

Hastings Law Journal
March, 2007

Articles

***777 PRINCIPLES FOR RESOLVING CONFLICTS BETWEEN TRADE SECRETS AND THE FIRST
AMENDMENT**

Pamela Samuelson [FNa1]

Copyright (c) 2007 UC Hastings College of the Law; Pamela Samuelson

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, [FN1] a faithless employee or former employee, [FN2] an abuser of confidences, [FN3] a trickster who uses deceit or other wrongful means to obtain the secrets, [FN4] or a knowing recipient of misappropriated information who is free-riding on the trade secret developer's investment. [FN5] 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 conduct vis-à-vis the secrets. [FN6]

On rare occasions, defendants invoke the First Amendment as a defense to claims of trade secrecy misappropriation. [FN7] There is no ***778** consensus in the caselaw or law review literature about whether trade secrets are categorically immune (or nearly so) from First Amendment scrutiny and whether preliminary injunctions forbidding disclosure of informational secrets should be considered prior restraints on speech. [FN8] This Article addresses these and related questions and offers a set of principles for mediating the tensions that occasionally arise between trade secrets and the First Amendment.

Part I considers why conflicts between trade secrecy law and the First Amendment have thus far been relatively rare. [FN9] Many trade secret injunctions do not raise First Amendment concerns either because of the nature of the secrets or of the conduct that trade secret law regulates. Various limiting principles of trade secrecy law mediate most free-speech-related tensions likely to arise when someone wants to disclose information that another claims as a trade secret.

Part II suggests that conflicts between trade secret and First Amendment interests may increase in the upcoming years. The increased use of mass-market licenses aimed at maintaining secrecy for information that would otherwise be lawful to acquire and disclose is one source of greater tension. Another arises from proposals to strengthen trade secret rights to safeguard them from threats posed by the Internet. DVD Copy Control Association v. Bunner [FN10] illustrates these trends. If trade secret ***779** rights become stronger, conflicts with free speech interests become more likely. [FN11]

Part III considers the contention that the First Amendment should have no role as a defense in trade secret cases, a view that the California Supreme Court arguably endorsed in Bunner III. [FN12] This Part criticizes,

among other things, the court's reliance on a characterization of trade secrets as property as a reason to reject First Amendment defenses in trade secret cases.

Part IV concludes that preliminary injunctions against disclosure of informational trade secrets should not be treated as prior restraints in ordinary trade secret cases. However, third parties who obtain trade secrets without participating in their misappropriation and who desire to publicly disclose these secrets as newsworthy contributions to public discourse should not be enjoined from such disclosures without satisfying the rigorous First Amendment prior restraints doctrine.

Part V considers several other First Amendment due process issues, such as whether the burden of proof in third party disclosure cases should be higher than in normal trade secret cases and whether appellate review of constitutionally relevant facts should be de novo when First Amendment defenses have been raised.

I. Why Conflicts Between Trade Secret Law and the First Amendment Have Been Rare Thus Far

Courts rarely consider First Amendment implications when issuing preliminary or permanent injunctions to prohibit the use or disclosure of trade secrets because defendants rarely raise the First Amendment as a defense to trade secret misappropriation claims. But why do they not invoke the First Amendment? One reason is because the First Amendment has no application in many trade secret cases. Another is that limiting doctrines internal to trade secrecy law mediate most of the tensions that are likely to arise when persons wish to disclose informational trade secrets that might have First Amendment implications.

***780** A. The First Amendment Often Has No Application in Trade Secret Cases

The First Amendment rarely has application in trade secret cases in part because many trade secrets are “things” that do not implicate First Amendment interests. [FN13] Firms may claim as trade secrets, for example, the molds they use to cast their products, precision tools for refining products within the factory, chemical processes, and the like. [FN14] Injunctions to stop use or disclosure of “thing” secrets generally do not affect First Amendment free speech interests.

Additionally, most trade secret injunctions aim to regulate illegal or unethical conduct. [FN15] Misappropriators may be enjoined, for example, from wiretapping a firm's phones to obtain trade secrets, soliciting customers using misappropriated information, going through a competitor's trash bins to obtain discarded documents, or using deceitful means to access the secret. [FN16] Regulating illegal conduct also does not implicate the First Amendment.

When courts decide whether to issue injunctions against use or disclosure of informational trade secrets, they are, moreover, typically faced with enforcing the agreements under which recipients of the secrets obtained them or the confidential relationships under which the secrets were disclosed to the defendants. Former employees, for example, may be enjoined from disclosing customer lists and other secret information to a new employer. [FN17] Caselaw suggests that injunctive relief to enforce ***781** non-disclosure obligations arising from a contract or deriving from confidential receipt of the information as against competitors is generally consistent with the First Amendment. [FN18]

Insofar as trade secret injunctions aim to stop private use or disclosure harmful to the plaintiff's economic interests, First Amendment interests are less weighty because the secrets are matters of private concern. [FN19]

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' products, training manuals for salespeople, and detailed data about a firm's customers are generally matters in which the public usually has little or no interest. Disclosure of such private information to the public would rarely form sound public policy, advance public discourse, or even be newsworthy. [FN20]

First Amendment interests are more salient in trade secret cases when the defendant's goal is to publicly disclose the secrets. Public disclosure of trade secrets is rare, however, because misappropriators generally have the same interest as the secret's developer in maintaining secrecy as against the public and other industry participants. [FN21] Misappropriators simply want to reuse the other firm's secrets in their own commercial enterprises without paying appropriate license fees or *782 being subject to restrictions that might attend licensed use. Revealing secrets to the public would not only thwart the misappropriator's intent to free-ride on the secret; it would also facilitate detection of the misappropriation and increase the likelihood that the trade secret developer will be able to take effective action against the misappropriator. [FN22]

B. The Limiting Principles of Trade Secret Law Generally Obviate the Need for First Amendment Defenses

Conflicts between trade secret law and the First Amendment have been rare because limiting doctrines of trade secrecy law mediate tensions that might otherwise arise. It has become well-recognized that limiting doctrines of copyright law, such as the idea/expression distinction and the fair use defense, [FN23] mediate tensions that might otherwise arise between copyright interests and the First Amendment. [FN24] Less well-recognized, but equally true, is that the limiting principles of trade secrecy law perform a similar function in mitigating potential conflicts between trade secrets and the First Amendment.

1. Reverse Engineering

Consider, for example, *Chicago Lock Co. v. Fanberg*. [FN25] Chicago Lock alleged that the Fanbergs misappropriated its trade secret key codes when they published a compilation of key code information and offered *783 the compilation for sale. [FN26] The Fanbergs obtained much of the key code information by reverse engineering Chicago locks for customers of their locksmith business, and the rest from other locksmiths who performed similar services. [FN27] Because the Fanbergs 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 Chicago Lock's trade secret claim and against enjoining publication of the Fanberg book. [FN28]

The Ninth Circuit did not find it necessary to invoke the First Amendment in support of this ruling, although an injunction against publication of the Fanberg book would obviously be difficult to justify under the First Amendment. [FN29] The Ninth Circuit did, however, express a constitutional concern about Chicago Lock's claim, saying that if California state trade secret law did not allow the Fanbergs to reverse-engineer Chicago locks and did not allow disclosure of the results of lawful 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 [state] trade secrets law would certainly be preempted by the federal scheme of patent regulation,” [FN30] invoking the Supreme Court's decision in *Kewanee Oil Co. v. Bicron Corp.* [FN31]

2. Preemption as a Check on Trade Secret Law

Kewanee considered the compatibility of trade secrecy and patent law. [FN32] Kewanee sued Bicon for trade secret misappropriation after the latter, founded by former Kewanee employees, began making large crystals very much like Kewanee's and selling them in competition with Kewanee. [FN33] Bicon argued that Kewanee's trade secret claim was preempted by federal patent law and policy. [FN34] In essence, Bicon argued that Kewanee should have gotten a patent for its crystal-making process instead of claiming the process as a trade secret, and courts should not reward Kewanee for failing to seek a patent. [FN35] Trade secret law, in Bicon's view, had created a significant obstacle to achieving important *784 patent policy objectives such as promoting disclosure of significant innovations and limiting the duration of legal protection available to them. [FN36] Kewanee's process was unpatented and, because Kewanee had been using it for several years without seeking a patent, it had become unpatentable. [FN37] Yet, trade secrecy law provided Kewanee with protection for a potentially infinite duration without any quid pro quo of disclosure to justify the grant of legal protection. [FN38] The Sixth Circuit Court of Appeals found Bicon's arguments persuasive; [FN39] the Supreme Court did not.

In concluding that trade secret law was compatible with patent law and policy, the Court focused on weaknesses of trade secrecy law. Trade secrets can easily be lost, not only by reverse engineering, [FN40] but also through accidental disclosure, independent creation by another, use of other proper means to obtain the secret, and all too often by misappropriation. [FN41] "Where patent law acts as a barrier," said the Court, "trade secret law functions relatively as a sieve. The possibility that an inventor who believes his invention meets the standards of patentability will sit back, rely on trade secret law, and after one year of use forfeit any right to patent protection is remote indeed." [FN42] But, as the Ninth Circuit *785 recognized in *Chicago Lock*, federal courts must exercise oversight when state trade secrecy decisions try to "plug" the leakiness of this law, for example, by making it more property-like, to ensure that state law does not interfere with federal intellectual property law objectives.

3. Accidental Disclosure

The leakiness of trade secrecy law is not only important to its compatibility with federal intellectual property law and policy, but also with the First Amendment. In *Religious Technology Center v. Lerma*, [FN43] for example, Religious Technology Center (RTC) sued the Washington Post for trade secrecy misappropriation, alleging that the Post knew or should have known that RTC claimed trade secret rights in certain Scientology texts. [FN44] RTC sought to preserve the trade secret status of the information after litigation documents containing the secrets were filed in court without a protective order. [FN45] RTC sent its agents to the courthouse to block access to the documents, but the Post was able to obtain a copy of the documents from a court clerk. [FN46] The court observed that "[a]lthough the Post was on notice that the RTC had made certain proprietary claims about these documents, there was nothing illegal or unethical about the Post going to the clerk's office for a copy of the documents." [FN47]

The court in *Lerma* did not need to invoke the First Amendment in support of its ruling because an internal limiting principle (or "weakness," to use Kewanee's terminology) of trade secrecy law adequately protected the First Amendment interests of the Washington Post, its reporters, and readers eager to know about Scientology practices. Had the court concluded that the Post's knowledge of RTC's proprietary claim sufficed to establish trade secret liability, the Post could have invoked the First Amendment as a basis for defending against RTC's trade secret claims. [FN48]

*786 4. Limits on Third Party Liability

Another “weakness” in trade secret law that sometimes aids in resolving tensions between trade secrecy law and the First Amendment are its rules on secondary liability. Trade secret law differs from copyright and patent law in that it requires a level of culpability for both primary and secondary liability. [FN49]

Primary transgressors are those who acquired the secret by improper means or who used or disclosed the secret in breach of a contract or a confidence. [FN50] Recipients of misappropriated secrets can be held secondarily liable only if they knew or had reason to know that the information they received from another was acquired by improper means or was subject to non-disclosure requirements under a contract or confidence. [FN51] When third parties are held liable for misappropriation as recipients of stolen trade secrets, it is generally in circumstances in which the third parties have engaged in commercial exploitations of the secrets in competition with the trade secret's developer. [FN52] As a consequence, First Amendment considerations do not arise when such secondary liability is imposed.

Courts are generally careful not to be too hasty in imputing knowledge of misappropriation to third party recipients of secrets. [FN53] In *Cabot Corp. v. Thai Tantalum, Inc.*, [FN54] for example, the Delaware Court of Chancery denied a motion for a preliminary injunction because the plaintiff sought to impute knowledge of the misappropriated secret to a third party recipient based upon the latter's knowledge of a lawsuit that *787 the plaintiff had initiated against the direct misappropriator. [FN55]

Merely knowing that information is claimed as a trade secret does not, moreover, give rise to liability if the information leaked out through no fault of the recipient. In *Lerma*, for example, RTC sought to hold the Post secondarily liable for trade secret misappropriation because the Post knew or ought to have known that information from its Scientology texts that an unnamed party had posted on the Internet for ten days were misappropriated secrets. [FN56] The Post's knowledge of RTC's claim of trade secrecy was irrelevant, however, because the information had been posted on the Internet and had become “effectively part of the public domain, impossible to retrieve.” [FN57] Once again, the limiting principles of trade secrecy law helped to protect the Post's interests in publication without any need to invoke the First Amendment.

Most of the trade secret cases in which First Amendment defenses have succeeded have involved journalists or news organizations who received and then published, or were about to publish, information obtained from persons whom the recipients arguably had reason to know might have misappropriated the secrets. [FN58] This is where First Amendment defenses have the greatest salience as a safeguard against expansive trade secret claims. [FN59]

5. Trade Secret Interests May Be Overridden by Other Societal Interests

Yet another limiting principle of trade secrecy law that minimizes the potential for conflict between this law and the First Amendment is the well-recognized privilege to disclose trade secrets “in connection with . . . information that is relevant to public health or safety, or to the *788 commission of a crime or tort, or other matters of substantial concern.” [FN60] If, for example, a firm considers certain chemicals used in its manufacturing process to be trade secrets, but those chemicals are toxins whose use violates environmental protection laws, the public policy of environmental safety is likely to override the firm's interests in protecting this information as a trade secret. [FN61]

Public policy also appropriately limits the enforceability of agreements between a firm and its employees that forbid disclosure of non-public information about the firm when government agents initiate legitimate inquiries into the firm's business. [FN62] Some state and federal “whistleblowing” statutes privilege disclosures

that might otherwise be regarded as trade secret misappropriations. [FN63] The Restatement of Unfair Competition also recognizes that a firm cannot enforce a contract that information should be treated as a trade secret when it is not, in fact, a secret. [FN64]

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

Conflicts between trade secrets and the First Amendment may become more common because of the increased importance of intellectual property in the U.S. economy in recent decades and the concomitant trend towards strengthening IP rights. As trade secret rights in information get stronger, tensions between trade secret law and the First Amendment are likely to increase. Furthermore, firms are now using mass market license agreements to keep information secret that would be discoverable and potentially disclosable under traditional principles of trade secrecy and IP laws. In addition, some commentators have argued that trade secret law must be strengthened to give greater legal protection to trade secrets because of their vulnerability to misappropriation via the Internet.

*789 A. The Rising Importance and Strengthening of Trade Secrets

As the U.S. economy has become increasingly information-based, the role of intellectual property laws has become important in promoting economic growth and in inducing firms to invest in the development of innovative products and services. [FN65] Firms are now more aware of the benefits of protecting intangible assets and now claim a broader range of non-public information as trade secrets than in the past. [FN66]

Perhaps in part because of the rising importance of intellectual property laws, trade secrecy law has gotten somewhat stronger over time. When *Kewanee* was decided, trade secret law was considered a relatively weak form of protection against certain forms of unfair competition, [FN67] and courts were skeptical of the notion that trade secret developers have “property” rights in their secrets. Today, trade secrecy law is widely perceived as a strong form of legal protection, [FN68] and courts and commentators more commonly refer to trade secrets as “property.” [FN69] The trend toward more expansive intellectual property protection may also indirectly encourage trade secret developers, among others, to make bolder claims than in past decades. [FN70] Together, these developments contribute to an enhanced potential for conflicts between trade secrecy and free speech interests.

B. Use of Mass Market Licenses to Strengthen Protection of Trade Secrets

In the past twenty years it has become increasingly common for firms to try to strengthen trade secrecy protection through mass market license terms that, if enforced, would plug some of the leaks that trade secrecy law would ordinarily allow. [FN71] The use of mass market licenses to *790 forbid reverse engineering has become common in the software industry. [FN72] Although the effort to deter reverse engineering through mass market licenses is mainly of concern because of its impact on ongoing innovation and competition, [FN73] it can also have free speech implications as well, for it can facilitate what some scholars have characterized as the “privatization” of information that would otherwise be public. [FN74] Four examples illustrate this potential.

1. *Edelman v. N2H2*

Benjamin Edelman is a technologist who wanted to reverse engineer a filtering program made by N2H2 that

has been used widely in public schools, libraries, and similar institutions to protect minors from exposure to indecent or otherwise harmful material posted on the Internet. [FN75] Edelman is skeptical about N2H2's claims of efficacy for this program. [FN76] The only effective way for him to find out what sites the program blocks is to reverse engineer the software. [FN77] Edelman believes this information is critically important to an ongoing public policy debate over whether legislatures should mandate use of filtering software in public schools and libraries. [FN78]

However, N2H2 regards the list of sites that its software blocks as a trade secret and only makes its program available under a mass-market license that forbids reverse engineering. [FN79] N2H2 also uses encryption to protect the block-list embedded in this program and claims that reverse engineering the encryption to analyze the block-list would violate the Digital Millennium Copyright Act (DMCA) anti-circumvention rules. [FN80] Edelman sought a declaratory judgment that his intended reverse *791 engineering activity was lawful, but the court dismissed the lawsuit, [FN81] leaving him no choice but to risk substantial liability or give up the effort to test the efficacy of the software. [FN82] This effectively privicized that information.

2. Microsoft and the Kerberos Specification

Microsoft utilized a similar mix of technology and mass-market licensing to try to maintain the trade secrecy status for a specification of a security system known as Kerberos. [FN83] Microsoft posted the specification on a website, but required those who wanted access to the specification to enter into a licensing agreement purporting to impose a non-disclosure requirement on licensees. [FN84] When a clever technologist figured out a way to get access to the specification without clicking "I agree" to the license, Microsoft asserted that the act of bypassing the license and disseminating information about how to bypass the license violated the DMCA anti-circumvention rules. [FN85] Although Microsoft did not pursue litigation against this circumvention after public outcry over this strategy, it was clearly intending to privicize this information.

