 Cal. Rptr.2d 338 (2001), appeal granted, 117 Cal. Rptr.2d 167 (2002).

[47] *Bunner*, 113 Cal. Rptr.2d at 344.

[48] DVD Copy Control Ass'n v. McLaughlin,Complaint for Injunctive Relief for Misappropriation of Trade Secrets, Case No. CV 786804 (Super. Ct. Ca., December 28, 1999) (cited hereafter as "DVD CCA Complaint"), para. 34-39.

[49] DVD Copy Control Ass'n v. McLaughlin, 2000 WL 48512 at 2 (Super. Ct. Ca. 2000). An opinion written to explain the acquittal of Jon Johansen for various violations of Norwegian law indicates that Johansen was not the person who actually reverse engineered CSS. See Sunde v. Johansen, Oslo Court of First Instance, Jan. 2003 (Jon Bing translation 1/03) at 5 (Johansen got CSS information from a person using the name "nomad").

including slashdot.org.[50] Numerous participants in the slashdot.org discussion about DeCSS, including Andrew Bunner, decided to post this program on their websites as part of a widespread protest against the motion picture industry's efforts to prevent dissemination of this program.[51] Others linked to sites where DeCSS was posted.[52]

After Bunner and other posters of and linkers to DeCSS ignored cease and desist letters, DVD CCA initiated a lawsuit in California state court charging Bunner, twenty other named individuals, and five hundred John Doe defendants, with trade secrecy misappropriation on the ground that Bunner and the other defendants knew or should have known that DeCSS embodied or was substantially derived from stolen trade secrets.[53] DVD CCA claimed that Johansen had stolen CSS trade secrets by reverse engineering CSS in violation of a click-through license.[54] DVD CCA persuaded the trial court to issue a preliminary injunction to restrain the defendants from posting or otherwise disclosing the DeCSS program, the master keys or algorithms of CSS, and any other information derived from DVD CCA's proprietary information.[55]

Viewed through the lens of traditional trade secrecy law, DVD CCA's claims seem remarkably weak. Reverse engineering a mass-marketed product has long been recognized as a legitimate way to acquire a trade secret.[56] Trade secret experts believe that it is almost inevitable that trade secrets will be reverse engineered.[57] The reverse engineering privilege of state trade secrecy law is an important factor in the Supreme Court's decision that trade secrecy law does not conflict with patent law because trade secrecy law is so much weaker than patent law.[58]

DVD CCA is trying to use mass market licenses to override the reverse engineering privilege of trade secrecy law and to be asserting that it can, in effect, bind the whole world not to reverse engineer globally distributed mass-marketed products it does not even manufacture through multiple layers of license requirements reaching down to the end-user. This is, at the very least, a very aggressive stretching of trade secrecy law. To rule as DVD CCA wishes "would, in effect, convert the [plaintiff's] trade secret into a state-conferred monopoly akin to the absolute protection that a federal patent affords."[59] In *Chicago Lock*, the Ninth Circuit Court of Appeals opined that "[s]uch an extension of California trade secrets law would certainly be preempted by the federal scheme of patent

---

[50] See, e.g., *Bunner*, 113 Cal. Rptr.2d at 343.
[51] See, e.g., DVD CCA Complaint, supra note xx, para. 50 (discussing protests).
[52] Id., 27 (defendants were charged with linking as well as posting of DeCSS).
[53] Id. , para. 5-29 (naming defendants).
[54] *McLaughlin*, 2000 WL 48512 at 2 (Sup. Ct. Ca. 2000).
[55] Id. at 3.
[56] See, e.g., Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 Yale L. J. 1575, 1582 (2002).
[57] See, JAMES H. A. POOLEY, TRADE SECRET LAW sec. 5.02[5] (1999).
[58] "Trade secret law provides far weaker protection in many respects than patent law. While trade secret law does not forbid the discovery of the trade secret by fair and honest means, e.g., independent creation or reverse engineering, patent law operates 'against the world,' forbidding any use of the invention for whatever purpose for a significant length of time….Where patent law acts as a barrier, trade secret law functions relatively as a sieve." *Kewanee*, 416 U.S. at 489-90.
[59] *Chicago Lock*, 676 F.2d at 404.

regulation."[60] At least one federal appellate court has ruled that anti-reverse engineering clauses in mass-market software licenses should not be enforceable because they conflict with federal intellectual property policy.[61] Moreover, most commentators oppose enforcement of anti-reverse engineering clauses in mass-market licenses.[62]

Also contributing to *Bunner* as a doubtful trade secrecy case is the question as to whether Johansen's actions should be deemed illegal under California law, given that he is a resident of Norway.[63] It is worth noting that DVD CCA has not brought a similar lawsuit against Johansen in Norway, and Johansen was recently acquitted of any wrongdoing in connection with reverse engineering of CSS in a Norwegian court. [64] Consider also that Johansen might have reverse engineered his father's or a friend's DVD player without clicking his personal agreement to be bound by a license with an anti-reverse engineering clause. It is also possible that one of DVD CCA's licensees failed to abide by its license obligations by failing to install CSS securely or install a license on the system Johansen used.[65] DVD CCA was, moreover, unclear about whether DeCSS embodied CSS secrets or was merely derived from what Johansen learned in the course of reverse engineering.[66] It is more difficult to justify enjoining disclosure of information derived from proprietary information than disclosure of trade secret information.

In any event, DVD CCA did not seek in the California lawsuit to enjoin Johansen from posting DeCSS on the Internet. Rather, DVD CCA sued Bunner and 520 other defendants. As is evident from DVD CCA's complaint, hundreds of persons from at least eleven different countries had posted or linked to hundreds of copies of DeCSS on the Internet.[67] No defendant in the *Bunner* case was alleged to have directly misappropriated CSS secrets. DVD CCA's theory was that all 521 Internet posters of DeCSS were liable for trade secrecy misappropriation under California law because they knew or should have known that CSS embodied or was derived from stolen trade secrets.[68] Given that DeCSS was available hundreds of Internet sites for at least two months before DVD CCA filed its lawsuit and three months before the preliminary injunction hearing (and for that matter, continues to be available on hundreds of Internet sites), one might have expected a judge to respond to the lawsuit by saying that whatever secrets about CSS one could

---

[60] Id.
[61] See, e.g., Vault Corp. v. Quaid Software Ltd., 847 F.2d 255 (5th Cir. 1988) (refusing to enforce anti-reverse engineering clause of shrinkwrap license under state law because it conflicted with federal copyright policy). But see Bowers v. Bay State Technologies, Inc., 302 F.3d 1332 (Fed. Cir. 2002) (enforcing an anti-reverse engineering clause of a shrinkwrap license).
[62] See, e.g., Samuelson & Scotchmer, supra note xx, at 1626-30 (recommending against enforcement of such license terms in software contracts and citing concurring commentators).
[63] See, e.g., Pavlovich v. Superior Court, 127 Cal. Rptr.2d 329, 339-43 (Sup. Ct. 2002) (ordering dismissal of trade secret claim against non-resident of California whose conduct directed at California consisted only of posting DeCSS on the Internet).
[64] An appellate court in Norway has, however, decided to hear the prosecutor's appeal of this acquittal. See Alleged Teenage Pirate Faces New Trial, CNET News, Feb. 28, 2003, available at http://news.com.com/2100-1025-990583.html.
[65] *Bunner*, 113 Cal. Rptr.2d at 344.
[66] *McLaughlin* at 1 (DVD CCA alleged that DeCSS embodies, uses, or is a substantial derivation of CSS).
[67] DVD CCA Complaint, supra note xx, para. 5-30, 48.
[68] Id., para. 49-50.

learn from DeCSS had already leaked out and this genie could not be put back in the bottle. *RTC v. Lerma* and other cases suggest that trade secrets are irretrievably lost when a non-misappropriating party republishes them on the Internet.[69]

So what explains Judge Elving's decision to issue a preliminary injunction? He was persuaded by the circumstantial evidence of DVD CCA's licensing practices that Johansen must have reverse engineered CSS in violation of a click-through agreement. From this, he concluded on a kind of "fruit of the poisonous tree" rationale that DeCSS must embody or be substantially derived from stolen trade secrets. The circumstantial evidence that Elving found "quite compelling" in holding Bunner and other defendants liable as fellow misappropriators of CSS secrets was "various defendants' inclination to boast about their disrespect for the law."[70] Elving was also impressed with the "considerable time, effort, and money [spent] in creating the intellectual property at issue in order to protect the copyrighted information contained on DVDs."[71] The judge did not seem to realize how novel was DVD CCA's theory that information about CSS should be protected as trade secrets in order to protect non-trade secret interests of non-parties to the lawsuit, that is, the interests of the motion picture industry in protecting copyrighted movies from unauthorized copying.[72]

Dangers of the Internet as a medium entered into Judge Elving's assessment as well. Without an injunction, the judge recognized that CSS secrets would be lost "given the current power of the Internet to disseminate information and the defendants' stated determination to do so."[73] To allow these trade secrets to be destroyed by posting them on the Internet would, in his view, encourage wrongdoers to post the fruits of their wrongdoing on the Internet and thereby escape liability.[74] Judge Elving characterized as "truly minimal" the harm to Bunner and others in being enjoined from posting DeCSS on the Internet.[75]

C. How Bunner's First Amendment Defense Fared in the Courts

Judge Elving thought so little of Bunner's First Amendment defense that he did not even mention that such a defense had been raised. He did, however, indicate that Bunner et al. were free to continue to discuss or criticize DVD CCA, the motion picture industry, or DeCSS on their websites "so long as [CSS] proprietary information…is not disclosed or distributed."[76] This failure to mention the First Amendment defense is

---

[69] See supra notes xx and accompanying text.
[70] *McLaughlin*, 2000 WL 48512 at 2.
[71] Id. at 2-3.
[72] See, e.g., Pamela Samuelson, *Reverse Engineering Under Siege*, 45 Comm. ACM 15 (Nov. 2002); Brief Amici Curiae of Intellectual Property Professors, Computer & Communications Industry Association, and U.S. Public Policy Committee of the Association for Computing Machinery submitted to the California Supreme Court in DVD Copy Control Ass'n v. Bunner July 10, 2002, available at http://www.law.berkeley.edu/cenpro/samuelson/news/index.html (explaining weaknesses of trade secrecy theory).
[73] *McLaughlin*, 2000 WL 48512 at 3.
[74] Id. at 3.
[75] Id. at 2.
[76] Id. at 3.

consistent with the view that injunctions in trade secrecy cases are categorically immune from First Amendment scrutiny, although Judge Elving did not endorse this view.[77]

The Court of Appeal, by contrast, was so taken with Bunner's First Amendment defense that it neglected to consider more conventional weaknesses in DVD CCA's trade secret claim.[78] It seems to have assumed that trial court was correct in concluding that DVD CCA had established a reasonable probability of success on the merits of the trade secrecy claim,[79] and went on to consider Bunner's First Amendment defense, concluding that the injunction did not meet First Amendment standards.[80]

Given its interest in the First Amendment issues presented in *Bunner*, one might have expected the Court of Appeal to take issue with Judge Elving's conclusion that wrongful knowledge, and hence, liability, of all 521 defendants for trade secrecy misappropriation was established based on boastful expressions of disrespect for the law by a few defendants.[81] After all, the First Amendment surely protects boastful statements and expressions of disrespect for the law,[82] and it would seem to be at odds with First Amendment principles for the statements of a few defendants to be the basis of liability of all 521 of them.[83] The Court of Appeal, however, obliquely mentioned the disrespect issue in a footnote indicating that "[t]here was no evidence that Bunner himself had ever contributed to any of these writings indicating disrespect for the law."[84]

The primary First Amendment issue that captured the Court of Appeals' attention was Bunner's claim that the DeCSS program itself was First Amendment-protected expression that he and others had a First Amendment right to republish.[85] It mattered a great deal to the Court of Appeal that Bunner had posted DeCSS in source code form,[86] which the court characterized as "a writing…which describes an alternative method of decrypting CSS-encrypted DVDs. Regardless of who authored the program, DeCSS is a written expression of the author's ideas and information about decryption of DVDs without CSS."[87] The Court of Appeal relied on federal court decisions holding, first, that computer program source code is First Amendment-protected expression, and second, that the prepublication licensing regime established by federal export control laws to

---

[77] See supra note xx and accompanying text.
[78] See sources cited supra note xx.
[79] *Bunner*, 113 Cal. Rptr. at 347.
[80] Id. at 347-52.
[81] See supra note xx and accompanying text.
[82] See, e.g., Street v. New York, 394 U.S. 576 (1969)(overturning conviction for casting contempt on any flag of the United States based on disrespectful statements).
[83] TBA
[84] *Bunner*, 113 Cal. Rptr. at 344, n. 5.
[85] Id. at 347-50.
[86] Id. at 348. At least one of the defendants in *Bunner*, namely, Emmanuel Goldstein, posted object code versions of DeCSS on his website. See DVD CCA Complaint, supra note xx, para. 11 (naming Emmanuel Goldstein as a defendant); Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001)(holding Corley, a/k/a Emmanuel Goldstein, liable for violating the DMCA anti-circumvention rules for posting object code forms of DeCSS on the 2600 website).
[87] *Bunner*, 113 Cal. Rptr. at 348.

forbid unlicensed distribution of encryption programs was an unconstitutional prior restraint, at least insofar as it concerned source code.[88]

Continuing in this vein, the Court of Appeal opined that Judge Elving's issuance of a preliminary injunction to stop publication of DeCSS source code was a regulation of "pure speech"[89] and a classic prior restraint that "'bears a heavy presumption against its constitutional validity.'"[90] The Court of Appeal went on to say that "DVD CCA's statutory right to protect its economically valuable trade secret is not an interest that is 'more fundamental' than the First Amendment right of free speech or even on an equal footing with the national security interests and other vital interests that have previously been found insufficient to justify a prior restraint."[91]

DVD CCA sought to support the lower court's preliminary injunction by relying upon decisions upholding preliminary injunctions in copyright cases.[92] The Court of Appeal rejected the copyright preliminary injunction analogy: "Both the First Amendment and the Copyright Act are rooted in the U.S. Constitution, but the UTSA lacks any constitutional basis. The prohibition on disclosure of a trade secret is of infinite duration, while the copyright protection is strictly limited in time, and there is no 'fair use' exception [in trade secrecy law] as there is for copyrighted material."[93] Commendable as was the effort to distinguish trade secrecy injunctions from copyright injunctions, the Court of Appeal's reasoning is not persuasive.