3. People v. Network Associates

Network Associates included a term in its mass market license forbidding disclosure of benchmarking data (i.e., information about how well the program performed when tested by a customer's engineers) or publication of reviews of its software without the firm's permission. [FN86] Cognizant of the implication of this licensing strategem for free speech and competition policy, the New York Attorney General's office successfully brought suit against Network Associates to compel the firm to drop these provisions from its mass market licenses. [FN87] The public had a *792 legitimate interest in thwarting this attempted privicization of information through a mass market license. Yet, other firms continue to use similar license terms. [FN88]

4. DVD CCA v. Bunner

DVD Copy Control Association (DVD CCA) is a non-profit entity created by major motion picture studios to hold and license certain intellectual property rights in DVD-related technologies. [FN89] As a condition of licensing these rights, DVD CCA required licensed makers of DVD players to install an encryption program known as the Content Scramble System (CSS) in their players to protect DVD movies from unauthorized copying, to undertake various security measures to ensure that CSS remained secret, and to include in licenses with their customers provisions forbidding reverse engineering of CSS. [FN90] DVD CCA believed that the web of licensing obligations it created through these agreements gave it rights to CSS as a trade secret that were, in effect, good against the world. [FN91]

In the summer of 1999, it became known that someone had reverse engineered CSS, and that person or another had written a program known as DeCSS that was capable of decrypting CSS. [FN92] Andrew Bunner was one of hundreds of people who learned about DeCSS from discussions about it on Slashdot and other websites and who decided to post the program on their webpages in late October 1999. [FN93]

Approximately two months later, DVD CCA sued Andrew Bunner, twenty other named individuals, and five hundred John Does for trade secret misappropriation, alleging that Bunner and his co-defendants knew or should have known that a computer program known as DeCSS, which they had posted on their websites, contained or was derived from *793 trade secrets that had been stolen from DVD CCA when someone reverse-engineered CSS in breach of an anti-reverse engineering clause of a DVD player license. [FN94] Bunner claimed a First Amendment right to post this information on the Internet, as well as denying that he was a misappropriator of trade secrets. [FN95]

In granting DVD CCA's motion for a preliminary injunction, the trial judge found that CSS had likely been reverse engineered in violation of a click-through agreement, that DeCSS embodied or was substantially derived from stolen trade secrets, and that Bunner and his co-defendants were liable as co-misappropriators of CSS secrets because they knew or ought to have known DeCSS contained stolen secrets, as witnessed by "various defendants' inclination to boast about their disrespect for the law." [FN96] The judge also took into account the "considerable time, effort and money [that had been spent] in creating the intellectual property at issue in order to protect the copyrighted information contained on DVDs." [FN97] He issued a preliminary injunction forbidding Bunner and his co-defendants from posting or otherwise *794 disclosing DeCSS or CSS secrets. [FN98]

Four years later, DVD CCA's trade secret claim was found to be too weak to support the grant of a preliminary injunction. [FN99] Because DeCSS had been available on hundreds of websites for about two months before DVD CCA commenced the lawsuit and three months before the preliminary injunction issued, the appellate court ruled that it was unlikely that DVD CCA could succeed in showing that any CSS-derived information embodied in DeCSS was protectable as a trade secret. [FN100]

Left for another day was the question whether DVD CCA should be able to use mass market licenses to override the reverse engineering privilege of trade secrecy law and to bind the whole world not to reverse engineer globally distributed DVD players it did not manufacture through multiple layers of license requirements reaching down to the end-user. [FN101]

Had the courts in Bunner been attentive to federal preemption considerations, they might have observed that upholding DVD CCA's claim "would, in effect, convert the [plaintiff's] trade secret into a state-conferred monopoly akin to the absolute protection that a federal patent affords." [FN102] As the Ninth Circuit said in *Chicago Lock*, "Such an extension of California trade secrets law would certainly be preempted by the federal scheme of patent regulation." [FN103] Such an extension of California trade secret law would also increase tensions between trade secret law and the First Amendment, for a reverse engineer of a program such as CSS might want to publish what he learned in a scientific paper. [FN104]

The problem posed by anti-reverse engineering and anti-disclosure terms of mass market licenses is relatively new. For many years, mass *795 market licenses were considered unenforceable as contracts of adhesion or as, at best, proposals for modifications to the contract that users did not accept by acts such as opening the package or installing the software. [FN105] The enforceability of mass market license restrictions on reverse engineering, in particular, has been much debated and not definitively resolved. [FN106] Software and other in-

formation technology developers have supported initiatives to validate these licenses, such as the Uniform Computer Information Transactions Act (UCITA), now in force in Virginia and Maryland. [FN107] UCITA declares that mass market licenses are valid and enforceable so long as users of computer information have manifested assent to the terms by such acts as using the product after notice that it is subject to a license. [FN108] The Federal Trade Commission and a group of state Attorneys General, among others, opposed UCITA out of concern about its impacts on consumers. [FN109]

*796 Although the initiative to promote UCITA has faltered, a new project on software licensing rules is underway. Based on preliminary drafts, it seems likely to validate mass market licenses, although it may be more balanced in regards to consumer interests. [FN110] In the interim, though, serious doubts raised about the enforceability of privity provisions in such licenses may be deterring some firms from being too aggressive in their use. [FN111] This may change if courts show more receptivity to these terms. Greater enforceability of state rules that “plug” the leakiness of trade secret law will enhance the potential for tensions between trade secrets and the First Amendment, as well as with trade secrets and federal intellectual property law.

C. The Internet as a Threat to Trade Secrets

The vulnerability of trade secrets to dissipation by postings on the Internet has been much discussed. [FN112] Commentators agree that tensions between trade secrecy law and the First Amendment increase when defendants raise free speech defenses to misappropriation claims involving Internet postings, although they differ about how courts should respond. [FN113] Those skeptical of First Amendment defenses point out that virtually anyone can become a publisher of information on the Internet, that information published on the Internet has a potentially global audience of millions of people, that anonymous postings may make it difficult to track down misappropriators, and that it may be difficult to quantify losses to trade secret developers or the misappropriators may be *797 judgment-proof. “With the Internet, significant leverage is gained by the gadfly, who has no editor looking over his shoulder and no professional ethics to constrain him.” [FN114] Because Internet disclosure of trade secrets may undermine incentives to invest in innovation and cause harm to industry and society, some commentators have proposed strengthening trade secret rights to respond to the grave dangers that the Internet poses for secrets. [FN115]

Trade secret rights can be strengthened in a number of ways: (1) enforcement of mass market license terms forbidding reverse engineering and disclosure of non-public information about the product, (2) stretching the concept of what is a protectable secret, (3) lowering the level of proof necessary to show that a secondary recipient of the secret should have known the information was a misappropriated secret when receiving it, (4) construing rights in trade secrets as “property” rights, and (5) declaring that trade secret claims are categorically immune from First Amendment challenges.

Bunner I illustrates the willingness to extend trade secret law in order to protect trade secrets against misappropriation on the Internet. Judge Elfving was concerned that unless he enjoined Bunner and others from posting of DeCSS, it would “encourage misappropriators [sic] of trade secrets to post the fruits of their wrongdoing on the Internet as quickly as possible and as widely as possible thereby destroying a trade secret forever. Such a holding would not be prudent in this age of the Internet.” [FN116] His view of Bunner and his co-defendants as intellectual property anarchists [FN117] contributed to his willingness to stretch trade secret law in four ways: (1) by treating the anti-reverse engineering clause of DVD CCA’s mass market license as enforceable as against Johansen and by extension, Bunner and his co-defendants, [FN118] (2) by construing CSS secrets as not having

been dissipated notwithstanding considerable Internet-based discussion about DeCSS and almost three months of postings on hundreds of sites, [FN119] (3) by concluding that Bunner and others must have known that DeCSS embodied DVD CCA's trade secrets *798 based on some bombastic statements by a few of them, [FN120] and (4) by neglecting to mention that Bunner had raised a First Amendment defense to DVD CCA's claims, [FN121] which is tantamount to saying that the First Amendment has no role in trade secret cases.

Posting information on the Internet does not, however, automatically cause it to cease to be a protectable trade secret. If trade secret information is posted on an obscure site on the Internet and the misappropriation is quickly detected, a trade secret developer will generally be able to obtain a court order to take the information down from the Internet site and forbid its reposting. [FN122] This is consistent with 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 sought a protective order. [FN123] Even if a document is publicly accessible on the Internet for some period of time, it will not lose its trade secret status if very few persons have actually seen the information. [FN124]

Of course, 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 the likelihood that its trade secret status will be lost. [FN125] This is unfortunate, but it is a risk inherent to trade secrecy law that information may leak out, particularly if it is susceptible to reverse engineering.

There have been fewer instances of trade secret misappropriation via the Internet than some commentators have predicted. [FN126] As noted *799 earlier, misappropriators of trade secrets typically do not publish the secrets to the world because they want to exploit the secret for their own commercial purposes. Firms can, in fact, take a number of steps to protect trade secrets from Internet misappropriation. [FN127] A significant deterrent to publication of trade secrets on the Internet is the high probability of detection of the misappropriation, and the consequent risk of substantial financial liability for misappropriation and/or criminal prosecution under state laws or the federal Economic Espionage Act. [FN128] The latter seems to have been adequate thus far to deter trade secret anarchists or vengeful persons from posting valuable trade secrets on the Internet.

The Internet certainly poses risks for trade secret developers--as indeed it poses for many other important societal interests (e.g., protecting children from pornography, protecting privacy and copyrights, preventing spam, spyware, 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. Courts in other cases, notably *Reno v. ACLU*, [FN129] have rejected arguments for lesser First Amendment protection for speech on the Internet.

III. Trade Secret Claims and Remedies are Not Categorically Immune From First Amendment Scrutiny

Those who argue that trade secret claims are categorically immune from the First Amendment rely heavily on the characterization of trade *800 secrets as "property," and on caselaw holding that property rights trump the First Amendment. [FN130] Most prominent among the property policy arguments made in support of categorical immunity is the importance of preserving trade secrets from misappropriation in order to preserve adequate incentives to invest in innovation. [FN131] Rights of exclusion are said to be important in trade secrecy as in real property contexts. [FN132] Injunctive relief is perceived as necessary because loss of trade secrecy may cause irreparable harm, damages may be difficult to measure, and defendants may be completely or par-

tially judgment-proof. [FN133]

Because Justice Janice Rogers Brown (now a federal circuit court judge), writing for the California Supreme Court in *Bunner III*, arguably endorsed the property-rights-trump-the-First-Amendment argument, [FN134] this Part will first discuss the court's reasoning and then explain why courts should abjure the property-rights-trump-the-First-Amendment argument in future cases. Countering this argument is a necessary prelude to the set of principles Part IV articulates on the proper role of the First Amendment in trade secret cases.

A. Categorical Immunity in *Bunner*

All three California courts to consider *Bunner's* First Amendment defense made a muddle of it. The trial court did not mention that *Bunner* had raised such a defense, let alone explain why *Bunner's* Internet posting didn't qualify for First Amendment protection. [FN135] The Court of Appeal, by contrast, was so smitten with *Bunner's* First Amendment defense that it initially neglected to consider the substantive weaknesses *801 of DVD CCA's trade secret claim. [FN136] Its First Amendment analysis, moreover, called into question the constitutionality of all preliminary injunctions against disclosure of informational trade secrets, not just the injunction in *Bunner*. [FN137] The California Supreme Court rightly chided the appellate court for neglecting to review the factual record, but then went overboard in the other direction by concluding that as long as plaintiffs made an adequate showing of trade secret misappropriation, preliminary injunctions forbidding disclosure are consistent with the First Amendment. [FN138] Neither extreme is sound law.

Bunner II epitomizes what Professor Richard Epstein has called "First Amendment exceptionalism," [FN139] that is, an overbroad view of the implications of the First Amendment in trade secret cases. In *Bunner II*, the Court of Appeal ruled that DeCSS was First Amendment-protected speech, [FN140] and that the preliminary injunction was "a prior restraint on *Bunner's* First Amendment right to publish the DeCSS program." [FN141] Prior restraints "on pure speech are highly disfavored and presumptively unconstitutional." [FN142] To overcome this presumption, "publication must threaten an interest more fundamental than the First Amendment *802 itself." [FN143] Because DVD CCA's trade secret interest was not more fundamental than the First Amendment, "a preliminary injunction cannot be used to restrict *Bunner* from disclosing DeCSS." [FN144] No exception from the prior restraint doctrine had been recognized for trade secrets, [FN145] and the caselaw upholding preliminary injunctions in copyright cases was inapposite because copyright and trade secrecy involve different statutory frameworks, policy considerations, and constitutional groundings. [FN146]

Microsoft and other firms filed an amicus brief in support of DVD CCA's appeal expressing "alarm[,] that if the lower court's decision is upheld, its consequences will extend well beyond the unlawful publication of trade secrets in this case to include a much broader array of situations in which the intellectual property of American businesses embedded in trade secrets." [FN147] Affirming *Bunner II* would, they asserted, risk making California into "a haven for intellectual property thieves." [FN148] The California Attorney General also submitted a brief arguing for reversal of the Court of Appeal's ruling. [FN149]

It, therefore, came as no surprise that the California Supreme Court reversed the appellate court's First Amendment ruling. Although it agreed with the Court of Appeal that DeCSS was First Amendment-protected speech, "that conclusion still leaves for determination the level of scrutiny to be applied in determining the constitutionality of an injunction prohibiting the dissemination of computer code," which depended on whether the injunction was content neutral or content based. [FN150] Justice Brown construed certain Supreme Court decisions as *803 treating injunctions as content neutral unless they involved government efforts to censor speech

based on its viewpoint. [FN151] She concluded that the injunction in *Bunner* was a content-neutral restraint on speech that passed intermediate scrutiny because trade secrecy law itself was neutral, [FN152] the lower court found that *Bunner* had misappropriated a trade secret, [FN153] trade secrets were property, [FN154] the government had a significant interest in protecting trade secrets, [FN155] and the highly technical nature of the secret made it a matter of only private concern. [FN156]

Bunner III characterizes its holding as “quite limited,” [FN157] and concludes that “the preliminary injunction does not violate the free speech clauses of the United States and California Constitutions, assuming the trial court properly issued the preliminary injunction under California’s trade secrecy law.” [FN158] Insofar as this statement implies that whenever there is an adequate factual basis for issuance of preliminary injunctions in trade secret cases, there is no need to consider free speech interests, I strongly disagree, particularly as applied to third party recipients of misappropriated secrets. [FN159]

Justice Moreno concurred, but expressed strong disagreement with ***804** Justice Brown’s First Amendment analysis. The decisions on which she relied, he pointed out, involved time, place, and manner restrictions on speech, [FN160] whereas the preliminary injunction in *Bunner* “is subject-matter censorship entirely prohibiting *Bunner* from publishing a particular type of information.” [FN161] She had, moreover, failed to consider the availability of alternative venues for communication of this information, which the Court’s time/place/manner precedents require. [FN162] The injunction foreclosed any channel of communication of the information at issue. Yet, Justice Moreno accepted the property characterization of trade secrets and cited approvingly decisions that had “recognized that the First Amendment right to free expression may be legitimately circumscribed by state law intellectual property rights.” [FN163]

The importance of the trade-secrets-as-property-rights argument as a justification for lowering the level of scrutiny in trade secret/First Amendment cases is evident from the more than twenty references to property rights in core parts of Justice Brown’s First Amendment analysis. [FN164] *Bunner III* also approvingly cited two law review articles endorsing the categorical immunity view of trade secrets and the First Amendment, both of which heavily rely on the assertion that trade secrets are property. [FN165]

It is certainly true that some cases have spoken of trade secrets as property, [FN166] that some real property cases have rejected First Amendment defenses raised by trespassers engaged in speech or protest activities, [FN167] ***805** and that certain decisions have opined that there is no First Amendment right to infringe intellectual property rights. [FN168] But other cases challenge the first and third propositions and the second has less force than its proponents are willing to concede.

Part III.B explains why trade secrecy law is better understood as a species of unfair competition law, not as “property” right analogous to land in the trespass cases or even to “true” intellectual property laws, such as patents and copyrights, for the purposes of analyzing First Amendment defenses. Because of its grounding in unfair competition principles, trade secrecy law has a far more limited scope than patents and copyrights, let alone real property. To strengthen trade secret rights so that they become more property-like increases the likelihood of federal preemption as well as of conflicts with the First Amendment.

Part III.C goes on to discuss why, even if one accepts that trade secrets are sometimes treated as “property,” this does not mean that claims for trade secrecy misappropriation are immune from First Amendment scrutiny. There is a more substantial caselaw giving credence to First Amendment defenses in intellectual property cases than the property-rights-trumps-the-First-Amendment view recognizes.

A. Trade Secrets are Not “Property” Akin to Patents, Copyrights or Land

Trade secrecy law emerged as a common law cause of action in the United States in the nineteenth century to provide remedies for two common forms of unfair competition: the use of improper means, such as bribery or deceit, to obtain another's valuable secret, and abuse of a confidence or contract under which another's valuable secrets had been disclosed. [FN169] Regulating improper acquisition of secrets and enforcing confidential relationships continue to be the core interests protected by trade secrecy law. [FN170] This is significantly different from what real property, patent, and copyright laws do.