D. Critique of the First Amendment Analysis in *Bunner*

1. The Trial Court Should Have Considered Bunner's First Amendment Defense.

Judge Elving should have considered Bunner's First Amendment defense. Even if a judge believes that a First Amendment defense in a trade secrecy case should not prevail, it is appropriate to explain why enjoining disclosure of an informational secret is consistent with the First Amendment. This is especially appropriate when the information is the subject of a public controversy and the person who wishes to disclose it was not responsible him- or herself for the initial alleged misappropriation of it.

---

[88] See Junger v. Daley, 209 F.3d 481 (6th Cir. 2000). See also Bernstein v. United States, 922 F. Supp. 1426 (N.D. Cal. 1996), aff'd, Bernstein v. United States, 176 F.3d 1132 (9th Cir. 1999), rehearing granted and opinion withdrawn, 192 F.3d 1308 (9th Cir. 1999).

[89] *Bunner*, 113 Cal. Rptr. at 348. The Court of Appeal relied in part on the Supreme Court's recent decision in Bartnicki v. Vopper, 532 U.S. 514 (2000) for the proposition that a naked prohibition of disclosure of information is a regulation of "pure speech" which has substantial First Amendment implications. Bunner, 113 Cal. Rptr. at 347. However, the Court of Appeal distinguished *Bartnicki* on several grounds: because it did not involve a trade secrecy claim, because the Court in *Bartnicki* had expressly declined to consider whether the same result would be appropriate in trade secret cases, and *Bartnicki* was not a prior restraint case. Id., n. 7.

[90] Id. at 345, quoting Wilson v. Superior Court, 13 Cal.3d 652, 657, 119 Cal. Rptr. 468 (1975).

[91] *Bunner*, 113 Cal. Rptr. at 351.

[92] Id. at 349. See, e.g., Lemley & Volokh, supra note xx, at 158-63 (discussing frequency of preliminary injunctions in copyright cases).

[93] *Bunner*, 113 Cal. Rptr. at 350.

2. First Amendment Defenses in Trade Secret Cases Should Not Be Rebuffed on the Ground that Trade Secrets Are Property.

One commentator, Andrew Beckerman-Rodau, believes that Judge Elving was correct in rejecting the First Amendment defense in *Bunner*.[94] He bases this conclusion on two related propositions: first, that trade secrets are property rights, and second, that the First Amendment does not trump property rights.[95] This commentator relies on certain real property cases holding that trespass was not justifiable merely because the defendants were engaged in speech or protest activities,[96] as well as some copyright and trademark decisions that concluded that there is no First Amendment right to "trammel on" intellectual property rights.[97]

Trade secrets certainly have a lesser claim to being classified as "property" rights than copyrights or patents because the Constitution empowers Congress to grant exclusive rights to authors and inventors, not to developers of trade secrets.[98] Trade secrets are, in contrast, protected against certain unfair competitive acts, such as use of wrongful means to acquire the secrets or breach of a confidential relationship.[99] Developers of trade secrets have no "exclusive rights" in them, but only protection for as long as the secrets do not become known through reverse engineering, independent discovery, or other leakages.[100] While the Supreme Court has ruled that trade secrets may be treated as "property" for some purposes, such as considering whether legislation allowing the government to disclose trade secrets constitutes a "taking" of private property,[101] the more historically accurate and appropriate framework for understanding trade secrecy law is as a species of unfair competition law.[102] This undermines the main premise on which Beckerman-Rodau relies for asserting that trade secret injunctions are immune from First Amendment review.

However, even if were it appropriate to characterize trade secrets as "property," this does not mean that the First Amendment has no role to play.[103] First Amendment

---

[94] See Beckerman-Rodau, supra note xx, at 20-23

[95] Id. See also Epstein, supra note xx, at 1037 (arguing against First Amendment defenses in trade secrecy cases because trade secrets are property).

[96] Beckerman-Rodau, supra note xx, at 64-65.

[97] Id. at 21, relying on Dallas Cowboy Cheerleaders, Inc. v. Pussycat Cinema, Ltd., 604 F.3d 200 (2d Cir. 1979). Professor Jed Rubenfeld has pointed out that the word "trammel" is inappropriate; surely the author of this widely cited opinion must have meant "trample on." Jed Rubenfeld,, *The Freedom of Imagination: Copyright's Constitutionality*, 112 Yale L.J. 1, 24 (2002).

[98] U.S. Constitution, Art. I, sec. 8, cl. 8.

[99] See RESTATEMENT OF UNFAIR COMPETITION, supra note xx, secs. 41, 43.

[100] See, e.g., *Kewanee*, 416 U.S. at 476.

[101] Ruckelshaus v. Monsanto Co., 467 U.S. 986 (1984). But see Pamela Samuelson, *Information As Property: Do* Ruckelshaus *and* Carpenter *Signal a Changing Direction in the Law?*, 38 Cath. U. L. Rev. 365 (1989) (criticizing the Court's analysis in *Ruckelshaus*).

[102] RESTATEMENT OF UNFAIR COMPETITION, supra note xx, sec. 38.

[103] See, e.g., Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop Other People From Speaking About You*, 52 Stan. L. Rev. 1049, 1063 (2000) ("Calling a speech restriction a 'property right'…doesn't make it any less a speech restriction, and it doesn't make it constitutionally permissible.") Volokh points out that characterizing Sullivan's interest in his reputation as

defenses have been successful in a number of intellectual property cases.[104] The First Amendment has an important role to play when the question is not *where* certain speech activities can take place (e.g., on the plaintiff's real property), but rather whether certain information can be disclosed to the public.[105] Several scholars have concluded that courts have been too quick to grant preliminary injunctions in both copyright and trade secret cases and insufficiently sensitive to free speech considerations, in large part because they have relied too heavily on the weak crutch of the property rights metaphor.[106]

3. Bunner's First Amendment Defense Was Based on More Than an Assertion of a First Amendment-based Right to Post Code as a Speech Act.

The Court of Appeal upheld Bunner's First Amendment defense because it agreed that DeCSS is First Amendment protected "speech" which Bunner had a right to republish. The appellate court characterized source code as the expression of an author in support of its conclusion that source code is speech.[107] This expresses a copyright-like perception of what constitutes First Amendment-protected speech.[108] There is, of course, substantial overlap between subject matters that copyright and the First Amendment deem to be protectable "expression," including news articles, books, photographs, and motion pictures. However, the overlap is not complete. There are some things—such as oral statements—that are First Amendment protected expression, but not protectable by copyright law,[109] and other things that copyright protects as expression—such as obscene movies—that do not qualify for First Amendment protection.[110]

The more appropriate way to analyze whether source code is First Amendment protected speech in the context of a case such as Bunner is to consider whether it is communicating ideas to others and contributing to a public debate. As Professor Post has observed:

---

a property interest wouldn't strengthen his libel claim against the New York Times, nor would characterizing the American flag as intellectual property of the U.S. change the First Amendment implications of flagburning. Id. at 1063-64.

[104] See, e.g., L.L. Bean, Inc. v. Drake Pub., Inc., 811 F.2d 26, 29 (1st Cir.), cert. denied, 483 U.S. 1013 (1987); Stop the Olympic Prison v. United States Olympic Committee, 489 F. Supp. 1112 (S.D.N.Y. 1980)(allowing use of Olympic symbol in protest against building a prison on a former Olympic site); Parks v. LaFace Records, 76 F.Supp.2d 775 (1999)(successful First Amendment defense in right of publicity case against songwriter who named a song for civil rights activist); Hicks v. Casablanca Records, 464 F. Supp. 426 (S.D.N.Y. 1978)(denying right of publicity claim brought by heirs of Agatha Christie against maker of film about an episode in her life based in part on First Amendment considerations).

[105] See also supra notes xx and accompanying text for cases specifically concerned with disclosure of trade secrets and other confidential information.

[106] Lemley & Volokh, supra note xx, at 182-84; Rubenfeld, supra note xx at 25.

[107] *Bunner*, 113 Cal. Rptr. at 348.

[108] See, e.g., Dan L. Burk, *Patenting Speech*, 79 Tex. L. Rev. 100, 107-09 (2000)(discussing the conception of software-as-speech and explaining differences between what constitutes protectable expression in the contexts of intellectual property law and the First Amendment).

[109] Oral statements do not satisfy the "fixation" requirement of U.S. copyright law. See 17 U.S.C. sec. 102(a) (requiring that original works of authorship be "fixed in a tangible medium of expression").

[110] See, e.g., Mitchell Bros. Film Group v. Cinema Adult Theatre, 604 F.2d 852 (5th Cir. 1979)(rejecting claim that obscene movies are uncopyrightable because they do not "promote the progress of Science").

> Publishing software in print is covered by the First Amendment because it forms part of public discourse and debate. We know that this same discourse and debate can occur over the Internet and in electronic form. So long as the publication of source code forms part of this public discourse and debate, it will be covered by the First Amendment, whether it is set forth in a printed article or in an online discussion.[111]

It is thus necessary to consider the social context within which source code exists. Some source code, such as the Snuffle program at issue in Bernstein v. United States, clearly qualifies as First Amendment protected "speech" because of its contribution to the communication of ideas within the cryptographic research community,[112] while other source code may not.[113]

Several factors support the view that DeCSS in source code form communicated ideas and contributed to public discourse. The very fact that Jon Johansen reverse engineered CSS, developed DeCSS, and posted the program on the Internet were matters of public interest and concern, as witnessed by news coverage about these developments.[114] Also matters of public debate were the efforts of the motion picture industry and DVD CCA to stop Internet-based dissemination of DeCSS, as witnessed by discussions on slashdot.org, other Internet sites, further news coverage about these developments and lawsuits in both California and New York challenging Internet distribution of the program.[115] Many who posted DeCSS on their websites did so to protest what they perceived to be heavy-handed tactics of the motion picture industry in asserting intellectual property rights as a basis for stopping dissemination of DeCSS, as witnessed by the boastful statements of disrespect for the law cited in DVD CCA's complaint.[116] Many in the information technology field had opposed adoption of the Digital Millennium Copyright Act's anti-circumvention rules as unwarranted regulations of technological development and posted DeCSS as a means to protest the law after its passage.[117] Bunner and at least some other posters of DeCSS also wanted the program to

---

[111] Robert Post, *Encryption Source Code and the First Amendment*, 15 Berkeley Tech. L.J. 713, 719 (2000).
[112] See Bernstein v. United States, 922 F. Supp. 1426 (N.D. Cal. 1996) (discussing Snuffle program).
[113] Post asserts that "[t]he author who distributes encryption source code to consumers to be used in [their computers] is therefore not participating in any public dialogue or debate. For this reason, regulation of encryption software in such contexts would seem to raise very different constitutional questions than any we have so far discussed. Such regulation appears, on its face, no different than the regulation of hardware in computers." Id. at 1720.
[114] See, e.g., Interview of Jon Johansen, Slashdot, available at http://slashdot.org/interviews/00/01/31/096228.shtml; Interview with Jon Johansen, LinuxWorld, available at http://www.linuxworld.com/linuxworld/lw-2000-01/lw-01-dvd-interview.html; Teenager Wins DVD Battle, available at http://news.bbc.co.uk/1/hi/technology/2635293.stm.
[115] *Bunner*, 113 Cal. Rptr. 338; *Corley*, 273 F.3d 429.
[116] DVD CCA Complaint, supra note xx, para. 50. While the First Amendment surely protects boastful statements of disrespect for the law, Judge Elving was correct that such statements may reveal a defendant's state of mind which may be relevant to his or her liability for tortious speech acts, whether libel or trade secret misappropriation.
[117] The Electronic Frontier Foundation, for example, has challenged the DMCA anti-circumvention regulations as unwarranted and unconstitutional. Bunner and many fellow defendants may have anticipated litigation under the controversial anti-circumvention provisions enacted by Congress in 1998 as part of the

be available to aid the development of an open source Linux-based DVD player.[118] Other computing professionals, including Carnegie Mellon University researcher David Touretsky, have posted DeCSS to educate the public about CSS and various ways to express how CSS might be descrambled.[119] Thus, because of its contribution to public debate, the Court of Appeal correctly concluded that DeCSS, at least in source code form,[120] was First Amendment protected expression.

4. The Court of Appeal Was Correct in Ruling That The Preliminary Injunction Against Bunner's Posting of Source Code Was a Prior Restraint on Speech.

The Court of Appeal was also correct in concluding that an injunction against disclosure of source code forms of DeCSS by Bunner and others was a restriction on "pure speech" in the *Bartnicki* sense and a prior restraint on speech that bears a heavy burden of justification in the face of a First Amendment challenge.[121]

While the Supreme Court has not articulated a specific exception to First Amendment prior restraint doctrine for cases involving trade secret misappropriation, preliminary injunctions in trade secret cases are generally consistent with the First Amendment because they restrain wrongful conduct, not speech.[122] To the extent preliminary injunctions in trade secret cases restrain speech, they generally do so in order to enforce express or implicit pledges to keep information confidential or to stop employees, former employees, licensees or other confidential recipients of secrets from breaching contracts. Moreover, most trade secret cases involve, as the Supreme Court observed in *Bartnicki*, matters of private, not public, concern.[123] Moreover, enjoining

---

Digital Millennium Copyright Act (DMCA), although they seem unlikely to have anticipated a trade secrecy lawsuit. Bunner's declaration in the California trade secret case denies any knowledge that DeCSS contained any trade secrets. See Declaration of Andrew Bunner in Opposition to Order to Show Cause Re Preliminary Injunction Against All Defendants, Jan. 7, 2000, available at http://www.eff.org/IP/Video/DVDCCA_case/20000107-pi-motion-bunnerdec.html.

[118] See Bunner Declaration, supra note xx, para. 8-11; Pavlovich v. Superior Court, 127 Cal. Rptr.2d 329, 339-43 (Sup. Ct. 2002).

[119] Gallery of CSS Descramblers, available at http://www-2.cs.cmu.edu/~dst/DeCSS/Gallery/.

[120] The principal argument that object code should be treated the same as source code for First Amendment purposes is that there is no bright line distinction between them. See Gallery of CSS Descramblers, supra note xx. From the standpoint of the EFF, this means that object code should be equally entitled to First Amendment protection as source code because computer scientists cannot know whether a program is an efficient and effective expression of programming ideas without executing the program in machine-readable form, and scientists frequently communicate by exchanging code with one another. From DVD CCA's standpoint, source code should be regulated the same as object code because it requires only trivial effort to compile or assemble a source code expression of a program into object code form and both forms of programs are aimed at efficient functionality, not communication with a human audience. "Software is a machine whose medium of construction happens to be text." Pamela Samuelson, Randall Davis, Mitchell D. Kapor, & J.H. Reichman, *A Manifesto Concerning the Legal Protection of Computer Programs*, 94 Colum. L. Rev. 2308, 2320 (1994).

[121] *Bunner*, 113 Cal. Rptr. at 345, 348.

[122] See supra note xx and accompanying text.

[123] See RESTATEMENT OF UNFAIR COMPETITION, supra note xx, sec. 39 (discussing wide array of trade secret subject matter).

disclosure of trade secrets is generally important to preserving adequate incentives to invest in research and development and promote innovation as well as to deter commercial immorality.[124]

5. The Court of Appeal's Reasons for Distinguishing Copyright Injunctions Were Unpersuasive.

The Court of Appeal offered three reasons why justifications for preliminary injunctions in copyright cases did not apply to trade secrecy claims: "Both the First Amendment and the Copyright Act are rooted in the U.S. Constitution, but the UTSA lacks any constitutional basis. The prohibition on disclosure of a trade secret is of infinite duration, while the copyright protection is strictly limited in time, and there is no 'fair use' exception [in trade secrecy law] as there is for copyrighted material."[125] Unfortunately, the Court of Appeal's analysis on all three points is flawed.

Trade secrecy law may not be grounded in the U.S. Constitution, but the Supreme Court, among others, has recognized that this state law serves an important complementary role to constitutionally grounded patents and copyrights in incenting investments in innovation.[126] Moreover, relying on its power to regulate interstate commerce, the U.S. Congress has enacted the Economic Espionage Act to protect trade secrets from misappropriation,[127] thus complementing further the relationship of trade secrecy and constitutionally grounded intellectual property laws. The absence of a specific provision in the U.S. Constitution conferring on Congress the power to regulate trade secrets does not have a significant bearing on whether copyright or trade secrecy law is, as applied to specific cases, consistent with the First Amendment.

While the Court of Appeal is correct that trade secrets may potentially be of infinite duration, it overlooked the point that trade secrets are often short-lived. Trade secrecy law has long been, by its very nature, a leaky form of legal protection.[128] The consistency of trade secrecy law with First Amendment principles is attributable, in substantial part to this leakiness. Trade secrets are, for example, susceptible to reverse-engineering. They may also be independently discovered, subject to accidental disclosures, or lost through misappropriation. Injunctions in trade secret cases often contain provisions reflecting these limiting principles of trade secrecy law. Trade secret injunctions may, for example, be limited in duration to the period of time it would take a

---

[124] See, e.g., *Kewanee*, 416 U.S. at 493. See also Epstein, supra note xx, at 1036-38.
[125] *Bunner*, 113 Cal. Rptr. at 350.
[126] See, e.g., Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 482 (1974).
[127] Pub. L. No. 104-294, 110 Stat. 3488 (codified at 18 U.S.C. ss. 1831-1839). For a discussion of this law and its justification, see, e.g., Rochelle C. Dreyfuss, *Trade Secrets: How Well Should We Be Able to Hide Them? The Economic Espionage Act of 1996,* 9 Fordham Intell. Prop., Media, & Ent. L.J. 1, 15 (1998); James H.A. Pooley, Mark A. Lemley, & Peter J. Toren, *Understanding the Economic Espionage Act of 1996*, 5 Tex. Intell. Prop. L.J. 177, 195 (1997).
[128] See, e.g, Dreyfuss, supra note xx.

legitimate reverse engineer to discover the secret.[129] Trade secret injunctions also routinely provide that the injunctions will be lifted if the secret later becomes public through no misdeed of the defendants.[130] Neither limitation was included in the trade secret injunction in the *Bunner* case.[131]

While trade secrecy law has no equivalent to copyright's fair use doctrine, there is some overlap in function between limiting principles of trade secrecy law and those of copyright law, for example, in privileging reverse engineering and independent creation. In cases such as *Chicago Lock v. Fanberg* and *RTC v. Lerma*, courts in trade secrecy cases were able to reach results consistent with First Amendment principles by relying on limiting doctrines of trade secrecy law to allow publication or republication of previously trade secret information by those who have not participated in misappropriation,[132] just as courts have relied on copyright's fair use doctrine when deciding that copyright rules are consistent with the First Amendment.[133]

6. The Court of Appeal Should Have Considered the Vulnerability of Trade Secrets to Destruction as a Reason Favoring Issuance of Preliminary Injunctions in Trade Secret Cases.

The Court of Appeal should have considered that injunctions are, in some respects, more justifiable in trade secrecy cases than in copyright cases. After all, copyright owners generally intend to make their protected works widely available to the public in order to recoup their investments. They simply want to control how, when and by whom the works are made available. Developers of trade secrets stand to lose not just some revenue and control over intellectual assets unless misappropriation of their secrets is preliminarily enjoined, as copyright owners would, but the intellectual assets themselves may be destroyed without appropriate injunctive relief.[134] The special vulnerability of trade secrets to destruction through disclosure does not mean that the First Amendment has no application to trade secrets, but it does mean that preliminary injunctions are often justifiable when trade secrets have been or are clearly about to be misappropriated. Although the Court of Appeal indicated in its *Bunner* decision that an injunction against publication of DeCSS might be an appropriate remedy after a full trial on the merits,[135] the availability of DeCSS on the Internet prior to trial would vitiate any secrets from CSS that the program might contain.

7. The Internet Is Not So Dangerous for Trade Secrets as to Warrant Lesser First Amendment Protection for Information Posted There.

---

[129] See, e.g., Data General Corp. v. Digital Computer Controls, Inc., 297 A.2d 433 (Del. Ch. 1971), aff'd, 297 A.2d 437 (Del. S. Ct. 1972)(injunction should last no more than the time it would take the defendant to reverse engineer the secret); RESTATEMENT OF UNFAIR COMPETITION, supra note xx, sec. 44(3), comment f.
[130] See, e.g., id.
[131] *McLaughlin*, 2000 WL 48512 at 3.
[132] See supra notes xx and yy and accompanying texts.
[133] See, e.g., Harper & Row Pub., Inc. v. Nation Enterp., 471 U.S. 539 (1985)(fair use contributes to compatibility of copyright and the First Amendment).
[134] See, e.g., Lemley & Volokh, supra note xx, at 229.
[135] *Bunner*, 113 Cal. Rptr. at 351.

Judge Elving was correct that posting information on the Internet should not automatically cause it to cease to be a protectable trade secret. If, for example, a misappropriator posts information on an obscure site on the Internet and the presence of the information there is quickly detected, a trade secret owner should generally be able to obtain a court order to take the information down from the Internet site and to forbid reposting of it. Such an outcome is consistent with other trade secret cases in which, for example, lawyers initially failed to seek a court order to seal documents containing trade secrets as part of court filings but realized this promptly and thereafter sought a protective order.[136] Just because the document might have been, in theory, publicly accessible for a short period of time does not necessarily mean it has lost its trade secret status, particularly if very few persons have actually seen the information.

However, the longer information is available on the Internet, the more sites at which it is available, the larger the number of people who have accessed the information, the farther word has spread about the availability of the information (e.g., through newsgroups or in chatrooms), the greater is the likelihood that trade secret status will be lost.[137] This is unfortunate, of course, but it is an inherent risk in relying upon trade secrecy law that the information will leak out, particularly information susceptible to being reverse engineered.

In explaining the preliminary injunction in *Bunner*, Judge Elving expressed concern that not enjoining Bunner and others from posting of DeCSS would "encourage misappropriators of trade secrets to post the fruits of their wrongdoing on the Internet as quickly as possible and as widely as possible thereby destroying a trade secret forever. Such a holding would not be prudent in this age of the Internet."[138] The Internet does, of course, pose risks for trade secret developers—as indeed it poses for many other important societal interests (e.g., children who may be exposed to harmful materials and Internet users who may suffer from spam and fraudulent solicitations)—but these risks are not so grave that courts should distort trade secret law or the First Amendment to make the rules stricter in cyberspace than in other realms.

There have, in fact, been relatively few instances of trade secret misappropriation via the Internet.[139] Judge Elving's ruling in *Bunner* is the only reported case in which the posting of alleged trade secrets on the Internet has been enjoined. The rarity of lost trade secrets or injunctions against public disclosure of trade secrets is particularly striking, given the prevalence of copyright infringement in the digital networked environment.[140]

---

[136] See, e.g., Gates Rubber Co. v. Bando Chemical Indus., Ltd., 9 F.3d 823, 849 (10th Cir. 1993)(inadvertent and inconsequential disclosures of trade secret at trial and short delay in sealing court records did not cause loss of trade secret status).

[137] See, e.g., *Lerma*, 908 F. Supp. at 1368-69 (information available in unsealed court records for two years and on the Internet for ten days).

[138] *McLaughlin*, 2000 WL 48512 at 3 (Cal. Superior 2000).

[139] But see Jennifer 8. Lee, Student Arrested in DirecTV Piracy Case, N.Y. Times, Jan. 3, 2003, at B2 (student arrested for stealing DirecTV trade secrets and posting them on the Internet).

[140] See, e.g., A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001)(discussing millions of users of Napster's peer to peer file sharing technology to swap digital music files).

The main reason trade secrecy status is rarely lost via the Internet is because misappropriators of trade secrets typically do not want to publish the secrets to the world, as would generally occur by Internet publication. Rather, they want to exploit the secret for their own commercial purposes. The well-established rule that a misappropriator of trade secrets cannot escape liability simply by posting trade secrets on the Internet addresses Judge Elving's concern.[141] Moreover, firms can take a number of steps to protect trade secrets from Internet misappropriation.[142] Finally, a significant deterrent to publication of trade secrets on the Internet is the likelihood of detection of the misappropriation, and the consequent risk of substantial financial liability for misappropriation as well as of criminal prosecution under the Economic Espionage Act.[143]

Thus, the dangers of lost trade secrets on the Internet, while substantial, are not as great as some commentators have feared.[144] They are certainly not so great as to require courts to be more generous in issuing injunctions than traditional principles would call for. Traditional limiting principles of trade secrecy law, as well as First Amendment considerations, support this conclusion.

E. What Should the California Supreme Court Do In *Bunner*?

The California Supreme Court may well—and should—resolve the *Bunner* case by deciding that whatever trade secret information from CSS can be discerned from DeCSS lost its status as a protectable trade secret after DeCSS was widely published in source code form on the Internet.[145] If the court decides to address the First Amendment defense

---

[141] See, e.g., *Lerma*, 908 F. Supp. at 1368.

[142] See, e.g., David G. Majdali, *Note, Trade Secrets Versus the Internet: Can Trade Secret Protection Survive the Internet?*, 22 Whittier L. Rev. 125, 145-55 (2000); Ryan Lambrecht, *Note, Trade Secrets and the Internet: What Remedies Exist for Disclosure in the Information Age*, 18 Rev. Litig. 317, 339-40(1999).

[143] See 18 U.S.C. sec. 1343 (Supp. 1998). See also Lambrecht, supra note xx, 18 Rev. Litig. at 361-62 (discussing criminal sanctions for trade secret misappropriation).

[144] See, e.g., Adkins, supra note xx, (emphasizing risks to trade secrets on the Internet).

[145] Judge Elving erred, as a matter of law, in ruling that reverse engineering of a mass-marketed product (which it presumed occurred in violation of a mass-market license agreement) constituted misappropriation of trade secrets learned from reverse engineering. He failed to consider the many policy reasons why California law and federal intellectual property policy strongly favor allowing mass-marketed products to be reverse engineered and the results of reverse engineering to be used and disseminated as the reverse engineer chooses. Judge Elving committed further legal error in ruling that Bunner's posting of the DeCSS program on the Internet was a continuation of the reverse engineer's purported misappropriation. By the time Bunner posted DeCSS on his website, DeCSS had already been broadly disseminated on the Internet. Even assuming that DeCSS contained CSS trade secrets (which is unclear), the availability of DeCSS on the Internet prior to Bunner's posting necessarily caused the loss of any such CSS trade secrets, even if DVD CCA was been correct (which it is not) that the reverse engineer had misappropriated CSS trade secrets. Regrettably, the Court of Appeals did not fully analyze DVD CCA's trade secret claims, focusing instead on Bunner's claim that issuance of a preliminary injunction in this case violated the First Amendment. While proper application of traditional limiting principles of trade secrecy law would have made it unnecessary for Bunner to raise a First Amendment defense, Judge Elving committed further error in failing to take seriously Bunner's First Amendment defense. Regrettably, the Court of Appeal's analysis of the First Amendment defense was flawed as well.

in the *Bunner* case, it should affirm the Court of Appeal, but do so on somewhat different reasoning than the Court of Appeal under the analysis developed in the next section.