Justice Holmes famously criticized the “property” characterization for trade secrets in *E.I. du Pont de Nemours Powder Co. v. Masland*:

The word property as applied to . . . trade secrets is an unanalyzed expression of certain secondary consequences of the primary fact that the law makes some rudimentary requirements of good faith. Whether the plaintiffs have any valuable secret or not, the defendant knows the *806 facts, whatever they are, through a special confidence that he accepted. The property may be denied, but the confidence cannot be. Therefore, the starting point for the present matter is not property or due process of law, but that the defendant stood in confidential relations with the plaintiffs. [FN171]

The American Law Institute took a similar view in its 1939 Restatement of Torts:

The suggestion that one has a right to exclude others from the use of his trade secret because he has a right of property in the idea has frequently been advanced and rejected. The theory that has prevailed is that the protection is afforded only by a general duty of good faith and that liability rests upon breach of this duty. [FN172] The more recent Restatement (Third) of Unfair Competition [FN173] does not take a stand on the trade secrets as property debate, but it observes that “[t]he dispute over the nature of trade secret rights has had little practical effect on the rules governing civil liability for the appropriation of a trade secret.” [FN174] Courts may characterize trade secrets as property because the secrets have value, [FN175] but they treat such rights as “effective only against defendants who used or acquired the information improperly.” [FN176]

An important respect in which trade secret law differs from real property and intellectual property laws is that the former does not grant developers any exclusive rights in their secrets, no matter how costly and time-consuming it may have been to develop the secrets or how valuable they are to their developers. Trade secrets are more properly characterized as “nonexclusive rights.” [FN177]

Copyrights and patents, by contrast, are “property” rights because the Constitution explicitly gives Congress power to grant authors and inventors “exclusive rights” in their writings and discoveries, [FN178] and Congress has implemented this constitutional power by explicitly granting qualifying innovators a set of exclusive rights to control certain exploitations of the protected innovations. [FN179] Patentees and copyright holders can exercise the right to exclude unauthorized persons from trespassing upon their rights, just as owners of real property can exclude unauthorized persons from their lands, [FN180] but all trade secret developers *807 can do is sue those who use improper means to get the secrets or breach a contract or confidence. Although trade secret law is sometimes clustered for the sake of convenience under the general rubric of “intellectual property” rights, this does not alter the essential nature of trade secrets as a form of unfair competition.

Insofar as trade secret law evolves to treating intangible interests in information as “property,” the risk grows that trade secret law will come into conflict with federal intellectual property law. Consider, for example,

the secrets at issue in *Bunner*. Copyright law would certainly consider the program CSS to be protectable property insofar as it is an original work of authorship fixed in a tangible medium of expression, [FN181] but the algorithms and data embodied in the program--the very things that DVD CCA claimed that *Bunner* misappropriated--would not be within the scope of property rights provided by copyright law. Copyright law specifically states that “[i]n no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.” [FN182] Facts and data are equally unprotectable elements of copyrighted works. [FN183] U.S. Supreme Court decisions, moreover, have characterized facts, data, and ideas as constitutionally unprotectable subject matters. [FN184] So if state trade secret law proprietizes elements of works that the Supreme Court asserts are constitutionally unprotectable as property, trade secret law may be preempted by federal law as well as being in conflict with the First Amendment. [FN185]

This is not to say that any time a state court refers to trade secrets as property, its statement is constitutionally suspect, but courts should use *808 the “property” word carefully and be specific about the scope of rights under consideration. As Justice Holmes observed almost a century ago, use of the term property to describe trade secrets is generally an “unanalyzed expression.” [FN186]

B. Trade Secrets May Be “Property” for Some Purposes, But This Does Not Immunize Trade Secret Claims from First Amendment Challenges

In *Ruckelshaus v. Monsanto Co.*, [FN187] the Supreme Court observed that trade secrets exhibit some characteristics of property. They can, for example, be assigned, form the res of a trust, and pass to trustees in bankruptcy. [FN188] More importantly, the Court held that trade secrets were eligible for treatment as property for purposes of determining whether government use or disclosure of them was compatible with the Fifth Amendment. [FN189]

Monsanto challenged legislation that authorized the Environmental Protection Agency (EPA) to do two things: (1) look at and make use of studies that Monsanto had submitted to the agency about the safety, efficacy, and environmental impacts of fungicides and pesticides when seeking approval to sell these chemicals in considering competitors' applications for approval to sell chemical equivalents, [FN190] and (2) disclose Monsanto's studies to the public if the EPA deemed such disclosure necessary to address health, safety, or environmental concerns. [FN191] Monsanto considered both rules to be unconstitutional “takings” of its private property. [FN192]

The Court decided that the rules allowing governmental use and disclosure of this trade secret information did not constitute a taking insofar as the government had not specifically promised not to use or *809 disclose the data submitted to the EPA. [FN193] The absence of such a promise meant that Monsanto did not have an investment-backed expectation that its secrets would not be used or disclosed by the EPA for those purposes. [FN194] There was, however, a five-year period in which the statute did promise that trade secret data submitted to the EPA would not be used in assessing competing applications or disclosed to the public. [FN195] Yet, even as to data submitted during this period, the Court went on to rule that the EPA could, in fact, use such data in considering competing applications and disclose the data to the public if necessary to respond to health and safety concerns. Use and disclosure of data submitted in these five years was a taking, but it was a taking for a public purpose. [FN196] Hence, the government could still use or disclose this data as long as it compensated Monsanto. [FN197]

While proponents of the trade-secrets-as-property conception tend to invoke Ruckelshaus as supporting the property concept, [FN198] a fuller review of the Court's ruling demonstrates that trade secret interests are balanced against other societal interests, and sometimes the larger societal interests override trade secret interests. The strong property right theory that Monsanto propounded was soundly trounced in Ruckelshaus. The Court in Ruckelshaus found the public interest in competition and public access to health and safety data more compelling than Monsanto's commercial interests in non-disclosure except insofar as the government explicitly promised during one five-year period not to use or disclose trade secret information submitted to the EPA. [FN199]

The public interest in access to newsworthy information is among the public policies with which courts must occasionally grapple in trade secret cases. In *O'Grady v. Superior Court*, for instance, Apple Computer claimed that there was not and could not be a public interest in access to any of its proprietary trade secrets that O'Grady published on his website. [FN200] The court responded that “[s]urely this statement cannot stand as a categorical proposition.” [FN201] Sometimes “[t]imely disclosure [of trade secrets] might avert the infliction of harm on many *810 thousands of individuals.” [FN202] Merely labeling the secrets as “confidential” or “proprietary” or quoting caselaw characterizing trade secrets as property rights “cannot drain them of compelling public interest.” [FN203] O'Grady involved “not a purely private theft of secrets for venal advantage, but a journalistic disclosure to, in the trial court's words, ‘an interested public.’” [FN204] When both property and free speech interests cannot be accommodated, “it is the quasi-property right that must give way, not the deeply rooted constitutional right to share and acquire information.” [FN205]

Professor Volokh has observed that simply “[c]alling a speech restriction a ‘property right’ . . . doesn't make it any less a speech restriction, and it doesn't make it constitutionally permissible.” [FN206] The First Amendment has an especially important role to play when the question is not where certain speech activities can take place (e.g., on the plaintiff's real property as in the trespass cases), but rather whether certain speech activities can take place at all (e.g., disclosing information claimed as a trade secret to the public). First Amendment defenses have, moreover, been successful in many intellectual property cases, [FN207] *811 including in trade secret cases. [FN208]

Leading intellectual property scholars have argued 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. [FN209] In *Eldred v. Ashcroft*, moreover, the Supreme Court explicitly criticized the D.C. Circuit for its assertion that copyright law is categorically immune from First Amendment challenges. [FN210] This suggests the Court would repudiate a similar theory in respect of trade secrets.

IV. Rethinking the Prior Restraints Doctrine as Applied to Trade Secrets

This Part argues that preliminary injunctions against public disclosure of informational trade secrets may be prior restraints on speech. The heavy presumption against prior restraints is sometimes appropriate in trade secrecy cases, especially those involving third party publishers of newsworthy information misappropriated by a second party.

A. Preliminary Injunctions Forbidding Public Disclosure of Informational Trade Secrets May Be Prior Restraints on Speech

CBS, Inc. v. Davis ruled that a preliminary injunction against public disclosure of informational trade secrets was a prior restraint on speech that bore a heavy presumption against constitutional validity under the First Amendment. [FN211] All but one of the seven reported decisions to have considered this question have agreed with CBS on this point. [FN212]

***812** In CBS, a state court preliminarily enjoined the network from broadcasting or otherwise revealing videotape footage it obtained by persuading an employee of Federal Beef Processors to wear and use undercover camera equipment in the plant during his work shift. [FN213] After learning of CBS's intent to feature this footage in a television news program, Federal sued to enjoin the broadcast, alleging, among other things, that the tape revealed "'Federal's confidential and proprietary practices and processes'" in violation of South Dakota trade secret law and that broadcast of the tape would cause it irreparable injury. [FN214] The South Dakota court granted the preliminary injunction "because the videotape 'was obtained by CBS, at the very least, through calculated misdeeds,'" which made "conventional First Amendment prior restraint doctrine . . . inapplicable." [FN215]

Justice Blackmun granted CBS's motion for an emergency stay of this preliminary injunction so that the broadcast could take place as scheduled, saying: [FN216]

Although the prohibition against prior restraints is by no means absolute, it has been considered acceptable only in "exceptional cases." Even where questions of allegedly urgent national security or competing constitutional interests, we have imposed this "most extraordinary remedy" only where the evil that would result from the reportage is both great and certain and cannot be mitigated by less intrusive measures. [FN217]

Even if "economic harm were sufficient in itself to justify a prior restraint," Justice Blackmun concluded, "speculative predictions" about harm are insufficient. [FN218] Although accepting that the court below was "no doubt . . . correct that broadcast of the videotape 'could' result in significant economic harm to Federal," [FN219] Justice Blackmun was not convinced that this proof satisfied constitutional standards.

Nor did CBS's alleged misdeeds render prior restraints doctrine inapplicable. "Subsequent civil or criminal proceedings, rather than prior restraints, ordinarily are the appropriate sanction for . . . misdeeds in the First Amendment context." [FN220] Had CBS engaged in criminal activity to obtain the videotape, this "could justify an exception to the prior restraint doctrine," he opined, but "the record as developed thus far contains no clear evidence of criminal activity on the part of CBS, and ***813** the court below found none." [FN221]

Justice Blackmun's pronouncements about the applicability of the prior restraint doctrine in informational trade secret cases are particularly notable given that he was among the dissenting justices in *New York Times Co. v. United States* who would have been willing to enjoin the Times' publication of the Pentagon Papers. [FN222] One might thus have expected Justice Blackmun to construe prior restraints doctrine more narrowly than his brethren. Yet, not only did he think the prior restraint doctrine applied, but he also intimated that First Amendment considerations required a more rigorous showing of likelihood of success on the merits and of irreparable harm before issuing preliminary injunctions to stop public disclosure of trade secrets. [FN223]

The CBS case also illustrates the risk of court-enforced private censorship that may lurk in the background of some trade secret cases. Viewed in a light favorably to CBS, one might perceive the plaintiff in CBS as having alleged trade secret misappropriation and sought an injunction in order to avoid embarrassment or other harm to the firm's reputation if a news broadcast raised public awareness about unsanitary or brutal conditions

inside its meatpacking factory. CBS was, in this view, giving the public access to information in which it had a legitimate interest in knowing, not misappropriating trade secrets.

The only decision to have concluded that preliminary injunctions against public disclosure of trade secrets are not prior restraints on speech is the opinion of Justice Brown in *Bunner III*. Although she acknowledged that CBS and other decisions characterized trade secret preliminary injunctions as prior restraints, [FN224] she construed certain subsequent decisions by the Court as limiting the prior restraint doctrine to instances in which the government was attempting to censor speech based on its content. [FN225] Moreover, “[a]s a single Justice order, CBS is *814 arguably not binding on this court.” [FN226] She also distinguished CBS as a case involving weak evidence of misappropriation. [FN227]

Justice Brown's analysis of the prior restraint doctrine and of CBS is simply wrong. Numerous courts, including the California Supreme Court, have characterized preliminary injunctions as prior restraints in cases involving private litigants where there was no contention or danger of governmental suppression of speech. [FN228] The subsequent Supreme Court decisions on which she relied involved time, place, and manner restrictions on speech, not rulings that forbade certain speech altogether, as did the injunction in *Bunner*. [FN229] While Justice Blackmun regarded the evidence of harm in CBS as speculative, [FN230] he did not challenge the lower court's finding about the use of improper means to obtain information Federal claimed as a trade secret. Thus, Justice Brown's analysis is flawed and should not be followed in subsequent cases.

B. A Heavy Presumption Against Issuance of Preliminary Injunctions Should Not Apply in Ordinary Trade Secret Cases

CBS, Inc. v. Davis is a highly unusual trade secrecy case in that: (1) the alleged misappropriator was a news organization, (2) its intent was to broadcast footage containing the alleged secrets, (3) conditions inside meatpacking firms were newsworthy matters of public concern, (4) the *815 harm that might arise from disclosure was speculative, and (5) such harm as occurred would most likely not be attributable to the loss of trade secrets. [FN231]

In ordinary trade secret cases, by contrast, trade secret defendants will be (1) private profit-making firms or individuals who work for or with such firms (2) who intend to make private uses or disclosures of another firm's secrets (3) as to information that is neither newsworthy nor a matter of public concern and (4) who have breached an enforceable contract to maintain secrecy, abused the confidence under which they received another's trade secrets, and/or used improper means, such as bribery or fraud, to obtain the secrets (5) under circumstances likely to give rise to substantial and irreparable harm arising from the defendants' competitive uses of the secret that are not easily monitored. [FN232]

A preliminary injunction is often necessary to protect trade secrets from further misuses and/or to preserve the status quo pending final adjudication of the dispute between the parties. Enjoining disclosure of trade secrets is generally important to preserving adequate incentives for firms to invest in research and development as well as to enforce basic norms of commercial ethics. [FN233] Thus, courts should not apply the prior restraints doctrine in cases involving a confluence of these ordinary trade secret factors. [FN234]

Garth v. Staktek Corp is an example of an ordinary trade secret case in which a First Amendment defense was properly rejected. [FN235] *Garth* *816 was a former participant in a joint venture to develop three-dimensional high-density memory packages for mini- and microcomputer applications who signed an agreement

not to use or disclose information generated and exchanged during the venture unless it had become public domain information. [FN236] Staktek, a successor-in-interest to the joint venture, sued Garth and his new employer for trade secret misappropriation and sought preliminary injunctive relief. [FN237] After finding that Garth violated the non-disclosure agreement by using and disclosing the venture's secrets to his new firm, the trial court granted the motion. On appeal, Garth and the firm argued that the preliminary injunction against further use or disclosure of Staktek's trade secrets was an unconstitutional prior restraint on speech. [FN238]

The Texas Court of Appeals stated that it was well-settled under Texas law that “injunctive relief may be employed when one breaches his confidential relationship in order to unfairly use a trade secret,” [FN239] but recognized that this rule needed to be consistent with the First Amendment and the Texas Constitution. “Texas law begins with the presumption that prior restraints on free speech are unconstitutional,” said the court, but “prior restraints may be permitted to prevent an imminent and irreparable harm, so long as no less restrictive alternative form of protection is available.” [FN240] It added: “Monetary compensation may not sufficiently protect the creator of a new product from unfair competition by those who improperly appropriate confidential information.” [FN241]

Because Garth's firm had attempted to sell the protected technology to other firms, the appellate court agreed that there was irreparable harm from the defendants' pattern of improper uses of the secret and there appeared to be no less restrictive way than a preliminary injunction to ensure that the defendants would not continue to misuse the secrets. [FN242] *Garth v. Statek* exhibits all five characteristics of an ordinary trade secret case that justifies not applying the prior restraint doctrine's heavy presumption of unconstitutionality.

***817 C. In Rare Cases, Preliminary Injunctions Against Public Disclosure of Information Obtained by Wrongful Means or in Breach of Contracts or Confidences Will Be Unconstitutional Prior Restraints**

The Restatement (Third) of Unfair Competition affirms the appropriateness of preliminary injunctions to prevent direct misappropriators of trade secrets from benefiting from their own misconduct. [FN243] *Jerma*, among other cases, endorses this principle. [FN244] In ordinary trade secret cases, wrongful conduct will be an important factor in the issuance of a preliminary injunction. [FN245]

Yet, direct misappropriators of trade secrets have sometimes successfully invoked the prior restraints doctrine. In *CBS*, for instance, Justice Blackmun vacated a preliminary injunction forbidding the network from broadcasting a videotape of meatpacking operations even though the state court found it had been obtained through misdeeds. [FN246] *CBS* thus suggests that courts should not adopt a blanket rule that preliminary injunctions are always appropriate against direct misappropriators who obtained trade secrets by wrongful means.

A factor weighing in favor of preliminary injunctions in cases involving public disclosures of trade secrets in breach of contractual or confidential obligations is the policy that “[p]eople should . . . be required to abide by their own promises.” [FN247] Enforcing contracts “helps preserve the potentially beneficial effects of confidentiality, and it fits our traditional conclusion that people are entitled to voluntarily waive their *818 constitutional rights and to get the benefits that such waivers may provide them.” [FN248] Caselaw can be found in support of this proposition, albeit in dicta. In *State ex rel. Sports Management News, Inc. v. Nachtigal*, for instance, the Oregon Supreme Court observed that the parties had debated “whether the constitution historically would permit a prior restraint on speech . . . if issued against an [A]didias employee, bound to confidentiality, who sought to disclose the alleged trade secrets.” [FN249] The court hinted, without deciding, that such an injunction would be valid.

Cohen v. Cowles Media Co. might initially seem to support this position. [FN250] Cohen sued Cowles Media for damages after he was fired from his job working for a candidate for governor because Cowles's newspapers disclosed, in breach of a promise of anonymity, that Cohen was a key source for a story Cowles published about charges levied against a candidate for lieutenant governor. [FN251] The Court allowed Cohen to proceed with his claims for damages suffered as a result of Cowles's breach of this promise. [FN252] However, nothing in the decision suggests that the Court would have upheld a preliminary injunction against Cowles's publication of Cohen's name because it had promised not to do so. Because the Court was so deeply split (5-4) on whether Cohen could recover damages for breach of this promise, [FN253] it is doubtful that the Court would have upheld a prior restraint on publication of this information by the newspapers. [FN254]

In ordinary trade secrecy cases, persons under contractual or confidential relationship obligations can be preliminarily enjoined from ***819** private disclosure of non-newsworthy secrets without offending the First Amendment because the social context of such disclosures does not implicate First Amendment values. [FN255] Yet, when significant public interests in disclosure are at stake, those who have contracted not to disclose information or who received the information in confidence may sometimes be justified in disclosing it. [FN256] Suppose, for instance, that a former tobacco industry executive revealed in an Internet blog information about trade secret-protected studies conducted by his prior firm that showed harmful health impacts of smoking. [FN257] Disclosure of this information would certainly vitiate the trade secret, and it might also violate a confidentiality agreement between the executive and his firm. The firm might sue the executive for trade secret misappropriation and move for a preliminary injunction to require the executive to take down this posting. A court considering such a motion might invoke *CBS, Inc. v. Davis* and other prior restraints precedents in denying the firm's motion. [FN258]

There may thus be some, albeit rare, circumstances in which a court would and should uphold First Amendment defenses in trade secrecy cases notwithstanding contractual or confidential non-disclosure obligations. It would be odd if courts were more willing to allow trade secrets to be dissipated by those who obtained the information by wrongful means, as in *CBS*, than by those who obtained the information in confidence or under contract, especially since the scope of a contract or of a confidence may not shimmer with clarity.

***820 D. When Third Party Recipients Propose to Disclose Newsworthy Confidential Information, Courts Should Invoke The Heavy Presumption Against Prior Restraints**

Most of the trade secret cases in which First Amendment defenses have been successful have presented a common pattern: (1) a third party journalist and/or news organization obtains non-public information from a second party that it later learns a first party claims as a misappropriated trade secret or confidential information; (2) the third party decides to publish the information because it is newsworthy; (3) because the third party is not bound by any contractual or confidential obligation to the first party (although the second party may be) and did not act in concert with the second party in any misappropriation of the secret, the third party feels justified in publicly disclosing the information; [FN259] (4) the first party then asserts that the third party knew or ought to have known the information was a misappropriated trade secret that should not be or should not have been made public and seeks a preliminary and/or permanent injunction; (5) the journalist and/or news organization then argues that the First Amendment privileges the disclosure.

In *Procter & Gamble Co. v. Bankers Trust Co.*, [FN260] for example, *Business Week* (BW) obtained information pertinent to Procter & Gamble's lawsuit against Bankers Trust (BT) from documents that had been

filed under seal. [FN261] Upon learning of BW's intent to publish a story about it, [FN262] lawyers for both parties immediately went to the trial court requesting a temporary restraining order (TRO) to forbid BW from publishing the information, alleging that it contained trade secrets from documents filed under seal in the case, publication of which would cause irreparable harm. [FN263] The trial court granted the TRO. [FN264] After a hearing to determine the source of the leak, the court determined that BW had knowingly violated the protective order and should therefore be permanently barred from publishing the information. [FN265] The trial court ***821** dismissed concerns about the First Amendment. [FN266]

The Sixth Circuit criticized the trial court for its insensitivity to First Amendment considerations, noting that “‘prohibiting the publication of a news story. . . is the essence of censorship,’ and is allowed only under exceptional circumstances.” [FN267] The trial court “fail[ed] to conduct any First Amendment inquiry before granting the two TROs” and “compounded the harm by holding hearings on issues that bore no relation to the right of Business Week to disseminate information in its possession.” [FN268] Instead of trying to determine the source of the leak, the trial court should have focused on whether Procter & Gamble and BT had shown exceptional circumstances that would justify a prior restraint on publication. [FN269]

In *State ex rel. Sports Management News, Inc. v. Nachtigal*, [FN270] the Oregon Supreme Court overturned a preliminary injunction forbidding Sports Management News (SMN) to publish reports about a new shoe design that Adidas claimed as a trade secret. [FN271] Adidas had only made this trade secret information available to select employees who were bound by confidentiality agreements not to reveal such information. [FN272] It was reasonable to infer that SMN knew that the information had been disclosed in breach of confidence. Yet, the court characterized a lower court order that SMN refrain from publishing any information derived from Adidas proprietary information as a “classic prior restraint” and overturned the lower court's order that SMN submit to the court for its approval any reports about Adidas products prior to publication. [FN273]

***822** In a third such case, *Ford Motor Co. v. Lane*, [FN274] the court denied Ford's motion for a preliminary injunction forbidding Lane from posting information on the Internet about unreleased new automobile designs and other non-public information that Ford claimed as trade secrets. [FN275] Ford argued that Lane knew that Ford employees were obliged not to leak secret information of this sort, therefore Lane knew the information had been misappropriated, and hence, he should be secondarily liable for the misappropriation. [FN276] Yet, because Lane did not have a contractual or confidential relationship with Ford and did not himself misappropriate the information, the court ruled that “Lane's alleged improper conduct in obtaining the trade secrets are not grounds for issuing a prior restraint.” [FN277]

Professor Epstein has criticized Ford as an example of First Amendment exceptionalism. [FN278] “As between the two immediate parties to the dispute,” says Epstein, “the full set of efficiency arguments opts strongly for the protection of trade secrets, given their essential role in modern industry.” [FN279] Lane knew full well that the persons from whom he got Ford's secrets had misappropriated them, and “[h]e decided to publish the trade secrets on his website to retaliate against Ford after a dispute about Lane's right to attend certain Ford trade shows and to use either the Ford trade name or its Blue Oval trademark on his website.” [FN280] The trial judge also was troubled about “whether Lane utilized the power of the Internet to extort concessions or privileges from Ford, by threatening to sell blueprints or other confidential documents.” [FN281]

Yet, it cuts in Lane's favor that he had been providing news about Ford and its designs on his website for some time, and still does. [FN282] Lane's knowledge that the information he published had been divulged in breach of a confidence or contract is not atypical of situations that news organizations routinely face. [FN283]

As Professor Volokh has observed, *823 “Leaks of confidential information are a staple of modern investigative journalism and have helped break many important stories.” [FN284] Courts should be “extremely wary” of deciding what news can and cannot be published. [FN285]

Nevertheless, I agree with Professor Epstein that courts should be careful in trade secret cases not to make too much of the Supreme Court prior restraint decisions, [FN286] especially of the Supreme Court's decisions in *New York Times v. United States* (the Pentagon Papers case) [FN287] or of *Bartnicki v. Vopper*, [FN288] which held that the First Amendment barred a suit for damages against third party publishers of illegally intercepted information. [FN289] Thus, it is well to consider what deference is due to the Pentagon Papers and *Bartnicki* decisions in judging the appropriateness of preliminary injunctions and other relief in trade secrecy cases.

1. *New York Times v. United States*

The facts of the Pentagon Papers case are well-known, but worth briefly restating. 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. [FN290] Ellsberg communicated with personnel at the *New York Times* and *Washington Post* about the documents and arranged for copies of them to be delivered to these newspapers. [FN291] The *Times* and the *Post* spent several months analyzing the documents, and then began publishing excerpts in their newspapers. [FN292] The United States sought to enjoin further *824 publication of excerpts. The Supreme Court ruled, 6-3, that the newspapers could continue publishing the Pentagon Papers over the government's objection. [FN293]

Each member of the Court wrote his own opinion. [FN294] Justices Black and Douglas were convinced that the press must always be free to publish news without prior restraint by the government. [FN295] Justice Brennan accepted that prior restraints were justifiable in an “extremely narrow class of cases,” [FN296] 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.” [FN297] Justices White and Stewart, in contrast, were persuaded that publishing these reports would cause “substantial damage” to U.S. interests, 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.” [FN298] 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 papers. [FN299] He pointed out that Congress had enacted numerous laws to punish those who wrongfully disclosed secret information, yet had refused to enact a law that would have given the Executive Branch authority to proceed against the newspapers in situations such as this. [FN300]

Chief Justice Burger and Justice Harlan, in dissent, were unsympathetic to the newspapers' pleas, in large part because the publishers knew that the documents had been stolen when they obtained them. [FN301] 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. [FN302]

First Amendment exceptionalists perceive the Pentagon Papers case *825 to present four 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 interests. [FN303] *Procter & Gamble Co.*, *Sports Management News*, and

Ford parallel the Pentagon Papers case in these respects. The exceptionalists argue that the economic interests of trade secret owners are less fundamental than the national security interests at stake in the Pentagon Papers case. [FN304] “If a threat to national security was insufficient to warrant a prior restraint in *New York Times Co. v. United States*,” said one court, “the threat to plaintiff’s copyrights and trade secrets is woefully inadequate.” [FN305]

The Court’s more recent First Amendment jurisprudence does not suggest that the Court today would rule differently in a next Pentagon Papers case. Yet, the Pentagon Papers case involved highly respected traditional news publishers, deliberative exercises of editorial judgment, news having a significant bearing on governmental decisions on matters of considerable public concern, and governmental attempts to assert censorial powers over the publication decisions of major newspapers. None of the trade secret/First Amendment cases has presented a similar confluence of peak First Amendment values. Yet, the trade secret cases in which First Amendment defenses have succeeded have involved journalists or news organizations who exercised some editorial judgment in deciding whether to publish information that they had reason to know had been misappropriated. It remains to be seen whether the courts will treat ordinary persons with an Internet connection or a website as eligible for the same First Amendment safe harbor from injunctive relief as in the Pentagon Papers. [FN306]

Several Justices in the Pentagon Papers were willing to accept that proof of grave and irreparable injury would justify a prior restraint. In trade secret cases, sometimes proof of this sort will be available. Several *826 Justices were also 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 statutes that expressly authorize issuance of preliminary and permanent injunctions, and preliminary injunctions are regularly granted in trade secret cases. [FN307]

Bartnicki v. Vopper [FN308] increases my confidence that a majority of the Court would regard as an unconstitutional prior restraint on speech a preliminary injunction against public disclosure of newsworthy secrets by a third party publisher who received the information without fault, even if it had reason to know the secrets had been misappropriated. Trade secrecy interests are important, but they must be weighed against the interests of a free press, among other societal interests. Third party publishers will have weighed the considerable risks of civil and criminal liability for misappropriation in deliberating about whether to publish. Because third party publication of trade secrets will be detectable, those who wrongfully publish trade secrets cannot expect that they will get off scot-free.

2. *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. [FN309] *Vopper*, a radio commentator who had previously been critical of the union, played a tape of the intercepted conversation on a local radio station. [FN310] The tape included talk of blowing up the front porches of homes of the union’s adversaries if the union didn’t get what it wanted. [FN311] The substance of the tape was subsequently republished by other local news media. [FN312]

Bartnicki and *Kane* sued *Vopper* and other media defendants for violating federal wiretap law which makes it illegal to “intentionally disclose [] . . . to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the [illegal] interception of a wire, oral, or electronic communication.” [FN313] They sought actual, statutory, and punitive damages,

as well as attorney fees. [FN314] Through discovery, Bartnicki learned that Vopper had obtained the tape from the head of a *827 local taxpayers' organization, Jack Yocum, who claimed the tape had been left anonymously in his mail box. [FN315] The trial court rejected Vopper's First Amendment defenses because it regarded the wiretap law as a content-neutral law of general applicability that satisfied intermediate scrutiny standards. [FN316] The Court granted certiorari to resolve a conflict among the circuits on First Amendment defenses in wiretap cases, and reversed. [FN317]

The Court did not question that the interception was intentional or that Vopper and his co-defendants had reason to know that the interception was illegal. [FN318] The question was whether it was consistent with the First Amendment to hold them liable for damages for disclosing the illegally intercepted information. [FN319] Justice Stevens, writing for a plurality of the Court, distinguished Bartnicki 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. [FN320]

The wiretap laws are content-neutral and their purpose--to protect the privacy of communications--was unrelated to the suppression of speech. [FN321] Yet, the wiretap law's prohibition on third party disclosure "is fairly characterized as a regulation of pure speech," and "[i]f the acts of 'disclosing' and 'publishing' information do not constitute speech, it is hard to imagine what does fall within that category." [FN322] Justice Stevens invoked several precedents upholding the right of the media to publish *828 certain lawfully obtained truthful information despite knowledge of laws forbidding its disclosure. [FN323] The Bartnicki plurality 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." [FN324] Justices Breyer and O'Connor concurred in the judgment, characterizing the public interest in disclosure in Bartnicki as "unusually high" and the speaker's privacy expectations as "unusually low" because of the threat of potential violence. [FN325]

There were thus six Justices who believed that the First Amendment shielded third party publishers of illegally obtained information from damage lawsuits when the information disclosed was of public concern.

3. Implications

Had the question in Bartnicki been whether the First Amendment would shield Vopper from a preliminary injunction against public broadcast of the contents of the tape, the Court would almost certainly have considered it an unconstitutional prior restraint on speech. After all, six Justices believed that the First Amendment immunized Vopper from damages claims. Less clear, however, is whether the Court would have made the issuance of a preliminary injunction turn on whether the information about to be broadcast was a matter of public concern. [FN326]

*829 Professor Volokh has argued that making the availability of preliminary injunctions turn on whether the information about to be disclosed is a matter of public or private concern would be highly dangerous to a free press, for it calls for "a highly subjective judgment." [FN327] Judicial decisions based on this distinction will "simply reflect [the courts'] judgments about who should win or lose in this case, rather than more prin-

ciplined judgments about the actual value of the speech to the public.” [FN328]

Bunner illustrates the subjectivity of this distinction. Although the California Supreme Court in Bunner III conceded that the secrets “may have some link to a public issue,” it characterized the CSS secrets as matters of private concern because they “convey only technical information about the method used by specific private entities to protect their intellectual property” and because Bunner “did not post them to comment on any public issue or to participate in any public debate.” [FN329] Bunner III asserted that disclosure of CSS secrets “adds nothing to the public debate over the use of encryption software or the DVD industry’s efforts to limit unauthorized copying of movies on DVD’s [sic].” [FN330] Bunner III, however, misconstrued the debate to which Bunner sought to make a contribution.

A U.C. Berkeley computer scientist, whose declaration was offered in support of Bunner’s opposition to a preliminary injunction, explained why access to information about encryption schemes, such as CSS, were matters of public concern:

8. Publication of . . . flaws in supposedly secure systems serves a vital public interest. As our society becomes increasingly dependent on computers, telecommunications, and other information systems, it is important that our critical shared infrastructure be trustworthy and free of systemic security flaws. At the same time, as electronic commerce becomes more prevalent, criminals gain an increasing financial incentive to exploit security vulnerabilities in our critical systems. The vulnerabilities I described above clearly illustrate that the risks are very real: much of our existing infrastructure contains serious security vulnerabilities in its design and implementation, even though this fact may not have been apparent to the public.

. . . .

10. Cryptography is one of the primary means of securing our critical ***830** information infrastructure against attack, and the study of cryptography must, I believe, form an essential foundation for our future information infrastructure. I believe that it is the scientific community’s duty to study these issues and to report on systemic risks that the public at large may not be aware of. One must understand the risks in order to prevent them from recurring.

. . . .

12. Publication and circulation of results is the accepted way to share ideas and advance scientific knowledge about cryptography. It is widely held that the only way to learn how to build secure systems is to be intimately aware of the techniques a typical attacker might use: to be a good codemaker, one must be an accomplished code breaker. Moreover, it is not enough merely to study the theory of code-breaking: it is crucial to understand how real-world security measures are broken in practice, if we wish to build and deploy real security systems. [FN331]

Scholarly works have, in fact, been published on CSS that would have been impossible if CSS stayed secret. [FN332]

Bunner III has been rightly criticized for suggesting that technical information is, by its nature, not of public concern. [FN333] The general public may not be able to understand all of the fine details of encryption technologies, nuclear power plant safety systems, or complex chemical processes, but scientists who assess the implications of these technologies for the security and safety of the public are engaged in discourse on matters of public concern when they publish information about their safety, security, and the like.