IV. Implications of *New York Times v. United States* and *Bartnicki v. Vopper* for Trade Secret Cases

All of the trade secret/free speech cases have invoked decisions pronouncing that prior restraints on speech and press are highly disfavored and presumptively unconstitutional.[146] Especially frequently invoked is the Supreme Court's decision in New York Times v. United States (widely known as the *Pentagon Papers* case).[147] If enjoining disclosure of secrets damaging to national security interests violates the First Amendment, courts understandably wonder how it could be consistent with the First Amendment to enjoin disclosures of trade secrets, given that these interests, while important, are obviously so much less fundamental than national security interests. Also seeming to support a broad role for the First Amendment in trade secrecy cases is the Supreme Court's very recent decision in *Bartnicki v. Vopper*, which held that a regulation forbidding disclosure of non-public information was a regulation of "pure speech" and unconstitutional as applied to innocent recipients of misappropriated information. The *Bartnicki* decision too influenced the Court of Appeal in favor of Bunner's First Amendment defense.[148] This section will review the Supreme Court's prior restraint and *Bartnicki* decisions, and suggest that while these decisions do have some bearing on the appropriateness of preliminary injunctions and other relief in trade secrecy cases, the Supreme Court's prior restraint decisions are not entitled to as much deference as the trade secret/First Amendment defenses have so far given them.

A. Prior Restraints and *New York Times v. United States*

The facts of the *Pentagon Papers* case are well-known, but worth briefly revisiting. Daniel Ellsberg obtained access to a set of documents analyzing the Vietnam War prepared for the U.S. Department of Defense while working for the Rand Corporation.[149] Ellsberg communicated with personnel at the New York Times and Washington Post about the documents and arranged for copies of the documents to be delivered to these newspapers. The Times and the Post spent several months analyzing the documents, and then began publishing excerpts in their newspapers. The United States government sought to enjoin further publication of excerpts of the documents. The

---

[146] The classic Supreme Court prior restraint decisions other than New York Times, Inc. v. United States include: Near v. Minnesota, 283 U.S. 697 (1931); Bantam Books, Inc. v. Sullivan, 372 U.S. 58 (1963); Freedman v. Maryland, 380 U.S. 51 (1965); Nebraska Press Ass'n v. Stuart, 427 U.S. 539 (1976).

[147] See, e.g., *CBS v. Davis*, 510 U.S. at 1345; *Proctor & Gamble*, 78 F.3d at 225; *Ford v Lane*, 67 F. Supp. 2d at 751; *RTC v. Lerma*, 897 F. Supp. at 263; *Bunner*, 113 Cal. Rptr. at 351. The *Sports Management News* decision was the only trade secret/free speech case that did not invoke the Pentagon Papers case. Because the Oregon Supreme Court was analyzing the constitutionality of the injunction in that case under the Oregon Constitution, it did not consider whether it would have reached the same result by interpreting the First Amendment. *Sports Management News*, 921P.2d at 1307-08.

[148] See supra note xx and accompanying text concerning the Court of Appeal's reliance on *Bartnicki*.

[149] The documents were constituted a classified study entitled "History of U.S. Decision-Making Process on Viet Nam Policy." *N.Y. Times*, 403 U.S. 714.

Supreme Court ruled that the newspapers could continue publishing the Pentagon Papers over the government's objection.[150]

Each member of the Court wrote his own opinion in the case.[151] Justices Black and Douglas were convinced that the press must always be free to publish news free from prior restraint by the government.[152] Justice Brennan accepted that prior restraints were justifiable in "an extremely narrow class of cases,"[153] but thought that the government's case against the New York Times and Washington Post was "predicated upon surmise or conjecture that untoward consequences may result."[154] In contrast, Justices White and Stewart were persuaded that publishing the papers would cause substantial damage to U.S. interests,[155] but believed that the government had not satisfied the "unusually heavy justification" for a prior restraint, especially "in the absence of express and appropriately limited congressional authorization for prior restraints in circumstances such as these."[156]

Justice Marshall questioned whether the inherent powers of the Executive Branch allowed it to invoke the equity jurisdiction of the Court to obtain an order restraining publication of the Pentagon Papers.[157] He pointed out that Congress had enacted numerous laws to punish those who wrongfully disclosed secret information, and that Congress had considered, but refused to enact, a law that would have given the Executive Branch authority to proceed against the newspapers in cases such as this.[158] Justices Burger and Harlan, who dissented, were unsympathetic to the newspapers' pleas in part because the publishers knew at the time they obtained the Pentagon Papers that the documents had been stolen.[159] All three dissenters objected to the haste with which the case had been brought before the Court and thought that the government should have had more of an opportunity to make its case.[160]

Proponents of a broad role for the First Amendment in trade secrecy cases perceive the *Pentagon Papers* case to present four highly salient characteristics: 1) the documents about to be published had been misappropriated; 2) although publishers of the documents had not participated in the initial wrongdoing, they knew that the documents to be published had been wrongfully obtained; 3) because of this, the publishers risked criminal and civil liability; and 4) publication of the documents could damage important

---

[150] A three paragraph per curiam decision preceded the nine opinions by the Justices. Id. at 714.
[151] Among the six Justices who voted against a prior restraint, Justices Black and Douglas concurred in one another's opinions, as did Justices White and Stewart as to their opinions. Justice Harlan wrote a dissenting opinion which Justices Burger and Blackmun joined.
[152] *N.Y. Times*, 403 U.S. at 714-24. Black and Douglas wrote separate opinions but concurred in one another's opinions. Holding that the publication of news can be enjoined, Black thought, "would make a shambles of the First Amendment." Id. at 714.
[153] Id. at 726. This was, in his view, only when the nation was at war, and the proposed publication would obstruct the war effort, as by publishing non-public details about the sailing dates of warships. Id.
[154] Id. at 725-26.
[155] Id. at 731.
[156] *N.Y. Times*, 403 U.S. at 732-33.
[157] Id. at 741-42.
[158] Id. at 744-45.
[159] Id. at 749-51 (Burger dissent); id. at 754-55 (Harlan dissent).
[160] Id. at 749-62.

interests.[161] Some trade secret cases parallel the *Pentagon Papers* case in all four respects, although the interests at stake in the *Pentagon Papers* case were U.S. national security and the lives of U.S. troops or operatives,[162] whereas in trade secret cases, the interests at stake are economic. Comparing the interests at stake, the Court of Appeal in *Bunner* concluded that "DVD CCA's statutory right to protect its economically valuable secret is not an interest that is 'more fundamental' or even on an equal footing with national security interests or other vital governmental interests that have previously been found insufficient to justify a prior restraint."[163] Similar reasoning is evident the handful of trade secret cases in which First Amendment/free speech defenses were successful.[164]

If the Supreme Court in the *Pentagon Papers* had been unanimous or nearly so on the First Amendment absolutist positions of Justices Black and Douglas or the near-absolutist position of Justice Brennan, perhaps it would be fair to infer that preliminary injunctions in trade secrecy cases, insofar as they forbid disclosures of non-public information, would be similarly constitutionally suspect. Even these Justices were First Amendment absolutists or near-absolutists as to the traditional press, as to news (in particular, as to news criticizing governmental decisions), and as to government attempts to assert censorial powers over the publication decisions of major newspapers. None of the trade secret cases so far have presented a similar confluence of peak First Amendment values. Even if we assume that these Justices would have been First Amendment absolutists or near-absolutists in cases involving private parties, trade secrets, and some non-media defendants, it is important to realize that several Justices in the *Pentagon Papers* were willing to accept that proof of grave and irreparable injury would justify a prior restraint. In some trade secret cases, proof of this sort will sometimes be available. Moreover, several Justices in the *Pentagon Papers* case were concerned with the lack of legislative authority for enjoining the press from publishing non-public government documents. Trade secret cases, by contrast, are typically brought under state trade secret statutes that expressly authorize issuance of preliminary and permanent injunctions.[165]

Consider too that although the Court of Appeal in *Bunner* stated that "the Supreme Court has never upheld a prior restraint, even faced with the competing interest of national security or the Sixth Amendment right to a fair trial,"[166] this is not exactly true. In Snepp v. United States, [167] for example, the Court upheld an injunction and other restrictions on publication of a book written of a former employee of the Central

---

[161] See, e.g., Greene, supra note xx, 543-48.

[162] Id. at 762-63 (Blackmun dissent)(giving credence to predictions that publication of the papers would result in "the death of soldiers, the destruction of alliances, the greatly increased difficulty of negotiation with our enemies, [and] the inability of our diplomats to negotiate")

[163] *Bunner*, 113 Cal. Rptr. at 351. It also quoted from another trade secret/first amendment case: "If a threat to national security as insufficient to warrant a prior restraint in New York Times v. United States, the threat of plaintiff's copyrights and trade secrets is woefully inadequate." Religious Technology Center v. Lerma, 897 F.Supp. 260, 263 (E.D. Va. 1995).

[164] See, e.g., *Proctor & Gamble*, 78 F.3d at 225; *Ford v. Lane*, 67 F.Supp.2d at 751.

[165] The Uniform Trade Secrets Act provides that "[a]ctual or threatened misappropriation may be enjoined." Id. at sec. 3.

[166] *Bunner*, 113 Cal. Rptr. at 351, citing Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 563 (1976) and New York Times Co. v. United States, 403 U.S. 713, 718-726 (1971).

[167] 444 U.S. 507 (1980).

Intelligence Agency who had promised as a condition of his employment with the agency not to publish works about his experiences without agency clearance. And in Seattle Times Co. v. Rhinehart,[168] a unanimous Supreme Court upheld a prior restraint on publication of newsworthy information about funding sources of a foundation about which the Seattle Times had published numerous stories. The prior restraint was justified, said the Court, because the Seattle Times obtained access to the information for the limited purposes of discovery in a lawsuit between it and Rhinehart and the information was subject to a protective order.[169]

The Supreme Court has also sometimes upheld regulatory regimes that authorize prior restraints when the legal standards are rigorous and there are procedural safeguards in place "designed to obviate the dangers of a censorship system."[170] For example, the Court upheld a statutory scheme permitting pre-publication injunctions of allegedly obscene books during the pendency of litigation as to whether specific works were obscene because the legal standards were clear and procedures had been established to ensure expeditious adjudication.[171] As long as standards for issuance of preliminary injunctions in trade secret cases are clear and procedures are suitably expeditious, it would seem that the Supreme Court would find preliminary injunctions in trade secret cases to be justifiable in general.

Whether preliminary injunctions are constitutionally valid if they forbid disclosure of non-public information obtained by wrongful means is somewhat unclear.[172] The *Pentagon Papers* decision obviously supports the right of the press to publish documents it knows to be stolen. However, it tells us nothing whatever about whether the government could have enjoined Ellsberg from disclosing the Pentagon Papers to major newspapers or more generally to the public, had the government learned about the impending disclosure before or while it was ongoing. In *CBS v. Davis*, Justice Blackmun (who, it should be noted, was dissenter in the *Pentagon Papers* case) lifted a preliminary injunction forbidding CBS from broadcasting as part of a news program a videotape of meat-packing operations which a state court found was illegally obtained on trade secret and other grounds.[173] Prior restraints, said Justice Blackmun, were only available "where the evil that would result from the reportage is both great and certain and cannot be militated by less intrusive means."[174] Justice Blackmun concluded that this burden had

---

[168] 467 U.S. 20 (1984).

[169] Some courts in state trade secret cases have considered First Amendment defenses but rejected them because of the existence of a contractual or confidential relationship obligation of non-disclosure. See, e.g., Garth v. Staktek Corp., 876 S.W.2d 545 (Tex. App. 1994)(contractual obligation); Cherne Indus., Inc. v. Grounds & Assoc., Inc., 278 N.W.2d 81 (Minn. 1979)(confidential relationship obligation).

[170] Freedman v. Maryland, 380 U.S. 51 (1965)(striking down a motion picture licensing regime because of long delays before judicial review of decision by censorship board).

[171] Kingsley Books, Inc. v. Brown, 354 U.S. 436 (1957).

[172] The *Sports Management News decision* indicates that "there may be circumstances where a restriction on publication…to protect property rights would be constitutional. The parties have discussed, for example, whether the constitution historically would permit a prior restraint on speech…if issued against an Adidas employee, bound to confidentiality, who sought to disclose the alleged trade secrets or against a publisher who had broken the criminal law to obtain the trade secrets." 921 P.2d at 1309, n.8.

[173] CBS, Inc. v. Davis, 510 U.S. 1315, 1315 (1994).

[174] Id.

not been met because the trial court had merely speculated that broadcast of the footage could cause harm.[175] This decision is significant in part because the state court had issued a preliminary injunction after being persuaded that CBS had been engaged in "calculated misdeeds" in acquiring the information, not as an innocent post-misappropriation recipient of the information.[176]

Because all of the trade secret/free speech cases except *CBS v. Davis* have involved claims of secondary liability for trade secret misappropriation, it is worth considering the Supreme Court's decision in *Bartnicki v. Vopper* which also involved secondary liability for disclosure of non-public information.