Although Bunner IV did not directly challenge Bunner III on the private/public concern distinction, it made some observations that undercut its private concern conclusion:

Well before DeCSS was released on the Internet, a number of people had become interested in unraveling the CSS security system. Users of the Linux computer operating system had organized a forum dedicated to finding a way to override CSS. Apparently DVD CCA had not licensed CSS to anyone making DVD drives for the Linux system, so that computers using Linux were incapable of playing DVD's [sic]. CSS was widely analyzed and discussed in the academic cryptography community As early as July 1999 comments on Slashdot revealed a worldwide interest in cracking CSS. [FN334]

The Court of Appeal, unlike the California Supreme Court, paid attention to reasons that Bunner gave for posting DeCSS on his website. Bunner believed DeCSS would contribute to making DVDs Linux-***831** compatible, and this would make the Linux platform more attractive to consumers and more competitive with Microsoft's platforms. [FN335] Providing source code of DeCSS to the Linux community was, Bunner believed, "an important and effective way to ensure programmers would have access to the information needed to add new features, fix existing defects, and in general, improve the 'deCSS' program." [FN336] Other posters of DeCSS may well have been protesting DVD CCA's effort to protect CSS through multiple layers of license restrictions on reverse engineering. [FN337]

The competitiveness of the Linux platform is obviously not as much a matter of public concern as, say, the war in Iraq. Yet, the U.S. Justice Department brought suit against Microsoft in the 1990s in part to challenge some of its technical design decisions and other practices as anti-competitive as to firms that threatened Microsoft's dominance in the operating system market. [FN338] European authorities similarly charged Microsoft with abuse of its dominant position for its effort to control compatible technologies, including the RealNetworks media player software. [FN339] European authorities also recently came to the United States to investigate whether rival makers of DVD technologies have unduly pressured motion picture studios to adopt one of two rival standards. [FN340] The California Court of Appeal recently gave a spirited explanation of the significance of news about an upcoming Apple Computer product whose publication Apple sought to suppress as a stolen trade secret. [FN341]

Bunner III's characterization of CSS secrets as private matters thus seems more a reflection of who Justice Brown thought should win the case than a well-reasoned analysis of the issue.

When ruling on a First Amendment defense in trade secret cases, courts may wish to consider whether the information about to be disclosed is newsworthy or of public concern. First Amendment interests of speakers are strongest when information meets one of these criteria. Yet, courts should recognize that "peril [is] posed to First Amendment values when courts or other authorities assume the power to declare ***832** what technological disclosures are newsworthy and what are not." [FN342] Newsworthiness may not be the appropriate standard for judging whether someone such as Bunner qualifies for a First Amendment privilege to disseminate information that another claims as a trade secret. [FN343] The focus should instead be on "whether the person seeking to invoke the [First Amendment] privilege' had 'the intent to use material--sought, gathered or received--to disseminate information to the public and [whether] such intent existed at the inception of the newsgathering process.'" [FN344] Under such a test, third party intellectual property anarchists and vengeful former employees would not succeed ***833** with First Amendment defenses for Internet posting of trade secrets, [FN345] although those who disseminated the secrets to promote public awareness and discourse might.

In sum, preliminary injunctions should not issue against public disclosure of trade secrets when four factors are present: (1) the party is being charged with secondary liability for trade secret misappropriation; (2) he or she did not participate in the direct misappropriation and was not in league with any direct misappropriator; (3) although he or she received the information from the direct misappropriator and may know or have reason to

know that it was misappropriated, he or she intends to disseminate the information as news; and (4) he or she does not intend to appropriate the commercial value of the secret in a manner competitive with the trade secret's developer. [FN346]

V. Other First Amendment Implications in Trade Secret Cases

The First Amendment has implications in trade secret cases not only for issuance of preliminary injunctions, but also for a range of other matters, such as whether trade secret disclosers can claim immunity from damage claims, whether trade secret claimants can obtain discovery of communications between third party publishers and those who disclosed trade secret information to them, and how much deference appellate courts should give to trial court findings when First Amendment defenses are raised in trade secret cases, as well as in tailoring injunctive relief for misappropriation.

A. The First Amendment May Require Limits on Damage Awards in Some Trade Secrets Cases

Professors Lemley and Volokh have argued that third party “publication of a trade secret by a party who isn't bound by the contract might be constitutionally protected even against a damages judgment.” [FN347] *834 This may, however, misstate the law and, perhaps, good policy.

Of course, the First Amendment immunity from damage awards in *Bartnicki* is consistent with other notable cases involving public disclosure of misappropriated information. In *Pearson v. Dodd*, for example, the D.C. Circuit affirmed a trial court decision that two newspaper columnists were not liable for violating Senator Dodd's privacy when they published information regarding alleged misdeeds discerned from documents that former employees had misappropriated from Dodd's office. [FN348] *Pearson* is consistent with *Bartnicki*, which also involved media defendants and matters of public concern. [FN349]

Despite Professor Volokh's misgivings about the subjectivity of the public/private concern distinction, [FN350] courts are likely to look to decisions such as *Bartnicki* in deciding that third party publishers of trade secrets should only be immunized from damages liability if the secrets disclosed pertain to matters of public concern. Too broad an immunity from damages liability may give third party publishers too little incentive to think twice about whether to reveal information that they know or have *835 reason to know are claimed as trade secrets. This may be an especially important factor insofar as disclosers of trade secrets are non-media third parties, such as *Bunner*.

In *Dun & Bradstreet, Inc. v. Greenmoss Builders*, for example, the Court rejected a First Amendment defense to damages liability as to non-media defendants. [FN351] *Dun & Bradstreet* (D&B) had sent a credit report to five customers stating that Greenmoss had filed for bankruptcy and had very few assets. [FN352] Greenmoss sued D&B for defamation, alleging that this false report had damaged its reputation; a jury returned a verdict in Greenmoss's favor and awarded compensatory and punitive damages. [FN353] Because it had no actual malice against Greenmoss, D&B claimed that the First Amendment should shield it from liability. [FN354] A majority of the Court disagreed, characterizing D&B as a non-media defendant whose credit reports on Greenmoss's financial situation involved a matter of private rather than public concern. [FN355]

Bunner III seems to suggest that trade secrets are always matters of private concern and that this is another reason that the First Amendment has little or no application in trade secret cases. Justice Brown viewed the

Court as having “expressly declined to extend *Bartnicki* to ‘disclosures of trade secrets or domestic gossip or other information of purely private concern.’” [FN356] She interpreted this declination as “recogniz[ing] that the First Amendment interests served by the disclosure of purely private information like trade secrets are not as significant as the interests served by the disclosure of information concerning a matter of public importance.” [FN357]

This misconstrues *Bartnicki*, which simply found it unnecessary to decide what implications the First Amendment might have for third party disclosures of private matters. *Bartnicki* should not be understood to say that trade secrets are, by their nature, only of private concern. Justice Breyer's concurrence recognized that the law had long recognized a privilege to disclose trade secrets when substantial public interests were *836 at stake. [FN358] Viewed in this light, *Bartnicki* arguably supports a role for the First Amendment in shielding those who disclose trade secrets of public concern (e.g., toxic ingredients in a chemical product) from damage awards. [FN359]

B. First Amendment Interests Should Be Considered When Trade Secret Claimants Litigate to Discover the Source of Leaked Trade Secret Information

While the trade secret/First Amendment case law has thus far focused mainly on whether third party publishers of secrets can be constitutionally enjoined from disclosing them, the identity of the person(s) from whom the publishers obtained the secrets will also be of interest to the trade secret's developer. Courts have only recently considered the First Amendment implications of a trade secret claimant's efforts to get discovery from a publisher who wants to protect its sources.

In *O'Grady v. Superior Court*, the California Court of Appeal ruled that a journalist's interests in protecting his sources outweighed a trade secret claimant's interests in obtaining information about and from the source in discovery, mainly because the trade secret claimant had not exhausted efforts to obtain this information by other means. [FN360] The litigation arose after Jason O'Grady published a series of articles on his eponymous “Power Page” website about a multimedia product (named *Asteroid*) under development at Apple Computer. [FN361] Apple sent O'Grady a cease and desist letter, claiming that the nonpublic information about product development he had posted was a valuable trade secret and directing him to take down this information. [FN362] Apple believed that O'Grady had reason to know the information was a trade secret because much of it came from a slide deck marked “Apple Need-to-Know Confidential.” [FN363]

Apple then brought a trade secret misappropriation suit against a set of “Doe” defendants. [FN364] It also obtained a subpoena to require O'Grady's email service provider to hand over all communications between *837 O'Grady and other persons pertinent to the *Asteroid* product. [FN365] When O'Grady learned of the subpoena, he moved for a protective order against the disclosure of this data. [FN366] The trial court denied this motion because “the publishers had involved themselves in the unlawful misappropriation.” [FN367] The Court of Appeal ruled that the trial court should have issued the protective order, relying principally on a First Amendment-based privilege in journalists to protect the identity of their sources. [FN368]

A threshold question was whether O'Grady qualified for the conditional privilege arising from the constitutional commitment to a free press:

The gist of the privilege is that a newsgatherer cannot to [sic] be compelled to divulge the identities of confidential sources without a showing of need sufficient to overbalance the inhibitory effect of such

disclosure upon the free flow of ideas and information which is the core object of our guarantees of free speech and press. [FN369] The Court of Appeal concluded that there was “no sustainable basis to distinguish [O’Grady] from the reporters, editors, and publishers who provide news to the public through traditional print and broadcast media.” [FN370]

It then applied a five-factor balancing test for deciding whether to require disclosure of source information [FN371] that the California Supreme Court had announced in *Mitchell v. Superior Court*. [FN372] The court considered, first, the nature of, and the journalist’s role in, the litigation at hand. [FN373] The court found significant that O’Grady was not a defendant in the litigation. [FN374] While Apple implied that he might be among the misappropriators of its secrets, this contention was, in the court’s view, “worse than speculative; it contradicts Apple’s own allegations that the Doe defendants are persons unknown to Apple,” adding that it would be a “gross impropriety [to use] the courts and their powers of compulsory *838 process as a tool and adjunct of an employer’s personnel department.” [FN375]

Second, the court considered the cruciality of the information. The identity of the trade secret misappropriator “goes to the heart of its claim,” yet this was offset somewhat “by the possibility that Apple might not identify the putative malefactor even if it obtains the discovery it seeks.” [FN376]

Third, the court considered whether the trade secret claimant had shown exhaustion of alternative sources to get the information sought from the journalist. [FN377] *Mitchell*, the court noted, regarded, “[c]ompulsory disclosure of sources as the last resort.” [FN378] Although Apple had interviewed employees in investigating the source of the leak, it had not interviewed them under oath. [FN379] Genentech’s amicus curiae brief argued that employers in Apple’s situation “should be excused from ‘conduct[ing] a needlessly disruptive and demoralizing internal investigation whenever it detects a theft of trade secrets.’” [FN380] The Court of Appeal was unpersuaded that courts should “relieve the employer of this dilemma by shifting its burdens onto third party journalists” because it would “impair interests of constitutional magnitude.” [FN381]

Fourth, it considered the importance of maintaining confidentiality of the information. [FN382] Apple asserted that there was no public interest in knowing the trade secrets. [FN383] The Court of Appeal disagreed with this assertion both as a “categorical proposition” and as applied to O’Grady’s publication. [FN384] “This case involves not a purely private theft of secrets for venal advantage, but a journalistic disclosure to . . . an interested public.” [FN385]

Finally, the court considered whether Apple had pleaded a prima facie case of trade secret misappropriation. [FN386] “Here it can be reasonably inferred from the circumstances shown by Apple that someone violated a duty not to disclose the information in question, and that the information constituted a trade secret.” [FN387] Even though the second and fifth factors weighed in Apple’s favor, the court concluded that Apple had not made *839 a strong enough showing to obtain discovery of confidential source information. [FN388]

The *Mitchell* factors will obviously play out differently in varying factual contexts, but they provide a sound mechanism for balancing the First Amendment interests of journalists and publishers and those of trade secret claimants in weighing whether confidential source information should be disclosed to trade secret claimants.

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

No consensus exists about the standard of proof that plaintiffs in informational trade secrecy cases should

meet in order to qualify for preliminary injunctive relief. At least three standards have been used or proposed: (1) use of the generally applicable standard for preliminary injunctions, that is, proof of a reasonable probability of success on the merits and a balance of harms to the parties that tips in favor of the plaintiff [FN389]; (2) a somewhat heightened standard when defendants claim First Amendment rights to disclose informational trade secrets [FN390]; and (3) a rigorous four-part standard for all informational trade secrecy preliminary injunctions. [FN391]

First Amendment advocate David Greene proposed the rigorous four-part standard for issuance of preliminary injunctions in trade secrecy cases that would: (1) impose a heavy presumption against the issuance of the injunction as a prior restraint, (2) require proof of serious irreparable harm to the trade secret owner, (3) require proof of harm beyond the claimant's economic interests in the secrets to counterbalance the constitutional interests at stake, and (4) recognize that the public interest favors enforcement of civil liberties. [FN392]

Greene's proposed standard is, however, unnecessarily severe, especially in ordinary trade secret cases. Use of the generally applicable standard for preliminary injunctions against the use or disclosure of trade secrets is unproblematic, from a First Amendment standpoint, when the trade secrets are not being used or disclosed to contribute to public discourse, but are or have been misappropriated for private use or disclosure for purposes of commercial exploitation to the plaintiff's detriment.

***840** In the rare cases in which plaintiffs in trade secret cases seek a preliminary injunction to prevent public disclosures of informational secrets, courts should require a greater showing of probability of success on the merits (i.e., a high probability of success) and a showing that grave and irreparable harm to the trade secret claimant will result from such disclosure. CBS and Procter & Gamble endorse such a heightened standard of proof to justify preliminary injunctions in such circumstances. [FN393] As Justice Blackmun observed in CBS, preliminary injunctions should not issue against public disclosure of trade secret cases, unless "the evil that would result from the [disclosure] is both great and certain and cannot be militated by less intrusive measures." [FN394] This is consistent with other decisions by the Supreme Court requiring heightened procedural and substantive standards when the law imposes prior restraints on publication. [FN395]

Greene is right that the economic interests of trade secret owners should not be given undue weight in cases raising First Amendment defenses and that free speech interests should be part of the balance of harms. But by insisting that there must be proof of harm to interests more fundamental than the constitutional interests in free speech, he underestimates the social interest in adequate protection of trade secrets. If the First Amendment cuts too broad a swath through trade secrecy law, it is not just the immediate economic harm to a trade secret claimant that is at stake, but societal interests in adequate incentives to invest in innovation, maintaining reasonable standards of commercial ethics, willingness to license secrets to others, and costs attributable to greater security measures. [FN396] These interests are of a constitutional dimension as well. [FN397]

As long as trade secret claimants are required to show a high probability of success on the merits and irreparable injury that counterbalances harms to free speech interests, First Amendment values should be adequately protected in those rare cases where trade secret and First Amendment interests are in conflict. [FN398]

***841** D. Appellate Courts Should Conduct De Novo Review When First Amendment Interests are at Stake in Trade Secret Cases

Bunner III holds that appellate courts should undertake a de novo review of the relevant constitutional facts

when defendants raise First Amendment defenses to trade secret misappropriation claims. [FN399] Deferential review of a trial court's findings of fact pertinent to the issuance of a preliminary injunction may be appropriate in an ordinary trade secret case, but such deference is not warranted when free speech and press interests are at stake. [FN400] If the de novo examination leads the appellate court to conclude that the injunction was "improper under California's trade secret law, then it should find that the trial court abused its discretion." [FN401] The California Supreme Court traced this free speech due process principle to the U.S. Supreme Court decision in *Bose Corp. v. Consumers Union of the U.S., Inc.* [FN402] Although *Bose* was a trade libel case, its endorsement of independent appellate review has been applied in a wide array of cases implicating free speech/press interests. [FN403]

Conducting independent appellate review of constitutional facts in such cases serves two purposes: to "prevent[] prejudiced or erroneous deprivation of constitutional rights by fact finders" and "to help prevent future mistakes by making the lines in free speech law clearer and more administrable." [FN404] The *Bunner* case illustrates the importance of such reviews.

The California Supreme Court in *Bunner III* directed the Court of *842 Appeal to conduct an independent review of the factual findings underlying the trial court's issuance of a preliminary injunction against *Bunner's* posting of DeCSS source code. [FN405] On remand, the Court of Appeal found that "DVD CCA presented no evidence as to when *Bunner* first posted DeCSS and no evidence to support the inference that the CSS technology was still a secret when he did so." [FN406] There was, moreover, "a great deal of evidence to show that by the time DVD CCA sought the preliminary injunction prohibiting disclosure of the DeCSS program, DeCSS had been so widely distributed that the CSS technology may have lost its trade secret status." [FN407] The trial court had thus abused its discretion in issuing the preliminary injunction which "burden[ed] more speech than necessary to protect DVD CCA's property interest and was an unlawful prior restraint upon *Bunner's* right to free speech." [FN408]

Both purposes of independent review were served in *Bunner*, for the preliminary injunction against posting of DeCSS on trade secrecy grounds had been erroneously granted on insufficient facts, and future courts might have construed *Bunner* as substantially stretching California trade secrecy law beyond its traditional bounds had the trial court's findings not been closely scrutinized by the appellate court. [FN409] Trial courts in future cases may be more likely to be more careful with fact-finding in similar cases because the Court of Appeal so forcefully explained deficiencies in the factual record and why the preliminary injunction should not have issued.

E. Injunctions in Informational Trade Secret Cases Should Include Standard Limitations to be Consistent with First Amendment Principles

Trade secret injunctions, whether preliminary or permanent, often provide that if the protected information becomes public or commonly known in an industry by means other than wrongful acts of the defendant, he or she will then be free to disclose the secrets as well. [FN410] Some injunctions, however, do not contain this limitation. [FN411] A trade *843 secrecy injunction that fails to include such a limitation will stifle the free flow of information without adequate justification. [FN412] 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. [FN413] To the extent they do not so provide, courts reviewing such injunctions ought to read such a limiting term into the order to comport with First Amendment principles.