B. *Bartnicki v. Vopper*

Bartnicki and Kane were union officials whose cell phone conversation about a contentious labor struggle in Pennsylvania was intercepted by an unknown person.[177] Vopper, a radio commentator who had previously been critical of the union, played a tape of the intercepted conversation on a local radio station. The tape involved a matter of public concern because it included talk of blowing off the front porches of homes of the union's adversaries if the union didn't get what it wanted.[178] The tape was subsequently republished by other local news media.[179]

Bartnicki and Kane sued Vopper and other media defendants for violating federal wiretap law which makes it illegal to "willfully disclose[]… to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the [illegal] interception of a wire, oral, or electronic communication."[180] Bartnicki and Kane sought actual, statutory, and punitive damages as well as attorney fees.[181] Through discovery, Bartnicki and Kane learned that Vopper had obtained the tape from the head of a local taxpayers' organization, Jack Yocum, who claimed the tape had been left anonymously in his mail box.[182] Although the trial court rejected the First Amendment defenses of Vopper, the other media defendants, and Yocum because it regarded the wiretap law as a content-neutral law of general applicability that satisfied intermediate scrutiny standards,[183] it

---

[175] Id.
[176] Like the Oregon Supreme Court in *Sports Management News*, 921 P.2d at 1309, n. 8, Justice Blackmun in *CBS v. Davis* suggested that a prior restraint might be justified if the publisher sought to be enjoined had violated the criminal law in obtaining the information. 510 U.S. at 1315.
[177] Bartnicki v. Vopper, 532 U.S. 514, 519 (2000).
[178] Id.
[179] Id.
[180] 18 U.S.C. sec. 2511(1)(c).
[181] *Bartnicki*, 532 U.S. at 520.
[182] Id. at 519.
[183] Id. at 521. Justice Rehnquist, along with Justices Scalia and Thomas, objected to the application of strict scrutiny in *Bartnicki* and expressed the view that they satisfied intermediate scrutiny. "These laws are content neutral; they only regulate information that was illegally obtained; they do not restrict republication of what is already in the public domain; they impose no special burdens upon the media; they have a scienter requirement to provide fair warning; and they promote privacy and free speech of those using

certified an appeal on the First Amendment issues.[184] After a divided appellate court ruled in favor of the First Amendment defenses,[185] the Supreme Court took certiorari to resolve a conflict among the circuits on First Amendment defenses in wiretap cases.[186]

The Supreme Court accepted Bartnicki's assertions that the interception was intentional and that Vopper and other defendants had reason to know that the interception was illegal. The question was whether it was consistent with the First Amendment to hold them liable for damages for disclosure of the illegally intercepted conversation. The Court decided it was not, distinguishing this from typical wiretap cases on three grounds: "First, respondents played no part in the illegal interception. Rather, they found out about the interception only after it occurred, and in fact never learned the identity of the person or persons who made the interception. Second, their access to the information on the tapes was obtained lawfully, even though the information itself was intercepted unlawfully by someone else. Third, the subject matter of the conversation was a matter of public concern."[187]

The Court agreed that the wiretap laws were content-neutral and that their purpose—to protect the privacy of communications—was unrelated to the suppression of speech.[188] The prohibition on disclosure, however, "is fairly characterized as a regulation of pure speech." Quoting from the appellate court decision in *Bartnicki*, the Court said: "'[I]f the acts of "disclosing" and "publishing" information do not constitute speech, it is hard to imagine what does fall within that category.'"[189] The Court relied upon several precedents upholding the right of the media to publish lawfully obtained truthful

---

cellular phones. It is hard to imagine a more narrowly tailored prohibition on the disclosure of illegally intercepted communications…." Id. at 548.

[184] The District Court certified two questions: first, whether imposition of liability on the media defendants was consistent with the First Amendment where the tape was illegally made but the media defendants did not participate in the illegal interception and the broadcast of contents was newsworthy, and second, whether it would violate the First Amendment to impose liability on Yocum for disclosing the contents to the media defendants. Id. The Court ultimately drew no distinction between Yocum and the media defendants in its First Amendment analysis. Id. at 525, n. 8.

[185] Bartnicki v. Vopper, 200 F.3d 109 (3rd Cir. 1999). The majority concluded that the disclosure provisions "deterred significantly more speech than necessary to protect the privacy interests at stake." Bartnicki, 532 U.S. at 522. Judge Pollack dissented on the ground that "the prohibition against disclosures was necessary in order to remove the incentive for illegal interceptions and to preclude compounding the harm caused by such intereceptions through wider dissemination." Id.

[186] The most directly conflicting precedent was Boehner v. McDermott, 191 F.3d 463 (D.C. Cir. 1999) (rejecting First Amendment defense). See also Peavy v. WFAA-TV, Inc., 221 F.3d 158 (5th Cir. 2000).

[187] *Bartnicki*, 532 U.S. at 525. Justices Breyer and O'Connor wrote a separate concurrence which emphasized that the public interest in disclosure in *Bartnicki* was "unusually high" and the public interest in nondisclosure was "unusually low" because the conversation included a threat of potential violence. Id. at 535, 540. Breyer's concurrence gave some examples of situations where disclosures would not be justified as matters of public concern. Id. at 540. However, Justice Rehnquist's dissent regarded the "matter of public concern" limitation to be "an amorphous concept that the Court does not even attempt to define." Id. at 541.

[188] Id. at 526.

[189] Id. at 526-27, quoting Bartnicki v. Vopper, 200 F.3d at 120. The Court distinguished disclosure of illegally intercepted communications such as Vopper's from other uses of illegally intercepted communications that did not raise significant First Amendment concerns. *Bartnicki*, 532 U.S. at 526-27.

information even though they knew of rules forbidding disclosure of such information.[190] Quoting from one such case, the Court observed 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.'"[191]

In response to the government's argument that holding disclosers liable was necessary in order to deter the interception of private conversations, the Court agreed that this rationale justified a ban on disclosure by the person who had illegally intercepted the communication.[192] However, "[t]he normal method of deterring unlawful conduct is to impose an appropriate punishment on the person who engages in it. If the sanctions that presently attach to a violation of sec. 2511(1)(a) do not provide sufficient deterrence, perhaps those sanctions should be made more severe. But it would be quite remarkable to hold that speech by a law-abiding possessor of information can be suppressed in order to deter conduct by a non-law-abiding third party."[193] There was, the Court observed, "no empirical evidence to support the assumption that the prohibition on disclosures reduces the number of illegal interceptions."[194]

The government also sought to justify the prohibition on disclosure of illegally intercepted communications on the ground that not doing so would have a chilling effect on private communications, a concern also within the ken of the First Amendment.[195] The Court agreed that this was a significant interest, but this was, in its view, a case where there were "important interests on both sides of the constitutional calculus,"[196] and in this case, "privacy concerns give way when balanced against the interest in publishing matters of public importance."[197]

---

[190] See, e.g., Smith v. Daily Mail Pub. Co., 443 U.S. 97 (1979) (publication of the name of a juvenile defendant); Florida Star v. B.J.F., 491 U.S. 524 (1989) (publication of the name of a rape victim); Landmark Communications, Inc. v. Virginia, 435 U.S. 829 (1978) (publication of information from confidential proceedings of state judicial review committee). The Court also relied on New York Times v. United States, 403 U.S. 713 (1971) as a case in which "the Court upheld the right of the press to publish information of great public concern obtained from documents stolen by a third party." *Bartnicki*, 532 U.S. at 528. The dissent objected to the Court's reliance on these precedents, distinguishing the former from *Bartnicki* because the information in those cases was already publicly available and the Court's concern was about press timidity and self-censorship, id. at 545-47, and the latter as "mystifying" given that the Pentagon Papers decision involved an attempted prior restraint by the government, not an action for damages, id.at 555.

[191] *Bartnicki*, 532 U.S. at 528, quoting Smith v. Daily Mail Pub. Co., 443 U.S. 97, 103 (1979).

[192] *Bartnicki*, 532 U.S. at 529.

[193] Id. at 529-30. The Court went on to say: "Although there are some rare occasions in which a law suppressing one party's speech may be justified by an interest in deterring criminal conduct by another, see, e.g., New York v. Ferber, 458 US 747 (1982), this is not such a case." *Bartnicki*, 532 U.S. at 530. The dissent pointed out that a similar rationale to the government's "dry up the market theory" in support of wiretap disclosure laws underlies the regulation of child pornography. Id. at 551-52.

[194] Id. at 531. The dissent was quite critical of the majority for not deferring to Congress' fact finding and reasonable judgment of the need for rules forbidding disclosure of illegally intercepted communications. Id. at 549-50.

[195] Id. at 532-33. The dissent gave much attention to this concern. Id. at 552-54.

[196] Id. at 533.

[197] Id. at 534.

Bartnicki is consistent with other decisions involving public disclosure of misappropriated information. In Pearson v. Dodd, for example, the Court of Appeals for the D.C. Circuit affirmed a trial court decision that two newspaper columnists could not be held liable for privacy violations for publishing information they obtained from copies of documents misappropriated by Dodd's employees, and reversed the trial court's ruling that the columnists were liable for conversion of the documents because the columnists had received copies of the documents, not originals.[198] Similarly, in Desnick v. American Broadcasting Co., the Court of Appeals for the Seventh Circuit affirmed dismissal of a lawsuit claiming damages from television broadcast of tapes surreptitiously made by persons who misrepresented their reasons for seeking eye examinations from an ophthalmic clinic.[199]

C. Implications for *Bunner* and Other Trade Secret/Free Speech Cases

The previous subsection's review of Supreme Court cases dealing with First Amendment defenses suggests five principles for analyzing First Amendment defenses in trade secrecy cases. This subsection will present these principles and explain why they suggest a relatively limited role for the First Amendment in trade secret cases.

1. First Amendment Defenses Will Rarely Succeed When the Defendant Is Under a Contractual or Confidential Relationship Obligation Not to Disclose A Trade Secret

The *Snepp* and *Seattle Times* decisions suggest that the U.S. Supreme Court would likely find no constitutional impediments to issuance of preliminary injunctions in ordinary trade secrecy cases when the defendants are under contractual obligations not to disclose trade secrets or are otherwise obliged by the confidential circumstances under which they received the secrets not to disclose them.[200] Preliminary injunctive relief in trade secret cases is especially appropriate where the disclosure pertains to information of private concern made to a private person or firm that would financially benefit from access to commercially valuable information developed by the plaintiffs.

This does not mean that persons under contractual or confidential relationship obligations will never be entitled to publicly disclose secret information on First Amendment or other public policy grounds. Consider, for example, the quandary of Jeffrey Toobin, who was under contractual obligations undertaken at the time of his employment as a prosecutor not to disclose non-public information about the Iran-Contra prosecutions except with the consent of the Office of Independent Counsel (OIC).[201]

---

[198] 410 U.S. 701 (D.C. Cir. 1968).
[199] 44 F.3d 1345 (7th Cir. 1995). However, the court sent the defamation claim back for further findings. See also Food Lion v. Capital Cities/ABC, 194 F.3d 505 (4th Cir. 1999)(rejecting trespass, fraud, and unfair trade practices claims against ABC for sending its agents to become employees in order to obtain information about food handling practices for a news story, although allowing claim to proceed for damages for breach of duty of loyalty as to Food Lion employees).
[200] See supra notes xx and accompanying text for discussion of *Snepp* and *Seattle Times*.
[201] Penguin Books USA, Inc. v. Walsh, 756 F. Supp. 770 (S.D.N.Y. 1991).

Toobin wrote a book about his experiences as an OIC prosecutor and submitted drafts of his book for review; he also made some changes to the text in response to some comments from the OIC. When the OIC would not agree to allow him to proceed with publication, Toobin sought a declaration that the OIC's excessive demands for excisions, unwarranted delays in clearing the book, and vague standards did not comport with First Amendment standards.[202] The trial court issued a declaration that Toobin was entitled to publish the book.[203] A parallel quandary in a trade secrecy context might involve a former tobacco industry executive who wants to publicly disclose information about internal studies of the health impacts of smoking which the firm had kept secret, disclosure of which would violate a confidentiality agreement.[204]

There is, moreover, good reason to doubt that the Supreme Court would have allowed a prior restraint injunction against Cowles Media whose papers decided to name Cohen as its source of information about criminal charges against a candidate for lieutenant governor in breach of its promise to him of anonymity.[205] Cohen sought compensatory and punitive damages against the paper after it published his name because he was fired from his job with a candidate for governor because disclosing the document about these charges violated his duty of loyalty. The Minnesota Supreme Court decided that allowing Cohen to recover damages would violate the First Amendment.[206] In a 5-4 decision, the U.S. Supreme Court reversed, ruling that Cohen should be able to recover damages on a promissory estoppel theory.[207] In view of the deep split on the Court as to post-disclosure damage recovery, it seems likely that the Court would have ruled against a prior restraint on publication of this information by the newspapers.[208] Admittedly, neither the *Toobin* nor the *Cohen* cases involved trade secrets, and the economic losses likely to flow from failure to enjoin disclosure of a trade secret may distinguish these cases. Yet, these decisions suggest that there may be some, albeit rare, circumstances in which the Court would uphold First Amendment defenses in trade secrecy cases.

Other public policy considerations may also limit the extent of trade secret protection for information disclosed under contractual or confidential non-disclosure

---

[202] Id. at 784-88.

[203] Id. at 788. Walsh appealed this decision to the Second Circuit Court of Appeals, but the appeal was dismissed as moot after Penguin published Toobin's book. See Penguin Books USA, Inc. v. Walsh, 929 F.2d 69 (2d Cir. 1991).

[204] See, e.g., Alan Garfield, *Promises of Silence: Contract Law and Freedom of Speech*, 83 Cornell L. Rev. 261, 264 (1998)

[205] Cohen v. Cowles Media Co., 501 U.S. 663 (1991).