The Restatement of Unfair Competition opines:

If 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. [FN414] Injunctions against use or disclosure of informational trade secrets should also generally be limited in duration. Forbidding the use or disclosure of misappropriated information for a period that approximates the time it would have taken the defendant to reverse engineer or otherwise obtain the information by proper means is reasonable given that trade secrecy law aims to provide reasonable lead time to innovators, not to give them perpetual exclusive property rights in the secrets. [FN415] Consistent with this principle, courts typically enjoin use or disclosure of protected secrets for a reasonable period of time, such as the amount of time it would take another person or firm to obtain the secret by reverse engineering. [FN416] The Restatement (Third) of Unfair Competition endorses such limitations on trade secret injunctions. [FN417] Yet, not all trade secrecy injunctions are so limited. [FN418] It is difficult to justify *844 on First Amendment as well as trade secrecy policy grounds an injunction that forbids use or disclosure of the information in perpetuity. [FN419]

Courts should also be wary of enjoining reverse engineering of trade secrets. Because reverse engineering is an essential part of ongoing innovation, even misappropriators should be able to reverse engineer lawfully obtained products in order to obtain access to the protected secret and other information during the term of the injunction, or at least to establish a "clean room" to conduct reverse engineering to obtain the secrets in a lawful manner, including ones he or she previously misappropriated. [FN420] If the subject matter being reverse engineered is computer program code, a reverse engineer arguably has a First Amendment right to reverse-analyze the code, [FN421] at least in the absence of a valid contractual restriction on reverse engineering, [FN422] and to make use of that information or disclose it.

Reverse engineers will generally be disinclined to publicly disclose information they have acquired through reverse engineering. Because reverse engineering requires expenditure of considerable time, money, and energy, the reverse engineer will typically want to maintain 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 research and development expenses, it is consistent with U.S. trade secrecy principles and arguably with First Amendment principles as well to allow this. [FN423] If the information was *845 lawfully reverse-engineered, the reverse engineer should also be free to publish it as a matter of First Amendment as well as trade secrecy law. [FN424]

Finally, trade secret injunctions should be narrowly tailored so that the termination of an unsuccessful collaboration does not result in barring former collaborators from continuing to work in the field. In *Southwest Research Institute v. Keraplast Technologies, Ltd.*, [FN425] a preliminary injunction unduly restricted the First Amendment interests of researchers. Southwest Research Institute (SWRI) had performed research and development work under contracts with Keraplast for ten years. [FN426] After a falling out between the firms over intellectual property rights, SWRI undertook independent research projects in this field. [FN427] Keraplast sued for trade secrecy misappropriation on the theory that "all of the knowledge [SWRI] obtained is proprietary and confidential to Keraplast." [FN428] The injunction forbade SWRI and its researchers from conducting further research, publishing, and otherwise communicating information related to the field of keratin-based technology. [FN429] This included, "without limitation, presentations, interviews, papers, advertisements, electronic or written communication or business inquiries." [FN430] The injunction also forbade SWRI from filing patent applic-

ations in this field, 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.” [FN431] The Texas appellate court found the injunction to be impermissibly overbroad, citing free speech considerations as a factor. [FN432] Other courts should follow the Texas appellate court's example in reviewing the breadth of injunctions to ensure that they do not unduly encroach on First Amendment rights.

Conclusion

This Article has taken a middle ground between two extreme positions. One such extreme is that trade secret claims are categorically immune from First Amendment scrutiny because trade secrets are “property” and enforcing these property rights is necessary to provide adequate incentives to invest in innovation. The other extreme is that preliminary injunctions against disclosures of trade secrets are presumptively unconstitutional prior restraints on speech and should *846 rarely if ever issue.

The middle ground recognizes that the First Amendment is not generally 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 because private uses and disclosures of trade secrets do not contribute in a meaningful way to public discourse.

But First Amendment defenses to trade secret claims should be taken seriously when raised by those who did not participate in misappropriating the information, who acquired the information lawfully, and who seek to make public disclosures of newsworthy information to contribute to public discourse. In exceptional cases, preliminary injunctions may conflict with First Amendment rights, even when defendants are in privity or have wrongfully acquired the information, as long as the speaker also aims to disclose secrets in order to promote public discourse. Preliminary injunctions that forbid public disclosure of trade secrets when disclosure would promote such discourse are prior restraints on speech that should bear a heavy presumption against constitutionality.

While much of this Article's analysis focused on when to treat preliminary injunctions in trade secret cases as prior restraints, it has offered several other principles to mediate and mitigate the tensions that occasionally arise between trade secrecy law and the First Amendment. First, it identified some circumstances in which trade secret disclosers should be immune from damage liability on First Amendment grounds. Second, it endorsed use of a First Amendment-sensitive balancing test for determining when to order third parties to disclose the identity of second party misappropriators. Third, it showed why courts should require heightened standards of proof when defendants raise appropriate First Amendment defenses to preliminary injunctive relief in trade secret cases. Fourth, it agreed with Bunner III that appellate courts should conduct de novo appellate review of constitutionally relevant facts in First Amendment-trade secret cases. Fifth, it argued that courts should consider First Amendment values carefully when crafting the scope of injunctive relief in trade secret misappropriation cases.

Finally, the Article explained why courts should be wary of efforts by 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 whether mass-market licenses or technical controls should override traditional default rules of trade secrecy law, such as the right to reverse *847 engineer a mass-marketed product.

Despite dire predictions of some commentators, trade secrets are surviving the challenges of the Internet age. Courts are able to 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 the flow of information about matters of public concern. Courts should 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 property right [FN433]--will not only distort free speech and free press principles, but undermine the competition and innovation policies of intellectual property laws.

[FN1]. Richard M. Sherman Distinguished Professor of Law and Information, University of California at Berkeley. This paper was supported by NSF Grant No. SES-9979852. It is a derivative work of a draft article entitled "Resolving Conflicts Between Trade Secrets and the First Amendment" posted on my website in March 2003 that has been cited in some articles published since then. I wish to thank Julie Cohen, Rebecca Eisenberg, Howard Freedland, Tait Graves, Paul Heald, Eddan Katz, Mark Lemley, David McGowan, Kurt Opsahl, Robert Post, Jason Schultz, Eugene Volokh, and participants in workshops at Boalt Hall and University of Michigan and Georgetown University Law Schools for insightful comments on an earlier draft of the paper.

[FN1]. See, e.g., *Union Carbide Corp. v. Exxon Corp.*, 77 F.3d 677, 678-79 (2d Cir. 1996); *Tracer Research Corp. v. Nat'l Env'tl. Servs. Co.*, 42 F.3d 1292, 1293 (9th Cir. 1994).

[FN2]. See, e.g., *Comprehensive Tech. Int'l. v. Software Artisans, Inc.*, 3 F.3d 730, 732 (4th Cir. 1993); *SI Handling Sys. v. Heisley*, 753 F.2d 1244, 1251 (3d Cir. 1985).

[FN3]. See, e.g., *Smith v. Snap-On Tools Corp.*, 833 F.2d 578, 579 (5th Cir. 1987); *Roberts v. Sears, Roebuck & Co.*, 573 F.2d 976, 978 (7th Cir. 1978).

[FN4]. See, e.g., *Telex Corp. v. Int'l. Bus. Machs. Corp.*, 510 F.2d 894, 897 (10th Cir. 1975); *Univ. Computing Co. v. Lykes-Youngstown Corp.*, 504 F.2d 518, 528 (5th Cir. 1974).

[FN5]. See, e.g., *Metallurgical Indus., Inc. v. Fourtek, Inc.*, 790 F.2d 1195, 1197-98 (5th Cir. 1986); *Data Gen. Corp. v. Grumman Sys. Support Corp.*, 834 F. Supp. 477, 481 (D. Mass. 1992).

[FN6]. Parts I.A and IV.B explain why trade secret cases generally do not pose First Amendment concerns.

[FN7]. See, e.g., *CBS, Inc. v. Davis*, 510 U.S. 1315, 1315 (1994). The First Amendment trade secrecy cases are discussed *infra* Part IV.

[FN8]. The commentator who most clearly adopts the categorical immunity position is Andrew Beckerman-Rodau. Andrew Beckerman-Rodau, *Prior Restraints and Intellectual Property: The Clash Between Intellectual Property and the First Amendment from an Economic Perspective*, 12 *Fordham Intell. Prop. Media & Ent. L.J.* 1, 5 (2001) ("[T]rade secrets, despite any expressive component, should be treated as property that falls outside the domain of the First Amendment."); see also Bruce T. Atkins, *Trading Secrets In the Information Age: Can Trade Secret Law Survive the Internet?*, 1996 *U. Ill. L. Rev.* 1151, 1151 (arguing for strengthening trade secret rights to ensure that they are adequately protected against Internet exposure); Richard A. Epstein, *Privacy, Publication,*

and the First Amendment: The Dangers of First Amendment Exceptionalism, 52 *Stan. L. Rev.* 1003, 1006 (2000) (critical of caselaw in which First Amendment defenses have been successful); Adam W. Johnson, *Injunctive Relief in the Internet Age: The Battle Between Free Speech and Trade Secrets*, 54 *Fed. Comm. L.J.* 517, 536 (2002) (offering a three-part test for balancing trade secret and First Amendment interests that weighs heavily in favor of trade secret owners); Franklin B. Goldberg, *Recent Developments: Ford Motor Co. v. Lane*, 16 *Berkeley Tech. L.J.* 271, 271 (2001) (questioning decisions applying the prior restraint doctrine of the First Amendment in trade secret cases). At the opposite end of the spectrum is David Greene. David Greene, *Trade Secrets, the First Amendment and the Challenges of the Internet Age*, 23 *Hastings Comm. & Ent. L.J.* 537, 552-55 (2001) (proposing four-part test for preliminary injunctions heavily weighted in favor of First Amendment interests); see also Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 *Duke L.J.* 147, 229-31 (1999) (preliminary injunctions in trade secret cases may raise serious First Amendment concerns); Eugene Volokh, *Freedom of Speech and Intellectual Property: Some Thoughts After Eldred*, 44 *Liquormart*, and *Bartnicki*, 40 *Hous. L. Rev.* 697, 739-48 (2003) (criticizing recent caselaw analyzing First Amendment defenses in trade secret and wiretap cases).

[FN9]. See, e.g., Roger M. Milgrim, *Milgrim on Trade Secrets* §12.06 (2002) (noting that First Amendment defenses have been rare in trade secret cases).

[FN10]. See *DVD Copy Control Ass'n v. McLaughlin*, No. CV 786804 2000, 2000 WL 48512 (Super. Ct. 2000), rev'd sub nom. *DVD Copy Control Ass'n v. Bunner*, 113 *Cal. Rptr. 2d* 338 (Ct. App. 2001), rev'd, 75 P.3d 1 (Cal. 2001), on remand to 10 *Cal. Rptr. 3d* 185 (Ct. App. 2004). For the sake of simplicity, textual and footnote references to this case will be designated, with respect to the trial court decision as *Bunner I*, the first Court of Appeal decision as *Bunner II*, the California Supreme Court decision as *Bunner III*, and the Court of Appeal on remand as *Bunner IV*.

[FN11]. Cf. Neil Weinstock Netanel, *Locating Copyright in the First Amendment Skein*, 54 *Stan. L. Rev.* 1, 2-7 (2000) (arguing that tensions between copyright and the First Amendment have increased as the scope of copyright protection has increased).

[FN12]. See 75 P.3d 1, 13-18 (2001) (holding that the significant government interest in trade secrets justifies a content-neutral injunction restraining First Amendment rights).

[FN13]. Flags and draft cards are, of course, "things," and conduct as to such things is sometimes protected by the First Amendment, as when flags are burned in protest against government policies. See, e.g., *Texas v. Johnson*, 491 U.S. 397, 420 (1989) (affirming reversal of conviction for flag desecration in protest of government policies on First Amendment grounds). As Robert Post has observed, the First Amendment may be implicated when the law regulates things that are integral parts of a medium through which First Amendment values are expressed in social interactions. See, e.g., Robert C. Post, *Encryption Source Code and the First Amendment*, 15 *Berkeley Tech. L.J.* 713, 715-17 (2000). Use and disclosure of thing-trade secrets do not implicate First Amendment medium interests.

[FN14]. The definition of trade secrets in the Restatement of Torts §757 cmt. b (1939) emphasizes "thing" secrets. A trade secret may consist of any formula, pattern, device, or compilation of information which is used in one's business, and which gives one an opportunity to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers. Generally it relates to the production of

goods, as, for example, a machine or formula for the production of an article. *Id.*

[FN15]. Conduct such as flag burning can, of course, be First Amendment protected (e.g., when done in protest of governmental policies). See, e.g., *Johnson*, 491 U.S. at 420. However, the kinds of conduct typically regulated by trade secret injunctions (e.g., against use of a particular chemical in a production process or forbidding bribery of a trade secret developer's employees or licensees) are not expressive in a First Amendment sense.

[FN16]. See, e.g., Restatement (Third) of Unfair Competition §43 (1993) (giving theft, fraud, unauthorized interception of communications, inducement of or knowing participation in a breach of confidence as examples of improper means to acquire a trade secret).

[FN17]. See, e.g., *Flotec, Inc. v. S. Research, Inc.*, 16 F. Supp. 2d 992 (S.D. Ind. 1998) (enjoining former employee from disclosure of previous employer's trade secrets to new employer); *Cybertek Computer Prods., Inc. v. Whitfield*, 203 U.S.P.Q. 1020 (Cal. App. Dep't Super. Ct. 1977) (similarly enjoining former employee).

[FN18]. See *infra* notes 233-42 and accompanying text. Most such injunctions forbid private uses and disclosures of the secret or confidential information in a manner that would breach the contract or confidence. When defendants intend to make public disclosures of the secrets and the secrets are newsworthy or otherwise of public concern, First Amendment considerations have greater weight.

[FN19]. Of course, the First Amendment can sometimes protect private disclosures as to matters of private concerns. A city ordinance that forbade residents to gossip about private matters would surely be unconstitutional under the First Amendment notwithstanding the fact that it concerned only private disclosures of private matters. The inevitable disclosure doctrine of trade secret law may also be incompatible with the First Amendment, particularly at a preliminary injunction stage. See *Lemley & Volokh*, *supra* note 8, at 232. Such cases typically involve injunctions against private disclosures, not public ones, as to matters of private concern. First Amendment concerns may, however, be adequately accommodated in inevitable disclosure cases as long as courts use this doctrine sparingly (e.g., where direct or circumstantial evidence indicates a high degree of likelihood of misappropriation and of irreparable harm), successful plaintiffs are required to subsidize their former employees during the period in which the injunction operates, and the duration of the injunction is short. See, e.g., *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1272 (7th Cir. 1995) (enjoining the defendant from working for the competitor for one month); *Lumex, Inc. v. Highsmith*, 919 F. Supp. 624, 636 (E.D.N.Y. 1996) (enjoining the defendant from working for the competitor for a period of up to six months). California courts have rejected the inevitable disclosure doctrine. See, e.g., *Schlage Lock Co. v. Whyte*, 125 Cal. Rptr. 2d 277, 281 (Ct. App. 2002).

[FN20]. The distinction between public and private concerns as it pertains to First Amendment trade secret claims is discussed *infra* notes 60-64 and accompanying text.

[FN21]. See *Bunner IV*, 10 Cal. Rptr. 3d 185, 195 (Ct. App. 2004) (the typical defendant in a trade secrecy case “has as much interest as the plaintiff has in keeping the secret away from good faith competitors and out of the public domain”).

[FN22]. See, e.g., *Epstein*, *supra* note 8, 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 trade secret to any other firms in the industry.”).

[FN23]. See 17 U.S.C. §102(b) (2000) (“In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or is embodied in such work.”); *id.* §107 (setting forth factors for determining fair use as a defense to infringement claims).

[FN24]. See, e.g., *Eldred v. Ashcroft*, 537 U.S. 186, 218-22 (2003) (holding that Copyright Term Extension Act did not violate the First Amendment); *Harper & Row Publishers v. Nation Enters.*, 471 U.S. 539, 559-60 (1985) (holding that the “fair use” defense is not strengthened or diminished by the importance of the work). Some classic scholarly articles articulate the internal limits of copyright as adequately accommodating First Amendment interests. See, e.g., Paul Goldstein, *Copyright and the First Amendment*, 70 *Colum. L. Rev.* 983 (1970); Melville B. Nimmer, *Does Copyright Abridge First Amendment Guarantees of Free Speech and Press?*, 17 *UCLA L. Rev.* 1180 (1970). These articles championed a view, accepted in *Eldred* and *Harper & Row*, that the idea/expression distinction and fair use accommodated tensions between copyright and the First Amendment. Many articles, however, take a more expansive view of the First Amendment as a constraint on the scope of copyright. See, e.g., Yochai Benkler, *Free As the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 *N.Y.U. L. Rev.* 354 (1999); Michael D. Birnhack, *Copyright Law and Free Speech After Eldred v. Ashcroft*, 76 *S. Cal. L. Rev.* 1275 (2003); Lemley & Volokh, *supra* note 8; Lawrence Lessig, *Copyright's First Amendment*, 48 *UCLA L. Rev.* 1057 (2001); Glynn S. Lunney, Jr., *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, 87 *Va. L. Rev.* 813 (2001); Netanel, *supra* note 11; Volokh, *supra* note 8.

[FN25]. 676 F.2d 400 (9th Cir. 1981).

[FN26]. *Id.* at 402-03.