[206] Cohen v. Cowles Media, Co., 457 N.W.2d 199 (1990).

[207] Id. at 670-71. The Court ruled that the law of promissory estoppel in Minnesota was a content-neutral law of general applicability, and that the First Amendment did not forbid its application to the press. Justices Blackmun, Marshall, Souter and O'Connor dissented.

[208] The dissenters objected to the "talismanic" invocation of the content-neutrality of promissory estoppel, and focused on the fact that "such laws may restrict First Amendment rights just as effectively as those directed specifically at speech itself," and regarded as "necessary to articulate, measure, and compare the competing interests involved in any given case to determine the legitimacy of burdening constitutional interests…." Id. at 677. But see Epstein, supra note xx, at 1033 (concluding that persons in Cohen's situation should be entitled to a preliminary injunction against disclosure of identity if this would breach a contract).

obligations.[209] For example, firms may require employees to sign confidentiality agreements that forbid disclosure of non-public information about the firm, and interpret this as forbidding employees to discuss the firm's business with anyone, including government agents, even though it may further important public interests for the employees to be able to speak with government agents.[210] Firms may also assert trade secrecy claims to deter employees from revealing information about, for example, a toxin used in his employer's manufacturing process in violation of environmental protection laws. Agreements of this sort may be unenforceable as a matter of public policy,[211] and in such cases, the firms asserting trade secret violations should be denied both injunctive relief and award of damages. To resolve tensions between public interests in disclosure and private trade secrecy interests, some state and federal "whistleblowing" statutes privilege certain disclosures that would otherwise be trade secrecy misappropriation.[212] Courts should also be skeptical about trade secret misappropriation claims premised on the theory that mass-market license provisions have created confidential or contractual non-disclosure requirements on members of the public, [213] including those that forbid reverse engineering of a mass-marketed product.[214]

2. First Amendment Defenses Should Rarely Succeed When the Defendant Has Directly Misappropriated A Trade Secret.

Although the *Snepp* and *Seattle Times* cases provide relatively strong support for issuance of preliminary injunctions in trade secret cases where the defendant is in privity with the plaintiff through a contractual or confidential relationship, the Supreme Court's decisions are less clear about whether preliminary injunctive relief should be available when the defendant is not in privity but has wrongfully acquired trade secrets.

CBS v. Davis is the only opinion issued by a Supreme Court Justice in a trade secret/First Amendment case, although it is not, of course, a decision by the Court.[215] However, this is a case in which a state court found that CBS had engaged in misdeeds in acquiring the videotape of the meat-packing operations it wanted to broadcast on a news program; this court also found that CBS's broadcast of the videotape would constitute trade secrecy misappropriation.[216] For Justice Blackmun, there was nothing talismanic

---

[209] See, e.g., Systems Operations, Inc. v. Scientific Games Dev. Corp., 425 F. Supp. 130 (D.N.J. 1977); U.S. v. Wallington, 889 F.2d 573 (5th Cir. 1989). See RESTATEMENT OF UNFAIR COMPETITION, supra note xx, sec. 40, comment c ("A privilege is likely to be recognized, for example, in connection with the disclosure of information that is relevant to public health or safety, or to the commission of a crime or tort, or other matters of substantial concern.").

[210] See, e.g., Garfield, supra note xx, at 264-66 (giving examples).

[211] Id. at 294-95. Even Epstein recognizes that trade secret rights should give way in some cases, as where health and safety impacts are at stake. Epstein, supra note xx, at 1043.

[212] See, e.g, 5 U.S.C.A. sec. 2320(b)(8); N.Y. Lab. Law sec. 740.

[213] See, e.g., Julie E. Cohen, *Call It the Digital Millennium Censorship Act: Unfair Use*, The New Republic Online, May 23, 2000 (discussing Microsoft's efforts to use a click-through license to impose a confidential relationship and non-disclosure obligations on those who wished to access a technical specification on an Internet site).

[214] See sources cited supra note xx.

[215] CBS, Inc. v. Davis, 510 U.S. 1315 (1994).

[216] Id.

about the fact that the plaintiff alleged misappropriation of trade secrets. He characterized the preliminary injunction as a classic prior restraint, which was presumptively unconstitutional, and concluded that speculation about harm from the broadcast was insufficient to meet First Amendment standards.[217] Blackmun announced that preliminary injunctions should not issue against disclosure of wrongfully obtained information unless "the evil that would result from the [disclosure] is both great and certain and cannot be militated by less intrusive measures."[218]

Adoption of a standard of this sort would be consistent with the default principle of First Amendment law which places responsibility on a speaker or publisher to weigh the consequences of possible civil or criminal liability for wrongful speech or publication and which trusts that rational assessments of risk will generally deter illegal speech and publication.[219] For the most part, this assumption against prior restraints works quite well. Before charging a public official with corruption, for example, newspapers tend to double-check their facts. This makes news reports more reliable than they might otherwise be, and it also reduces the risk the papers will be sued for millions of dollars in damages for libel. It seems fair to assume that the risk of civil and criminal liability substantially deters wrongful disclosures of trade secrets as well as other wrongful speech acts.

And yet, to generalize from Blackmun's opinion that a heavy presumption against preliminary injunctions should required in all trade secrecy cases seems unwarranted in ordinary trade secret misappropriation cases in which non-privity defendants intend to privately disclose the plaintiff's secrets to third parties in order to allow those parties to exploit commercially valuable secrets without paying the appropriate license fee and otherwise complying with license restrictions that the plaintiff routinely imposes. First Amendment defenses will also generally be implausible in such cases because the secrets will be matters of private, not of public, concern, where the disclosures will not advance public discourse or other public interests.

More difficult is the question about what standard to apply when courts are asked to issue preliminary injunctions against *public* disclosures of trade secrets by persons who have wrongfully acquired them. Judge Elving in *Bunner* worried that failing to enjoin the posting of misappropriated trade secrets on the Internet would encourage wrongdoers to post the fruits of their wrongdoing on the Internet in order to escape liability.[220] This concern, although warranted to some degree, ignores that trade secret anarchists or vengeful former employees or licensees who publicly disclose trade secrets can be held criminally responsible for trade secret misappropriation, and the public nature of their disclosures will ensure detection of the misappropriation, and usually of their identity. Civil suits for damages may also be available, although some commentators worry that misappropriators may not be adequately deterred from wrongful public disclosures of

---

[217] Id.
[218] Id.
[219] See, e.g., Greene, supra note xx, at 543, 551-52.
[220] *McLaughlin*, 2000 WL 48512 at 3.

trade secrets insofar as they are persons of modest means who would, in essence, be judgment-proof.[221]

And yet, Elving's basic insight—that courts should not establish rules that encourage wrongdoers to think that public disclosure will immunize them from liability—has some merit. Without preliminary injunctive relief, public disclosure will destroy the secrets and may cause irreparable harm to the plaintiff, and even post-disclosure injunctions may sometimes be appropriate. The Restatement of Unfair Competition opines that "[i]f the public disclosure results from the defendant's own unauthorized conduct, injunctive relief may remain appropriate until the information would have become readily ascertainable to the defendant through proper means. However, if the defendant's disclosure results in extensive use of the information by others, a continuing injunction may yield little benefit to the plaintiff."[222]

However, *CBS v. Davis* suggests that courts should sometimes be cautious about enjoining public disclosure of information claimed as a trade secret. The facts of *CBS v. Davis* suggest that claims of trade secrecy misappropriation may have been asserted in order to protect the firm against embarrassment or criticism.[223] *CBS v. Davis* also involved a traditional media defendant whose intent was to broadcast the information sought to be enjoined as part of a news program. In such cases, perhaps plaintiffs should have to prove certain and irreparable harm before being entitled to preliminary injunctive relief, as Justice Blackmun indicated in *CBS v. Davis*.

3. First Amendment Defense Are Most Likely to Succeed As to Innocent Recipients of Information Secrets of Public Concern Who Wish to Publicly Disclose Them.

Holding media and non-media defendants for disclosure of illegally obtained information to the public was held to be inconsistent with the First Amendment in *Bartnicki* for three reasons: first, because the defendants had not themselves illegally obtained the information, second, because the defendants had innocently received the misappropriated information, and third, because the information disclosed was of public concern.[224] Even though the Court accepted that the defendants ought to have known, after receiving the information, that it was illegally obtained, this did not change the Court's conclusion on the First Amendment defense.[225] *Bartnicki* has important

---

[221] See, e.g., Epstein, supra note xx, at 1038.
[222] RESTATEMENT OF UNFAIR COMPETITION, supra note xx, comment f at 504.
[223] Although the plaintiff alleged that the videotape revealed trade secrets about the firm's meat processing practices and the trial court issued an injunction indicating a likelihood of success on the merits, the principal concern of the firm may well have been to avoid the embarrassment of public disclosure of meatpacking processes which CBS deemed newsworthy. In this respect, *CBS v. Davis* resembles Desnick v. American Broadcasting Co., 44 F.3d 1345 (7th Cir. 1995) and Food Lion v. Capital Cities/ABC, 194 F.3d 505 (4th Cir. 1999) which also involved surreptitious taping of internal events at firms as part of investigative reporting.
[224] *Bartnicki*, 532 U.S. at 525.
[225] Id.

implications for both preliminary injunctive relief and awards of damages in trade secrecy cases.[226]

Trade secret claims are sometimes brought against third parties who received information without knowing it was misappropriated. Traditional principles of trade secret law preclude liability for innocent recipients for uses or disclosures of the secret prior to notice of misappropriation, but continued use or disclosure after the trade secret's developer gives notice that the information was misappropriated may give rise to liability.[227] When the information is of private, rather than, public concern, and the injunction sought is against private disclosure of the information, neither First Amendment nor other public policy considerations will generally preclude preliminary or permanent injunctive relief or awards of damages. However, innocent recipients of misappropriated information can sometimes avoid injunctive relief if, for example, they have made substantial investments in reliance on the lawfulness of the information.[228]

Relatively few trade secrecy cases will closely parallel *Bartnicki* by involving defendants who did not themselves participate in the misappropriation of trade secret information (or act in league with the misappropriators), who received the misappropriated information innocently (even if they later found out it had been misappropriated), and who want to publicly disclose the information because it is of public concern. Yet, some will.

All of the trade secrecy cases in which free speech defenses have prevailed (except *CBS v. Davis*) have arguably been of this sort. The *Sports Management News* case, for example, involved the publisher of a newsletter who knew or should have known that information about new Adidas products it wanted to publish was confidential information that Adidas wished to protect as a trade secret. Yet, the Oregon Supreme Court overturned issuance of a preliminary injunction against the newsletter's publication as an unconstitutional prior restraint.[229] Proctor & Gamble v. Bankers' Trust involved a temporary restraining order forbidding Business Week from publishing information it obtained from documents the magazine knew or had reason to know had been leaked to it in violation of a discovery order that aimed to protect trade secrets; yet, the Sixth Circuit Court of Appeals ruled that the TRO was an unconstitutional prior restraint on speech.[230] The trial court in *Ford v. Lane* did not deny that Lane knew or should have known that the documents which Ford employees leaked to him contained Ford trade secrets and that the leaks violated employee obligations not to disclose the firm's secrets. Yet the court decided that issuance of a preliminary injunction to stop Lane from posting this information on the Internet would be an unconstitutional prior restraint of speech. *Bunner* arguably also fits this profile. Bunner did not himself misappropriate CSS. He got DeCSS from one of the many public postings of this program on the Internet. He

---

[226] See, e.g., Lemley & Volokh, supra note xx, at 230 ("publication of a trade secret by a party who isn't bound by the contract must be constitutionally protected even against a damages judgment, and certainly ought to be protected against a preliminary injunction")
[227] See, e.g., RESTATEMENT OF UNFAIR COMPETITION, supra note xx, sec. 40(b)(3), comment d.
[228] Id.
[229] Id.
[230] Proctor & Gamble Co. v. Bankers Trust Co., 78 F.3d 219 (6th Cir. 1996).

denied knowing that DeCSS contained stolen trade secrets at the time of the initial posting, but he certainly became aware that DVD CCA claimed DeCSS embodied stolen trade secrets when he was sued for trade secret misappropriation. Bunner republished DeCSS source code in order to facilitate communication with members of the open source community who were interested in developing an open source Linux-based DVD player.[231] *Bartnicki* suggests that defendants in cases of this sort may also not be liable in damages on First Amendment grounds.

---

[231] Even though *Bartnicki* obviously involves a very different legal claim than *Bunner*—violation of federal wiretap laws as compared with a violation of state trade secrecy law—there are many similarities between the two cases. In both cases, liability was premised on public disclosure of illegally obtained information that the plaintiffs wanted to remain private, not the initial receipt and possession of it. Defendants in both cases were charged as secondary wrongdoers (i.e., they were not the persons who illegally obtained the information in dispute). Rather, they were persons remote in time and place from the allegedly illegal acts, and they did not act in league with primary wrongdoers, nor aid or abet them. Defendants in both cases denied that they knew or had reason to know that the information they published resulted from another's wrongful act, although the plaintiffs alleged that the defendants should be held liable because they should have known the information was illegally obtained, even if they did not actually know this.

The statutes in both *Bunner* and *Bartnicki* are content-neutral; yet, on the face of both statutes, disclosure of even matters of public concern would be unlawful. In both cases, two important conflicting interests had to be balanced. Moreover, holding Bunner and others liable for republishing DeCSS source code will no more deter youngsters such as Johansen from reverse engineering encryption software such as CSS in violation of shrinkwrap licenses than holding Vopper liable for damages to Bartnicki would deter illegal interceptions of cell phone conversations.

There are several reasons why *Bunner* is an even more plausible First Amendment case than *Bartnicki*. Most important is the fact that *Bartnicki* involved a claim for damages for a public disclosure of private information, whereas the relief sought in *Bunner* was a preliminary injunction. It is, moreover, telling that DVD CCA did not seek damages against Bunner or any of the other 520 co-defendants even though DVD CCA alleged that Bunner's publication of DeCSS on the Internet was alleged to be certain to have profoundly destructive effects on DVD CCA's licensing business. DVD CCA further alleged that the availability of DeCSS on the Internet would have profoundly destructive effects on the motion picture industry, the computer industry, and the consumer electronics industry; yet, no firm from these industries joined the lawsuit as a co-plaintiff seeking damages. DVD CCA's goal was to suppress the publication of DeCSS and any other CSS proprietary information, which is all the more reason for courts to be concerned about this injunction as a prior restraint.

This is not to say that *Bartnicki* unequivocally supports Bunner's First Amendment defense. For one thing, the *Bartnicki* opinion explicitly says that the Court was not deciding whether a constitutional interest in public disclosure would outweigh trade secrecy or other "purely private" interests. *Bartnicki*, 532 U.S. at 533. Counterbalancing this statement, however, is Justice Breyer's concurring opinion which relies on the Restatement of Unfair Competition for the proposition that a public interest in disclosure may outweigh trade secrecy interests when public health or safety, commission of a crime or tort, or other matters of substantial concern are at stake. Id. at 539. If the controversy over DeCSS was a matter of public concern and the posting of DeCSS was an integral part of this controversy, these factors would favor Bunner's First Amendment defense.

The concurrence of Justices Breyer and O'Connor sought to narrow the scope of the Court's ruling in *Bartnicki* by pointing to the unusually high public interest in disclosure in that case and the unusually low interest in secrecy of a threatening statement that caused the balance to tilt toward disclosure. Id. at 540. Because the *Bunner* case involves a preliminary injunction, and not an award of damages, it seems likely that Justices Breyer and O'Connor would be concerned enough about the prior restraint issues in *Bunner* to be persuaded that the balance of interests should tilt toward disclosure for this reason even if they did not believe their *Bartnicki* concurrence standard of unusually high interests in disclosure and unusually low interests in non-disclosure was met.

Before concluding that preliminary injunctions should never issue against public disclosure of trade secrets when these three factors are present—that is, non-participation in the misappropriation, innocent receipt of the information, and information of public concern—it is worth reflecting on some difficulties that attend this standard. For one thing, such a standard may encourage, unwittingly or not, the "laundering" of misappropriated information. X may be more inclined to misappropriate information and pass it to Y if Y cannot be enjoined or even held liable in damages for publishing the information, even if Y knew or had reason to know it was misappropriated. As long as X can find a way to pass the information along anonymously, both X and Y may avoid liability and the trade secret developer will be left without a remedy.

Second, it begs the question about what criteria should be used to determine whether information is of public or private concern in the context of trade secrecy law. Should information be considered of public concern just because someone wants to make it public? If the information is newsworthy, does that mean it is automatically of public concern? Can information be of public concern if it is not newsworthy? If the information is not of concern to all members of the public, how many members of the public must care before it becomes a matter of public concern? Everyone can agree that publication of the Pentagon Papers involved matters of public concern, but it is more difficult to say with a straight face that unpublished designs of sneakers or automobiles are matters of public concern, even if the fact that someone wanted to publish them to the world arguably made them newsworthy. Bunner wanted to share DeCSS source code with other open source developers, but this is a small subset of the public, and it is, moreover, at least contestable whether the development of an open source DVD player is a matter of public concern. Before too much reliance is placed on a tripartite test adapted from *Bartnicki*, it should also be noted that Justices Breyer and O'Connor concurred in the decision (thereby providing a majority of 6-3 in favor of the First Amendment defense) because the information disclosed in that case was of unusual public concern and the interest in non-disclosure was unusually low. While this indicates a lack of consensus in the Court as to liability for damages for public disclosure of misappropriated information (which might be relevant in some trade secrecy cases), this qualification is unlikely to affect the Court's view about prior restraint injunctions. But it should be noted that as fuzzy as the private vs. public concern distinction is, even fuzzier would be a standard that depended on unusually high or low interest in disclosure or non-disclosure.

Third, the tripartite standard may direct attention away from factors that ought to be taken into account in some cases. Two commentators have criticized the *Ford v. Lane* decision in part because they believe that Lane's principal reason for publishing secret design information about Ford vehicles on the Internet was to retaliate against Ford for challenging to Lane's domain name (which included the word "ford").[232] Moreover, even if it is generally reasonable to trust the judgment of traditional media about whether matters they intend to publish are matters of public concern, everyone with Internet access cannot necessarily be trusted to the same degree.

[232] See, e.g., Epstein, supra note xx, at 1037; Goldberg, supra note xx, at 272, 291.

Even with these caveats, the tripartite standard is a useful tool for courts faced with assessing whether First Amendment considerations should limit liability or injunctive relief in trade secret cases as to persons who are not in privity with the plaintiff and did not themselves misappropriate trade secret information. As Justice Stevens observed in Bartnicki: "The normal method of deterring unlawful conduct is to impose an appropriate punishment on the person who engages in it. If the sanctions that presently attach…do not provide sufficient deterrence, perhaps those sanctions should be made more severe. But it would be quite remarkable to hold that speech by a law-abiding possessor of information can be suppressed in order to deter conduct by a non-law-abiding third party."[233] Courts have grappled with the private v. public concern distinction in the past, and have managed to apply them with some degree of success. Finally, judges should be able to distinguish between vengeful or anarchistic publishers of trade secrets and those who are genuinely seeking to disclose matters of public concern. To confine First Amendment protections to media defendants only is inconsistent with, among others, *Bartnicki v. Vopper* and *Reno v. ACLU*.

4. A High Probability of Success and of Irreparable Injury Should Be Required to Support Preliminary Injunctions to Stop Disclosure of Information Secrets of Public Concern

To persuade a court to issue a preliminary injunction in trade secrecy cases, plaintiffs must generally show two things: a reasonable probability of success on the merits, and a balance of harms to the parties that tips in favor of the plaintiff. From a First Amendment standpoint, this standard is unproblematic when the trade secrets at issue are "thing" secrets, when the plaintiff seeks only to regulate the defendant's conduct, such as use of information secrets in a competitive manufacturing process, when the injunction pertains to private disclosures of information of private, rather than public, concern.

When plaintiffs are seeking a court order to prevent public disclosures of informational secrets alleged to be of public concern, perhaps courts should require a greater showing of probability of success on the merits (e.g., a strong probability of success) and a showing that the balance of harms tips strongly in favor of the plaintiff or that grave and irreparable harm will result. The *CBS v. Davis* decision provides support for a heightened level of proof of harm before enjoining public disclosure of trade secret information.[234] The Court has also insisted on heightened procedural and substantive standards when the law seeks to impose prior restraints on publication.[235] While some

[233] Id. at 529-30. The Court went on to say: "Although there are some rare occasions in which a law suppressing one party's speech may be justified by an interest in deterring criminal conduct by another, see, e.g., New York v. Ferber, 458 US 747 (1982), this is not such a case." *Bartnicki*, 532 U.S. at 530. The dissent pointed out that a similar rationale to the government's "dry up the market theory" in support of wiretap disclosure laws underlies the regulation of child pornography. Id. at 551-52.
[234] See supra note xx and accompanying text.
[235] See, e.g., Freedman v. Maryland, 380 U.S. 1 (1965)(striking down Maryland motion picture censorship law because it lacked procedural safeguards).

have proposed far more stringent requirements in trade secrecy cases,[236] the heightened standard of proof as to liability and as to harm should suffice to balance First Amendment interests with the private interests at stake in trade secret cases. Moreover, expeditious appellate review should be available when preliminary injunctions are sought against public disclosures of trade secrets alleged to be of public concern, and First Amendment defenses have been raised.[237]

5. Trade Secret Injunctions Should Include Standard Limitations to Comport with First Amendment Principles

It is common for trade secret injunctions to provide that the bar on disclosure of trade secrets by a particular defendant will cease to be in effect if the information becomes public or commonly known in an industry by other means than through the wrongful acts of the defendant.[238] A trade secrecy injunction that fails to include a limitation of this sort may stifle flows of information without clear justification.[239] To be consistent with First Amendment principles, trade secrecy injunctions ought to include provisions allowing the defendants to disclose previously secret information if it has become public or commonly known in an industry other than through their fault.[240]

---

[236] One commentator has recommended adoption of a four part standard before courts issue preliminary injunctions in trade secret cases. Greene, supra note xx, at 553-54. This would involve, first, a presumption against the issuance of a prior restraint, second, proof of serious irreparable harm to the trade secret owner, third, a showing of harm to more than an economic interest to counterbalance the constitutional rights involved, and fourth, a recognition that the public interest favors enforcement of civil liberties. Id. For reasons discussed above, most trade secret cases do not implicate the First Amendment because they regulate private disclosures of information, matters of public concern, and merely enforce contractual or confidential obligations of non-disclosure or enjoin wrongful conduct. Even in cases where First Amendment defenses are plausible, Greene's First Amendment standard is unduly onerous, especially in requiring the plaintiff to show more than an economic interest before a preliminary injunction could issue.

[237] In this respect too, Bunner has been done an injustice. More than three years have passed since the preliminary injunction issued against his posting of DeCSS on the Internet. Although the Court of Appeal ruled that this preliminary injunction was unconstitutional, it remains in effect during the pendency of the case before the California Supreme Court. Even its ruling in his favor would not prevent a stay until U.S. Supreme Court review which might take another two years or possibly more.

[238] See, e.g., Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 474 (1974).

[239] See, e.g., Conmar Products Corp. v. Universal Slide Fastener, 172 F.2d 150 (2d Cir. 1949)(injunction unavailable once trade secrets have been disclosed in a patent)

[240] In view of the considerations discussed in this subsection, the preliminary injunction in *Bunner* is also troublesome from a First Amendment standpoint because it did not contain a limiting provision about Bunner's right to disclose CSS secrets evident from the source code form of DeCSS if this information became public, as indeed it has become (see, e.g., Gallery of CSS Descramblers, supra note xx). Nor was there a provision in the *Bunner* injunction for limiting the duration of the ban on disclosure to a period of time within reverse engineering might take place. Presumably this is because Judge Elving accepted DVD CCA's position that reverse engineering of CSS could not be done lawfully any where in the world because of the web of restrictive licensing agreements that DVD CCA and its predecessors in interest had imposed on their licensees and those licensees imposed on others.

While it may be sound to forbid a misappropriator of trade secrets from publishing the secrets for a reasonable period of time,[241] it is difficult to justify an injunction that forbids that person from disclosing the information for an unlimited duration.[242] At some point, even a misappropriator should be able to speak about information that has become widely known.

It is also common for trade secrecy injunctions to be limited in duration to the time it would take to reverse engineer the secret rather than to misappropriate it.[243] Forbidding the use or disclose misappropriated information for a period that approximates the time it would have taken him or her to reverse engineer the secret is reasonable given that trade secrecy law aims to provide reasonable lead time to innovators, not to give them exclusive property rights of infinite duration in the secrets. Even a misappropriator should be able to disclose the information after the developer of the secret has had a chance to recoup its investment through the passage of time. This too promotes freer flows of information than if the injunction is of indefinite duration. To be consistent with First Amendment principles, trade secrecy injunctions ought also to include provisions permitting defendants to disclose the secret information after the passage of sufficient time for reverse engineering to take place.[244]

Finally, trade secret injunctions should be narrowly tailored so that the end of an unsuccessful collaboration does not result in excluding one of the firms from continuing

---

[241] See, e.g., *McLaughlin*, 2000 WL 48512 at 3 (misappropriators should not be able to escape liability by posting secrets on the Internet); Syntex Ophthalmics, Inc. v. Tsuetaki, 701 F.2d 677 (7th Cir. 1983)(enjoining misappropriator for time necessary to obtain information by proper means).

[242] See, e.g., Religious Technology Center v. Netcom On-line Comm. Services, Inc., 923 F. Supp. 1231, 1256 (N.D. Cal. 1995)("Although Ehrlich cannot rely on his own improper postings to support the argument that the Church's documents are no longer secrets…, evidence that another has put the alleged trade secrets in the public domain prevents RTC from further enforcing its trade secret rights in those materials." It is also difficult to justify a ban on other uses of the trade secret information after the secret has been dissipated because of the acts of third parties, although not necessarily on First Amendment grounds. However, the Supreme Court has upheld contractual obligations to keep paying royalties for previously secret information that later became public after the contract had been made. See, e.g., Aronson v. Quick Point Pencil Co., 440 U.S. 257 (1979).

[243] See, e.g., RESTATEMENT OF UNFAIR COMPETITION, supra note xx, comment f to Sec. 44 at 503 ("[I]njunctive relief should ordinarily continue only until the defendant could have acquired the information by proper means….More extensive injunctive relief undermines the public interest by restraining legitimate competition.")