[FN27]. *Id.* at 404.

[FN28]. *Id.* at 404-05.

[FN29]. See *Post*, *supra* note 13, at 718 (books are a medium of communication “unambiguously covered by the First Amendment”).

[FN30]. *Chicago Lock Co.*, 676 F.2d at 405.

[FN31]. 416 U.S. 470 (1974).

[FN32]. *Id.* at 473-74.

[FN33]. *Id.*

[FN34]. *Id.*

[FN35]. For a more detailed account of Bicon's argument, see the Sixth Circuit's decision in *Kewanee Oil Co. v. Bicon Corp.*, 478 F.2d 1074 (6th Cir. 1973), *rev'd*, 416 U.S. 470 (1974).

[FN36]. The Supreme Court had earlier ruled that state law is preempted when it creates an obstacle to achieving objectives of patent law. See *Sears, Roebuck & Co. v. Stiffel Co.*, 376 U.S. 225, 232-33 (1964) (liability for copying of lamp designs under state unfair competition preempted by federal patent law because the designs

were unpatented); *Compco Corp. v. Day-Brite Lighting, Inc.*, 376 U.S. 234, 238-39 (1964) (accord). Justices Brennan and Douglas dissented in *Kewanee* on the ground that the decision “is at war with the philosophy” of *Sears and Compco*. *Kewanee*, 416 U.S. at 495 (Douglas, J., dissenting) (“[E]very article not covered by a valid patent is in the public domain.”).

[FN37]. *Kewanee* had used the process internally for several years, and was thus ineligible for a patent on it under 35 U.S.C. §102(b). *Kewanee*, 416 U.S. at 474.

[FN38]. *Kewanee*, 416 U.S. at 496 (Douglas, J., dissenting) (“By a patent, which would require full disclosure, [Kewanee] could have obtained a 17 year monopoly against the world. By the District Court's injunction, which the Court approves and reinstates, [it] gets a permanent injunction running into perpetuity against respondents.”).

[FN39]. See *Kewanee Oil Co. v. Bicron Corp.*, 478 F.2d 1074, 1086 (6th Cir. 1973). The Court of Appeals ruled that the trial court's findings of fact as to the misappropriation claim were not clearly erroneous and “it was evident from the record that the individual Respondents appropriated to the benefit of Bicron secret information on processes obtained while they were employees” of *Kewanee's* predecessor in interest. *Kewanee*, 416 U.S. at 474.

[FN40]. See, e.g., *James Pooley, Trade Secrets* §5.02[1] (2006) (asserting that most trade secrets are reverse engineered). The Court was even clearer about the constitutional significance of reverse engineering in *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, which struck down a Florida unfair competition law that the Court construed as outlawing the most efficient means of reverse engineering an unpatented product, namely using a plug-mold to make a competing boat hull. 489 U.S. 141, 160 (1989). Reverse engineering, said the Court, is “an essential part of innovation,” likely to yield insights and variations on products that “may lead to significant advances in the field.” *Id.* Moreover, “the competitive reality of reverse engineering may act as a spur to the inventor” to develop further patentable ideas. *Id.*

[FN41]. *Kewanee*, 416 U.S. at 489-90.

[FN42]. *Id.* at 490. Justice Marshall was not persuaded that this prospect was “remote indeed,” but he concurred in the judgment on the ground that patent and trade secret law had a long history of co-existence, and Congress was well aware of this. *Id.* at 494.

[FN43]. 908 F. Supp. 1362 (E.D. Va. 1995).

[FN44]. *Id.* at 1364-66.

[FN45]. *Id.*

[FN46]. *Id.*

[FN47]. *Id.* at 1369. Documents containing the secrets had also been posted on the Internet for ten days. *Id.* at 1368.

[FN48]. See *Religious Tech. Ctr. v. Lerma*, 897 F. Supp. 260, 262 (E.D. Va. 1995) (Washington Post successfully raised the First Amendment as a shield against issuance of temporary restraining order and preliminary injunction). Because the secrets in *Lerma* were embodied in a text, protecting this information through trade secret law would not create an obstacle to fulfilling objectives of the patent system, but preemption concerns might

nevertheless arise. Copyright law, as pointed out *supra* note 23, does not protect the ideas and information in protected works and allows fair uses, such as publishing excerpts in newspapers such as the Post. If a judge construed state trade secret law to protect the information in RTC's work, notwithstanding its accidental disclosure, such a ruling would arguably be preempted by copyright law and policy because it would protect information that copyright law treats as public domain, once the work has been disclosed to the public.

[FN49]. In the U.S. direct (or primary) patent and copyright infringement are strict liability offenses. See 35 U.S.C. §271(a) (2000); 17 U.S.C. §501 (2000). That is, anyone who violates one of the exclusive rights granted to innovators is an infringer (e.g., making a copy of a copyrighted work or using a patented invention) without regard to the actor's fault. Patent and copyright law require some culpability, however, to establish indirect (or secondary) liability. See, e.g., 35 U.S.C. §271(b)-(c) (providing that active inducement is required for liability; no contributory infringement exists unless actor is making a technology that he knows was specially adapted for infringement); *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005) (explaining that contributory infringement requires showing knowledge that one is contributing to infringement; vicarious liability requires showing a failure to supervise and control an infringer; inducement liability requires affirmative acts of inducement and a specific intent to induce infringement).

[FN50]. See, e.g., Unif. Trade Secrets Act §1(a) (amended 1985), 14 U.L.A. 619 (2005); Restatement (Third) of Unfair Competition §§40, 43 (1993).

[FN51]. See, e.g., Unif. Trade Secrets Act §1(b) (amended 1985), 14 U.L.A. 619 (2005); Restatement (Third) of Unfair Competition §40 (1993).

[FN52]. See, e.g., Restatement (Third) of Unfair Competition §40 cmt. c (1993) (“The unauthorized disclosure of a trade secret ordinarily occurs as part of an attempt to exploit the commercial value of the secret through use in competition with the trade secret owner or through a sale of the information to other potential users.”).

[FN53]. Yet, courts do impose liability if the recipient had reason to know that he received misappropriated information. Restatement (Third) of Unfair Competition §40 cmt. c (1993).

[FN54]. No. 12580, 1992 WL 172678 (Del. Ch. July 22, 1992).

[FN55]. *Id.* at *1-*2. Trade secrecy law also enables an innocent recipient of trade secrets who made substantial investments in reliance on its right to use the information, subject to an obligation to pay royalties for use of misappropriated secrets. See, e.g., Restatement (Third) of Unfair Competition §45 cmt. g (1993).

[FN56]. *Religious Tech. Ctr. v. Lerma*, 908 F. Supp. 1362, 1368-69 (E.D. Va. 1995).

[FN57]. *Id.* at 1368. Someone who posts a trade secret on the Internet “may be liable for trade secret misappropriation, [but] the party who merely downloads Internet information cannot be liable for misappropriation because there is no misconduct involved in interacting with the Internet.” *Id.*; accord *Religious Tech. Ctr. v. F.A.C.T.NET, Inc.*, 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 Tech. Ctr. v. Netcom On-line Commc'n. Servs., 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 individual has put the alleged trade secrets in

the public domain prevents RTC from further enforcing its trade secret rights in those materials.”).

[FN58]. See, e.g., *State ex rel. Sports Mgmt. News, Inc. v. Nachtigal*, 921 P.2d 1304 (Or. 1996); *infra* note 249 and accompanying text.

[FN59]. See, e.g., *Volokh*, *supra* note 8, at 741 (arguing that trade secret injunctions, as applied to third parties, should be subject to strict scrutiny).

[FN60]. Restatement (Third) of Unfair Competition §40 cmt. c (1993) (“[D]isclosure of another’s trade secret for purposes other than commercial exploitation may implicate the interest in freedom of expression or advance another significant public interest.... The existence of a privilege to disclose another’s trade secret depends upon the circumstances of the particular case, including the nature of the information, the purpose of the disclosure, and the means by which the actor acquired the information.”).

[FN61]. A newspaper intending to publish this information would surely raise the First Amendment to any charge of misappropriation raised by the firm wanting to protect its secrets, and would likely win.

[FN62]. See, e.g., Alan Garfield, *Promises of Silence: Contract Law and Freedom of Speech*, 83 *Cornell L. Rev.* 261, 264-66 (1998) (giving examples).

[FN63]. See, e.g., 5 U.S.C.A. §2302(b)(8) (West 1996 & Supp. 2006); N.Y. Lab. Law §740 (West 2002 & Supp. 2006).

[FN64]. See, e.g., Restatement (Third) of Unfair Competition §40 (1993). This too is part of the weakness of trade secret law that mitigates tensions that would otherwise arise between trade secret law and the First Amendment.

[FN65]. See, e.g., 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, 197 (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).

[FN66]. See, e.g., Robert P. Merges, *One Hundred Years of Solicitude: Intellectual Property Law, 1900-2000*, 88 *Cal. L. Rev.* 2187, 2233-40 (2000) (discussing expansions in intellectual property protection during the twentieth century). See generally *Expanding the Boundaries of Intellectual Property: Innovation Policy for a Knowledge Society* (Rochelle Dreyfuss et al. eds., 2001).

[FN67]. See *supra* note 33 and accompanying text.

[FN68]. See, e.g., Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 *Cal. L. Rev.* 241, 243 (1998).

[FN69]. See, e.g., *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1002 (1984) (holding trade secrets to be property for purposes of takings law); see also *infra* notes 169-92 and accompanying text (considering the property conception of trade secret law).

[FN70]. See, e.g., *Group One, Ltd. v. Hallmark Cards, Inc.*, 254 F.3d 1041, 1050 (Fed. Cir. 2001) (plaintiff arguing for an “equitable trade secret theory,” even though secret had been subsequently published); *DTM Re-*

search, L.L.C. v. AT & T Corp., 245 F.3d 327, 331-33 (4th Cir. 2001) (plaintiff arguing that mere possession, rather than ownership, is sufficient to bring a trade secret misappropriation claim).

[FN71]. For an excellent discussion of the innovation and competition policy concerns arising from the use of mass market licenses to plug the leakiness of trade secrecy law, see generally Rochelle C. Dreyfuss, Do You Want to Know a Trade Secret? How Article 2B Will Make Licensing of Trade Secrets Easier (But Innovation More Difficult), 87 Cal. L. Rev. 191 (1999).

[FN72]. See, e.g., Dennis S. Karjala, Federal Preemption of Shrinkwrap and Online Licenses, 22 U. Dayton L. Rev. 511, 520 n.28 (1997); Mark A. Lemley, Beyond Preemption: The Law and Policy of Intellectual Property Licensing, 87 Cal. L. Rev. 111, 129 (1999).

[FN73]. See, e.g., Pamela Samuelson & Suzanne Scotchmer, The Law and Economics of Reverse Engineering, 111 Yale L.J. 1575, 1582-94 (2002).

[FN74]. See Jonathan Zittrain, What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication, 52 Stan. L. Rev. 1201, 1203 (2000).

[FN75]. See Complaint for Declaratory and Injunctive Relief at 13-15, Edelman v. N2H2, Inc., 263 F. Supp. 2d 137 (D. Mass. 2003) (No. 02-CV-11503-RGS), available at <http://www.aclu.org/FilesPDFs/edelman.pdf>.

[FN76]. Id. at 10-15.

[FN77]. Id. at 37.

[FN78]. Edelman was an expert witness in American Library Ass'n v. United States, 201 F. Supp. 2d 401, 442-44 (E.D. Pa. 2002). He studied over- and under-blocking by testing filtering programs against various individual sites. Id. However, this technique provided incomplete analysis of the efficacy of filtering programs. Id.

[FN79]. See Complaint, supra note 75, at 24.

[FN80]. See Press Release, Am. Civil Liberties Union, In Legal First, ACLU Sues Over New Copyright Law (July 25, 2002), available at <http://www.aclu.org/privacy/speech/14811prs20020725.html>.

[FN81]. Edelman v. N2H2, Inc., 263 F. Supp. 2d 137, 138 (D. Mass. 2003). Because Edelman had not entered into a licensing agreement with N2H2, the court agreed with N2H2 that he was seeking an advisory opinion. Id. at 138-39.

[FN82]. Edelman abandoned this project after his case was dismissed because he feared risks of litigation. E-mail from Ben Edelman to author (July 28, 2006, 14:45:55 AST) (on file with author). A similar lawsuit, albeit one brought by a rightholder against reverse engineers, is discussed in Declan McCullagh, Mattel's Filtering Fiasco to Court, WIRED News, Mar. 27, 2002, <http://www.wired.com/news/business/0,1367,35196,00.html>. Mattel, owner of rights in the Cyber Patrol filtering software, sued two cryptanalysts who reverse engineered Cyber Patrol in breach of a mass market license forbidding reverse engineering and then developed "cphack.exe," software that enabled users to bypass the filter. Id. The defendants settled this lawsuit by transferring their copyrights in the software to Mattel, which sought to revoke the open source license under which the software had been distributed so it could sue for infringement any sites that had posted "cphack.exe." See The Story of CPHack, <http://cphack.robinlionheart.com> (last visited Mar. 1, 2007).

[FN83]. See Julie E. Cohen, Call It the Digital Millennium Censorship Act: Unfair Use, New Republic Online, May 23, 2000, <http://www.law.georgetown.edu/faculty/jec/unfairuse.html>.

[FN84]. Id.

[FN85]. Id.

[FN86]. *People v. Network Assoc., Inc.*, 758 N.Y.S.2d 466, 467-68 (Sup. Ct. 2003).

[FN87]. Id. at 470-71. The New York Attorney General's Internet Bureau persuaded the court to enjoin Network Associates from selling software under conditions that prohibited consumers from disclosing the results of benchmark tests or from publishing reviews of Network Associates's products without permission. Id. at 471.

[FN88]. See, e.g., AttachmateWRQ Software License Agreement, http://mx.attachmate.com/NR/rdonlyres/DF244244-583F-4B84-BF30-90912B128245/0/SLA_eng.pdf (last visited Mar. 1, 2007). For further discussion of policy implications of such clauses, see, for example, Genelle I. Belmas & Brian N. Larson, Clicking Away Your Free Speech Rights: The Enforceability of Gagwrap Licenses, 12 *Comm. L. & Pol'y* 37 (2007).

[FN89]. *Bunner III*, 75 P.3d 1, 6-7 (Cal. 2003).

[FN90]. Id.

[FN91]. Id.

[FN92]. Id. at 7-8. The DVD CCA claimed that a Norwegian teenager named Jon Johansen was the reverse engineer who breached such a license. See *Bunner I*, No. CV 786804, 2000 WL 48512 at *2 (Super. Ct. Cal. Jan. 21, 2000). Johansen was not, however, the person who reverse engineered CSS. See *Sunde v. Johansen*, No 02-507 M/94 (Oslo Court of First Instance Jan. 7, 2003), available at http://www.eff.org/IP/Video/Johansen_DeCSS_case/20030109_johansen_english_decision.rtf (noting that Johansen obtained the reverse engineered information from a person using the moniker "nomad").

[FN93]. *Bunner IV*, 10 Cal. Rptr. 3d 185, 189-90 (Ct. App. 2004).

[FN94]. Complaint for Injunctive Relief for Misappropriation of Trade Secrets at ¶¶ 34-39, *DVD Copy Control Ass'n v. McLaughlin*, No. CV 786804 (Super. Ct. Cal. Dec. 28, 1999), available at http://www.eff.org/IP/Video/DVDCCA_case/19991228-complaint.html. DVD CCA also sued for trade secret misappropriation a firm that sold T-shirts on which the text of DeCSS was printed. See Sara Crasson, Are DeCSS T-Shirts Dirty Laundry? Wearable, Non-Executable Computer Code as Protected Speech, 15 *Fordham Intell. Prop. Media & Ent. L.J.* 169, 169 (2004). At about the same time as DVD CCA commenced the *Bunner* case, Universal City Studios and other motion picture studios brought suit against a journalist named Eric Corley, alleging that posting and linking to DeCSS violated the anti-circumvention rules of the DMCA. See *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 436 (2d Cir. 2001). Corley's principal defense was that he had a First Amendment right to publish DeCSS. Id. The Second Circuit Court of Appeals upheld a permanent injunction forbidding Corley to post or link to source or object code forms of DeCSS. Id. at 458-60. After this decision was rendered, lawyers for the motion picture industry sent a cease and desist letter to Dr. David Touretsky, a computer science researcher at Carnegie Mellon University, demanding that he take down his Gallery of CSS Descramblers, which featured many different expressions of how to descramble DVD CCA's encryption program. David S.

Touretzky, Gallery of CSS Descramblers, <http://www.cs.cmu.edu/~dst/DeCSS/Gallery> (last visited Mar. 1, 2007). Dr. Touretzky declined to do so. Id.

[FN95]. See Defendant's Memorandum of Points and Authorities in Opposition to Order to Show Cause Re: Preliminary Injunction, DVD Copy Control Ass'n, Inc. v. McLaughlin, No. CV 786804 (Super. Ct. Cal., Jan. 7, 2000), http://www.eff.org/IP/Video/DVDCCA_case/20000107-pi-motion-response.html.

[FN96]. Bunner I, No. CV 786804, 2000 WL 48512, at *2 (Super. Ct. Cal. 2000).