[244] Most often reverse engineers will not be inclined to disclose publicly the information they have acquired through reverse engineering. After all, the time, money and energy expended in the reverse engineering process will often be substantial, and the reverse engineer will typically want to hold the acquired information as its own trade secret. If the reverse engineer wishes to privately license what it learned from the reverse engineering process as a way of recouping its R&D expenses, it is consistent with U.S. trade secrecy principles to allow this to occur. The EU, however, prohibits private and public disclosures of information obtained in the course of decompilation of computer programs for purposes of achieving interoperability. See Council Directive 91/250 on the Legal Protection of Computer Programs, art. 6(2), 1991 O.J. (L122) 42, 45. This Directive puts at risk authors of books such as ANDREW SHULMAN, ET AL., UNDOCUMENTED WINDOWS: A PROGRAMMER'S GUIDE TO RESERVED MICROSOFT WINDOWS API FUNCTIONS (1992). I would argue that this aspect of the Directive could not be enforced in the U.S. consistent with the First Amendment.

to work in the field. In Southwest Research Institute v. Keraplast Technologies, Ltd.,[245] for example, a Texas appellate court reversed a preliminary injunction that forbade SWRI and its researchers from researching, publishing, or communicating information related to the field of keratin-based technology. This included "without limitation, presentations, interviews, papers, advertisements, electronic or written communication or business inquiries."[246] The injunction also forbade SWRI from filing any patent applications, initiating any tests or research to be performed by third parties, and applying for research grants or submitting contract research proposals to any private enterprise or government."[247] SWRI had done research and development work under contracts with Keraplast for ten years. After a falling out between the firms over intellectual property rights, SWRI undertook its own research projects and Keraplast sued for trade secrecy misappropriation on the theory that "all of the knowledge [SWRI] obtained is proprietary and confidential to Keraplast."[248] The Texas appellate court found the injunction to be impermissibly overbroad, citing free speech considerations as a factor.[249]

V. Conclusion

Trade secret claims are not categorically immune from First Amendment scrutiny, as some have claimed. Nor, however, is the granting preliminary injunctions against disclosures of trade secrets automatically entitled for treatment as classic prior restraints on speech which are presumptively unconstitutional, as others have claimed. This article has explained why the First Amendment is generally not implicated in trade secret cases. When defendants are under contractual or other obligations not to disclose secrets to others, holding them to their promises is generally consistent with the First Amendment. When defendants have misappropriated information, preventing disclosure of wrongfully acquired information is also generally consistent with the First Amendment. Trade secret law is grounded in unfair competition principles, protecting relationships and steering second comers to fair means of acquiring secrets, as by reverse engineering. First Amendment defenses may, however, be successful in exceptional cases, even when defendants are in privity or have wrongfully acquired the information. First Amendment defenses are most likely to succeed as to those who did not participate in misappropriating the information, who acquired the information lawfully, and who seek to make public disclosures as to matters of public concern.

Tensions between trade secrecy law and the First Amendment will not, however, abate even if the principles recommended in the article are widely adopted. Tensions between these legal rules are likely to be exacerbated by efforts of trade secret developers to stop "leaks" of trade secrets through use of mass-market licenses and technological access controls to protect secrets from discovery or disclosure. Courts should take First Amendment principles and other public policy considerations into account when deciding

[245] 2003 Tex. App. 49 (4th Dist. Ct. Ap. 2003)
[246] Id. at 3.
[247] Id.
[248] Id. at 8.
[249] Id. at 6.

whether mass-market licenses or technical controls should override traditional default rules of trade secrecy law, such as the right to reverse engineer a mass-marketed product.

Bunner is an example of a far-reaching claim of trade secrecy protection. In essence, DVD CCA claims an entitlement to control all access to and disclosure of information embedded in millions of mass-marketed products throughout the world. The trade secrecy theory in that case hinges on the enforceability of anti-reverse engineering clauses of mass market licenses which the trade secret claimant had contractually required its licensees to impose on the licensee's licensees.

A similar claim underlies the Edelman v. N2D2 case, which is pending in federal court in Massachusetts. N2D2 is the maker of a filtering software program that is widely used by public schools and libraries, among others, to protect minors from exposure to indecent or otherwise harmful material posted on the Internet. Edelman, a technologist who is skeptical about N2D2's claims of efficacy for this program, wants to reverse engineer it to get information about what sites the software blocks which he regards as critically important to the public policy debate about legislative mandates of filtering software.[250] However, N2D2 makes the program available under a mass-market license that forbids reverse engineering. In addition, N2D2 has used encryption to protect the block-list embedded in the program and claims that reverse engineering the encryption to analyze the block-list would violate the DMCA anti-circumvention rules.[251] Microsoft too has asserted a mixed encryption/mass-market license strategy to impose contractual obligations on those who wanted access to the Kerberos specification for a security system. To get access to this information, users were asked to click on a license that purported to impose a non-disclosure requirement on licensees, and when some clever technologist found a way to bypass the license and get access to the specification, Microsoft claimed that the act of bypassing the license and disseminating information about how to bypass the license violated the DMCA anti-circumvention rules.[252]

In dealing with the emerging challenges to trade secrecy law presented in cases such as *Bunner*, courts must necessarily balance the private interests of trade secret developers who cannot justify investments in innovation if the law does not adequately protect them and the public's interest in promoting flows of information about matters of public concern. Courts must take care to ensure that they do not unwittingly rip trade secrecy law from its roots in unfair competition principles in response to arguments that stronger protection for trade secrets is necessary to protect incentives to invest in innovation. Preserving confidential relationships, respecting contractual obligations, and promoting fair competition should continue to be the mainstay of trade secrecy law. Making trade secret law considerably stronger—converting it, as some recommend, to a strong

---

[250] Edelman was an expert witness in American Library Ass'n v. United States, 201 F.Supp.2d 401 (E.D. Pa. 2002). He studied over- and under-blocking by testing filtering programs against various individual sites. However, this technique provided incomplete analysis of the efficacy of filtering programs.

[251] See American Civil Liberties Union Freedom Network, In Legal First, ACLU Sues Over New Copyright Law, available at http://archive.aclu.org/issues/cyber/Edelman_N2H2_feature.html.

[252] See, e.g., Cohen, supra note xx.

property right[253]—will not only distort free speech and free expression principles discussed in this article, but undermine the competition and innovation policies that underlie intellectual property laws.

VI . A Postscript on the Code-as-Speech Issue in *Bunner*

The California Supreme Court may resolve the *Bunner* case on trade secrecy grounds. The course of least resistance would be to rule that widespread publication of DeCSS on the Internet dissipated the trade secrets, so that even if Johansen had been a misappropriator, CSS secrets revealed in DeCSS are like the proverbial horse that is out of the barn. Or it may decide that the anti-reverse engineering clause of the mass-market license clause in this case is unenforceable. But it took the case to review the Court of Appeal's analysis of Bunner's First Amendment defense. In the body of the article, I have argued that Bunner's First Amendment defense should succeed because he was not himself a misappropriator of CSS secrets, because he acquired DeCSS lawfully, and because his reasons for republishing DeCSS make the secrets the program contains matters of public concern. In this postscript, I will address the code-as-speech component of Bunner's First Amendment defense, an issue which, in my view, is orthogonal to the more conventional First Amendment defense considered in the body of the article.

If the California Supreme Court rules on Bunner's First Amendment defense, the losing party will almost certainly petition the U.S. Supreme Court for certiorari. If the Bunner case goes up to the U.S. Supreme Court, it will require the Court to consider whether source or object code forms of computer programs are protectable by the First Amendment, to what degree, and the level of scrutiny that should be applied to legal rules regulating disclosure, publication, or distribution of programs in either source or object code form. All of these questions would be matters of first impression for the Supreme Court, and they lie at the heart of the First Amendment defense Bunner's lawyers have put forth.

The Supreme Court is more likely to grant certiorari in *Bunner* if the California Supreme Court affirms the Court of Appeal's decision because this result would put the California court in direct conflict with the Second Circuit Court of Appeals' decision in *Universal City Studios, Inc. v. Corley*.[254] The *Corley* decision explicitly took issue with the Court of Appeal's First Amendment analysis in *Bunner*.[255] Like Bunner, Corley

---

[253] Richard Epstein, for example, asserts "[t]he entire edifice of property protection is undermined" if people like Lane cannot be enjoined from posting information on his website which Ford considers a trade secret. Epstein, supra note xx, at 1046. However, trade secrecy law is more limited in its reach than Epstein seems to realize. Trade secrecy law protects relationships and protects against unfair means of acquiring someone's trade secrets. Lane did not violate a contractual obligation to Ford of non-disclosure; he did not have a confidential relationship with Ford; and he did not engage in wrongful acts such as bribery, fraud, or burglary in order to obtain the secret. The leakiness of trade secrecy law is not a "bug" of trade secrecy law, but rather a "feature" which needs to be preserved if trade secrecy law is not to become a super-strong patent of unlimited duration.

[254] 273 F.3d 429 (2d Cir. 2000)

[255] Id. at 452-53.

raised a First Amendment defense in a lawsuit challenging his posting of DeCSS on the Internet. In one key respect, Corley's First Amendment defense is more plausible than Bunner's because Corley is a journalist who posted DeCSS in the course of news coverage on the controversy about this program. Journalists are typically viewed with more favor than non-journalists when they raise First Amendment defenses. In other respects, however, Bunner's First Amendment defense may be stronger than Corley's because Bunner was enjoined prior to trial on the merits on a weak factual record, because his First Amendment defense was ignored by the trial court, and because Bunner posted source code in order to aid the development of an open source DVD player, whereas Corley posted object code.

After trial on the merits, Judge Kaplan enjoined Corley from posting or linking to DeCSS in both source and object code forms. The Second Circuit agreed with Corley that both source and object code forms of computer programs enjoy First Amendment protection,[256] but opined that the functionality of computer programs limited the extent of First Amendment protection accorded to them, and hence affirmed the injunction both as to source and object code.[257] The court did not consider whether there were any significant differences between source and object code forms of programs, although its rationale for limiting First Amendment protection for code is more apt and more persuasive as to object code. Nor did it consider whether there might be communicative purposes for publishing source code, such as those that motivated Bunner. An additional factor causing the Second Circuit to regard DeCSS as entitled to lesser First Amendment protection was because of the dangers that the Internet posed for owners of intellectual property rights.[258]

Computer technologists would likely find it strange, and perhaps even perverse, if courts made a distinction between source and object code. In most respects, these forms of programs are equivalent. And there is, as technologists well know, no absolutely firm way of distinguishing between them, given that it is sometimes possible for source code to be directly executed and given that some humans can read object code. From the standpoint of the First Amendment, however, it may matter whether a person who posts code on the Internet is trying to communicate ideas and information in the program with others in his field or community, or whether the code is being disseminated to enable execution of its functionality. If some defendants in *Bunner* posted DeCSS as part of a protest against the motion picture industry's aggressive assertions of intellectual property rights or in order to educate people about how CSS works, courts might view these postings differently than postings for purposes of encouraging people to use DeCSS to infringe copyrights in DVD movies.

It is difficult to believe the U.S. Supreme Court would analyze the First Amendment issues raised in *Bunner* as superficially as the Second Circuit did in *Corley*. The Court would almost certainly consider relevant differences between source and object code, and would likely decide to treat source code, although perhaps not object code, as First

[256] Id. at 448-49.
[257] Id. at 452.
[258] Id. at 454.

Amendment protected speech.[259] The Court would also be likely to give some weight to the fact that Bunner posted this program on the Internet in order to make information available to aid in the development of a Linux-based DVD player and that others did so in protest against the motion picture industry. The enthusiasm with which the Court embraced the Internet as deserving full First Amendment protection in *Reno v. ACLU*,[260] suggests that the Court would not accept the Second Circuit's view that the Internet is such a dangerous environment that lesser First Amendment protection should be available for Internet publications.

The Supreme Court would likely also notice that the legal claims in *Corley* and *Bunner* are quite different. Corley was charged with violating a law forbidding distribution or "providing" of "technologies" primarily designed to circumvent technical measures, such as CSS, that copyright owners were using to control access to their works.[261] In object code form, DeCSS falls within the reach of the DMCA anti-tool rules, but it is far less clear that source code alone would do so. Bunner was charged with secondary liability for trade secret misappropriation. If Bunner wins on state trade secrecy grounds, the motion picture industry almost certainly challenge any attempt by Bunner to repost DeCSS in source code form on the ground that this would violate the DMCA anti-circumvention rules. Although the Second Circuit enjoined posting of source as well as object code, it did not really address the statutory interpretation issue as to source code, nor as noted above, did it give serious attention to the First Amendment issues posed by source code.

DVD CCA would surely emphasize to the Supreme Court, as it has done in the California courts in *Bunner*, the harm to copyright owners of motion pictures that it asserts would flow from the availability of DeCSS on the Internet. This is an appropriate issue to raise in the context of claims under the DMCA anti-circumvention rules. But it is strange to raise this issue in the context of the *Bunner* case, given that it involves trade secret, not copyright, claims, and given the absence of copyright industry plaintiffs in the case. Yet, the Supreme Court has often been quite attentive to the interests of the copyright industries.[262] The Supreme Court may be reluctant to rule that Bunner has a First Amendment right to post DeCSS on the Internet if it would cause grave harm to this important copyright industry. The Court has never considered whether preliminary injunctions in copyright cases are consistent with its prior restraint decisions, or whether copyright interests are more fundamental than the national security and constitutional interests that it has held to be insufficient to justify prior restraints on speech. The *Bunner* case would provide an opportunity for the Court to address these issues.

---

[259] See, e.g., Lemley & Volokh, supra note xx, at 210(questioning whether object code would qualify for First Amendment protection).
[260] 521 U.S. 844 (1997).
[261] 17 U.S.C. sec. 1201(a)(2).
[262] See, e.g., Eldred v. Ashcroft, 123 U.S. 769 (2003)(upholding Copyright Term Extension Act which extended the duration of existing copyrights as proper exercise of Congressional power under Article I, sec. 8, cl. 8); Harper & Row Pub., Inc. v. Nation Enterp., 471 U.S. 539 (1985)(rejecting fair use and First Amendment defenses to copyright infringement based on The Nation's publication of excerpts from Gerald Ford's memoirs).

It is, of course, possible that the Supreme Court will affirm Bunner's First Amendment right to post DeCSS in source code form on the Internet in order to communicate the ideas and information the program contains with others. Such a ruling would have important implications for any claims that major motion picture studios might bring against Bunner's reposting of DeCSS on the Internet under the DMCA anti-circumvention rules.