[FN97]. Id. at *3. The judge did not seem to grasp the novelty of 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. See, e.g., Pamela Samuelson, Reverse Engineering Under Siege, *Comm. ACM*, Oct. 2002, at 15 17-19; Brief of Intellectual Property Law Professors et al. as Amici Curiae Supporting Defendant at 12-17, 75 P.3d 1 (Cal. 2003), available at http://www.law.berkeley.edu/cenpro/samuelsong/projects_papers/2002sp_dvd_bunner_brief.pdf (explaining weaknesses of this aspect of DVD CCA's trade secrecy theory).

[FN98]. Bunner I, 2000 WL 48512, at *1.

[FN99]. Bunner IV, 10 Cal. Rptr. 3d 185, 187 (Ct. App. 2004). The First Amendment issues raised in Bunner IV are discussed infra notes 334-46 and accompanying text.

[FN100]. Bunner IV, 10 Cal. Rptr. 3d at 189-90.

[FN101]. Only Justice Moreno, in his concurrence in Bunner III, recognized the novelty of this aspect of DVD CCA's claim:

[N]owhere has it been recognized that a party wishing to protect proprietary information may employ a consumer form contract to, in effect, change the statutory definition of "improper means" under trade secret law to include reverse engineering so that an alleged trade secret holder may bring an action even against a nonparty to that contract.

Bunner III, 75 P.3d 1, 28 n.5 (Cal. 2003) (Moreno, J., concurring). The Court of Appeal found a different flaw in DVD CCA's claim. Bunner II, 113 Cal. Rptr. 2d 338, 342 (Ct. App. 2002). Apparently Xing, one of DVD CCA's licensees, neglected to abide by its contractual obligations to DVD CCA and failed to install CSS securely or omitted end-user licenses in its products. Id. at 344. Some commentators have argued that evidence of misappropriation of the CSS secrets was also weak. See Alex Eaton-Salners, DVD Copy Control Association v. Bunner: Freedom of Speech and Trade Secrets, 19 Berkeley Tech. L.J. 269, 279-80 (2004).

[FN102]. *Chicago Lock Co. v. Fanberg*, 676 F.2d 400, 404 (9th Cir. 1982).

[FN103]. Id.

[FN104]. See Bunner IV, 10 Cal. Rptr. 3d at 189 ("CSS was widely analyzed and discussed in the academic cryptography community."); id. at 190 (discussing news coverage about DeCSS).

[FN105]. See Mark A. Lemley, Intellectual Property and Shrinkwrap Licenses, 68 S. Cal. L. Rev. 1239, 1239-48 (1995) (discussing the caselaw).

[FN106]. An anti-reverse engineering clause of a software license was enforced in *Bowers v. Bay State Techs.*,

Inc., but Bay State had also infringed Bowers's copyright, which may have colored the court's judgment on the lawfulness of its reverse engineering. 320 F.3d 1332, 1341-44 (Fed. Cir. 2003). 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. See *Vault Corp. v. Quaid Software Ltd.*, 847 F.2d 255, 270 (5th Cir. 1988). Bunner has a particularly strong claim for not being bound by a DVD CCA required license given how remote he was from the reverse engineering activities and any license that may have been breached, as well as how remote DVD CCA was from the reverse engineer. Commentary on the enforceability of anti-reverse engineering clauses of mass market licenses has mostly been critical of the idea. See, e.g., Samuelson & Scotchmer, *supra* note 73, at 1626-30 (recommending against enforcement of such license terms in software contracts and citing commentators who have considered the issue).

[FN107]. UCITA was once expected to become Article 2B of the Uniform Commercial Code. Concerns about the relationship between proposed Article 2B and intellectual property law were discussed at a conference organized by the Berkeley Center for Law and Technology at Boalt Hall in April 1998 on "Intellectual Property and Contract Law for the Information Age." See generally Symposium, *Intellectual Property and Contract Law for the Information Age: The Impact of Article 2B of the Uniform Commercial Code on the Future of Information and Commerce*, 87 Cal. L. Rev. 1 (1999); Symposium, *Intellectual Property and Contract Law for the Information Age: The Impact of Article 2B of the Uniform Commercial Code on the Future of Information and Commerce*, 13 Berkeley Tech. L.J. 809 (1998). Shortly after that conference, the American Law Institute withdrew as a cosponsor of Article 2B. See Special Committee on Security Interests, Section of Intellectual Property Law, ABA, Annual Report 1999-2000 (2000). The National Conference on Commissioners of Uniform State Laws later promulgated it as UCITA. Although adopted in Maryland and Virginia, UCITA has not met with favor in other states. Lauria J. Flynn, *The Battle Lines Are Drawn in the Struggle for a Uniform Standard in Software Licensing for all 50 States*, N.Y. Times, Sept. 16, 2002, at C3. Yet, mass market licenses are often enforced. Indeed, recent caselaw has even enforced terms of service as contractual obligations notwithstanding an absence of proof of assent; merely using a website has been held to create a contract under the website developer's terms of use. See generally Mark A. Lemley, *Terms of Use* (Mar. 2, 2007) (unpublished manuscript, on file with author).

[FN108]. UCITA §209 (1999).

[FN109]. See, e.g., Letter from Joan Z. Bernstein et al. of the Federal Trade Commission, to John McClaugherty of the National Conference on Commissioners of Uniform State Laws (July 9, 1999), available at <http://www.ftc.gov/be/v990010.htm>.

[FN110]. See American Law Institute, *Principles of the Law of Software Contracts*, Preliminary Draft No. 2 (2005).

[FN111]. See Karjala, *supra* note 72, at 520 n.28; Lemley, *supra* note 72, at 129.

[FN112]. See, e.g., Atkins, *supra* note 8, at 1196 ("Trade secret law is in danger of extinction on the Internet."); Beckerman-Rodau, *supra* note 8, at 29-30 (discussing risks of the Internet for trade secrets); Sahara Murthy, Comment, *Public Concern--A Newsworthy Exception to the Grant of Preliminary Injunctions in Trade Secrecy Cases*, 36 Golden Gate U. L. Rev. 219, 220 (2006) ("[T]he Internet has multiplied the risk of loss of a trade secret").

[FN113]. The First Amendment advocate who gives most weight to First Amendment interests and least to trade

secret interests when they conflict is Greene, *supra* note 8, whose four-part test for resolving conflicts between trade secret law and the First Amendment is discussed *infra* notes 391-92 and accompanying text. Volokh argues for strict scrutiny when preliminary injunctions are under consideration as to third party recipients who want to publish them. See Volokh, *supra* note 8, at 739-48. Murthy proposes an exception to trade secrecy law for publication of newsworthy information of public concern. Murthy, *supra* note 112, at 238-42. At the opposite end of the spectrum are Beckerman-Rodau, *supra* note 8, at 57-66, who believes the First Amendment has no role to play in trade secret cases, *id.* at 62-63, and Atkins, *supra* note 8, at 1187-96, who would impose duties on third party recipients of misappropriated information to investigate its provenance before publishing information, in effect, creating a new right of privacy for trade secrets. Johnson offers a balancing test for mediating between trade secret and First Amendment interests; it would weigh the nature of the information (e.g., how technical it is; how much investment was required to develop it), the way in which the defendant obtained it, and the comparative harm to the intended publisher and the trade secret developer, such that the greater the harm to the trade secret developer, the less likely a First Amendment defense would be to succeed. See Johnson, *supra* note 8, at 540.

[FN114]. *Ford Motor Co. v. Lane*, 67 F. Supp. 2d 745, 753 (E.D. Mich. 1999).

[FN115]. See Atkins, *supra* note 8, at 1187-96; Beckerman-Rodau, *supra* note 8, at 57-65; Johnson, *supra* note 8, at 540-41; Goldberg, *supra* note 8, at 292-93; see also *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 454 (2d Cir. 2001) (listing dangers of Internet as reason for lesser First Amendment protection for posting information on the Internet).

[FN116]. *Bunner I*, No. CV 786804, 2000 WL 48512, at *3 (Super. Ct. Cal. 2000).

[FN117]. See *id.* at *2-*3. Without an injunction against posting DeCSS, the motion picture industry's efforts to protect DVDs from unauthorized copying would "become completely meaningless." *Id.* The court not only perceived *Bunner et al.* to be trade secret anarchists, but also intellectual property anarchists, as the main threat posed by DeCSS was to copyrighted DVD movies.

[FN118]. See *id.* at *2.

[FN119]. See *id.* at *3.

[FN120]. See *id.* at *2.

[FN121]. See *id.* at *3-4.

[FN122]. See *Bunner IV*, 10 Cal. Rptr. 3d 185, 192-93 (Ct. App. 2004) ("Publication on the Internet does not necessarily destroy the secret if the publication is sufficiently obscure or transient or otherwise limited so that it does not become generally known to the relevant people, i.e., potential competitors or other persons to whom the information would have some economic value."); *id.* at 253-54 (injunction appropriate if information on Internet has not become publicly known).

[FN123]. See, e.g., *Gates Rubber Co. v. Bando Chem. 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).

[FN124]. See, e.g., Victoria A. Cundiff, *Trade Secrets and the Internet: A Practical Perspective*, 14 *Computer*

Law. 6 (1997) (offering suggestions for how trade secret owners can protect trade secrets to protect against Internet dissipation); see also Elizabeth Rowe, *Saving Trade Secret Disclosures on the Internet Through Sequential Preservation*, 42 *Wake Forest L. Rev.* (forthcoming Spring 2007) (setting forth a test for preserving trade secrets that have been posted on the Internet).

[FN125]. See, e.g., *Religious Tech. Ctr. v. Lerma*, 908 F. Supp. 1362, 1368-69 (E.D. Va. 1995) (information available in unsealed court records for two years and on the Internet for ten days); *Bunner IV*, 10 Cal. Rptr. 3d 185, 248 (Ct. App. 2004) (information displayed on or linked to at least 118 websites for more than three months before the lawsuit was filed).

[FN126]. See *Karjala*, supra note 72; *Lemley*, supra note 72. Besides the *Bunner* and *RTC* cases, the caselaw on the Internet posting of trade secrets is very sparse. See *Ford Motor Co. v. Lane*, 67 F. Supp. 2d 745, 746 (E.D. Mich. 1999) (denying preliminary injunction against third party posting of trade secrets about car designs on First Amendment grounds); *O'Grady v. Superior Court*, 44 Cal. Rptr. 3d 72, 76-77 (Ct. App. 2006) (issuing protective order against subpoena seeking information about the sources of leaked trade secrets). This contrasts sharply with the prevalence of copyright infringement on the Internet. See, e.g., *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1019 (9th Cir. 2001) (discussing millions of users of Napster's peer-to-peer file sharing technology to swap digital music files).

[FN127]. See, e.g., *Cundiff*, supra note 124; 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).

[FN128]. See 18 U.S.C.A. §§1831-1839 (West 2006); see also Lambrecht, supra note 127, at 361-62 (discussing criminal sanctions for trade secret misappropriation). There have been some criminal actions brought against Internet misappropriators. See *United States v. Genovese*, 409 F. Supp. 2d 253, 254-55 (S.D.N.Y. 2005) (posting Microsoft proprietary code on the Internet was prima facie violation of EEA); Jennifer Lee, *Student Arrested in DirecTV Piracy Case*, *N.Y. Times*, Jan. 3, 2003, at C2 (student arrested for stealing DirecTV trade secrets and posting them on the Internet). The Department of Justice has been vigorously prosecuting those who violate the EEA. See Computer Crime and Intellectual Property Section, Department of Justice, *Economic Espionage Act Cases*, <http://www.usdoj.gov/criminal/cybercrime/eeapub.htm> (last visited Mar. 1, 2007).

[FN129]. 521 U.S. 844, 870 (1997) (ruling that Internet speech was entitled to the highest degree of First Amendment protection and rejecting arguments that the Internet was so dangerous that lower levels of First Amendment protection should be available).

[FN130]. See, e.g., *Epstein*, supra note 8, at 1037. Professor Epstein does not use the term "categorical immunity," but says that the First Amendment prohibition against prior restraints has no application at all in trade secret cases. *Id.* at 1042.

[FN131]. *Beckerman-Rodau*, supra note 8, at 5; *Epstein*, supra note 8, at 1035.

[FN132]. *Beckerman-Rodau*, supra note 8, at 12; *Epstein*, supra note 8, at 1037.

[FN133]. *Beckerman-Rodau*, supra note 8, at 29-30; *Epstein*, supra note 8, at 1038.

[FN134]. *Bunner III*, 75 P.3d 1, 11-16 (Cal. 2003). Justices Werdegar and Moreno wrote concurring opinions expressing a more liberal view of the role of the First Amendment in trade secret cases. See *id.* at 20 (Werdegar, J., concurring) (“[T]he First Amendment does not necessarily preclude injunctive relief in trade secret cases.”); *id.* at 21-26 (Moreno, J., concurring) (extensively criticizing Justice Brown’s analysis of First Amendment precedents).

[FN135]. The trial judge obliquely referred to free speech interests by observing 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.” *Bunner I*, No. CV 786804, 2000 WL 48512, at *4 (Super. Ct. Cal. 2000). Yet, the judge was not wholly inattentive to *Bunner*’s First Amendment rights, for he rejected DVD CCA’s request to enjoin *Bunner* and his co-defendants from linking to websites where CSS information might be found on the ground that such an order would be “overbroad and extremely burdensome” because “[a] website owner cannot be held responsible for all of the content of the sites to which it provides links.” *Id.* But see *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 434-35 (2d Cir. 2001) (upholding an injunction against a journalist’s linking to sites where DeCSS could be found as consistent with the First Amendment).

[FN136]. It assumed, without deciding, that the trial court had correctly concluded that DVD CCA had established a reasonable probability of success on the merits for the trade secrecy claim. *Bunner II*, 113 Cal. Rptr. 2d 338, 347 (Ct. App. 2001). In *Bunner IV*, 10 Cal. Rptr. 3d 185, 192-93 (Ct. App. 2004), the Court of Appeal decided that DeCSS had been too widely posted on the Internet for too long for DVD CCA to claim CSS-derived information were protectable secrets. For further discussion, see *infra* note 334 and accompanying text.

[FN137]. *Bunner II* did not articulate any limiting principles on the scope of First Amendment protection in trade secret cases. See *infra* notes 147-49 and accompanying text for Microsoft’s interpretation of *Bunner II*. The decision also erred in expressing no opinion on whether an injunction against publication of DeCSS might be an appropriate remedy after a full trial on the merits, without realizing that the availability of DeCSS on the Internet prior to trial would vitiate any secrets from CSS that the program might contain. See *Bunner II*, 113 Cal. Rptr. 2d at 351.

[FN138]. *Bunner III*, 75 P.3d at 11-12.

[FN139]. Epstein, *supra* note 8, at 1006. He defines this as “the belief that the First Amendment weights the scales above and beyond what a sensible theory of freedom of speech, understood as part of a general theory of freedom, would require.” *Id.* Epstein did not discuss *Bunner II*, as the case was decided after his article was published. In the context of trade secrecy, Epstein regards “mechanical application” of prior restraint law, as in *Bunner II*, as a manifestation of this phenomenon. *Id.* at 1042. Although Robert Post has not commented on First Amendment defenses in trade secret cases, he has pointed out that the First Amendment does not apply in every case in which liability is predicated on some speech or communicative act. See, e.g., Post, *supra* note 13, at 715. Post argues that the social context in which communication takes place must be taken into account in deciding whether the First Amendment has salience in cases involving speech and communication. *Id.*

[FN140]. “‘Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment.’” *Bunner II*, 113 Cal. Rptr. 2d at 348 (quoting *Junger v. Daley*, 209 F.3d 481, 484-85 (6th Cir. 2000)). *Junger* made a First Amendment challenge to export control laws insofar as they forbade disclosure of encryption source code without getting a license approval from a government agency. *Junger*, 209 F.3d at 482.

[FN141]. Bunner II, 113 Cal. Rptr. 2d at 350.

[FN142]. *Id.* at 351.

[FN143]. *Id.*

[FN144]. *Id.* at 352.

[FN145]. DeCSS was not “lewd, profane, obscene or libelous, nor did it involve any fighting words,” and so accepted limitations on First Amendment protection for such speech did not apply. *Id.* The court saw no justification for creating a new exception. *Id.*

[FN146]. As set forth by the Court of Appeal in Bunner II:

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.

Id. at 350; accord Lemley & Volokh, *supra* note 8, at 158-63 (discussing frequency of preliminary injunctions in copyright cases).

[FN147]. See Brief of Microsoft Corp. et al. as Amici Curiae Supporting Respondent at 1-2, Bunner III, 75 P.3d 1 (Cal. 2003) (No. S102588), available at http://www.eff.org/IP/Video/DVDCCA_case/20020718_bunner_ms_amicus_brief.pdf.

[FN148]. *Id.* at 2.

[FN149]. See Brief of Attorney General Lockyer as Amicus Curiae Supporting Respondent at 2-4, Bunner III, 75 P.3d 1 (No. S102588), available at http://www.eff.org/IP/Video/DVDCCA_case/bunner-ca-ag-amicus.pdf.

[FN150]. Bunner III, 75 P.3d at 11. Justice Brown also took issue with the Court of Appeal's conclusion that the preliminary injunction was a prior restraint. See *id.* at 16-20. This aspect of Bunner III is discussed *infra* Part IV.A. Justice Brown may have been influenced by the Second Circuit Court of Appeals's ruling in *Universal City Studios, Inc. v. Corley*, for Justice Brown cited this decision and its lower court counterpart several times. See *id.* at 6-29 (citing 273 F.3d 429 (2d Cir. 2001)). Corley also applied First Amendment intermediate scrutiny in judging the constitutionality of an injunction against posting of the same DeCSS code as in Bunner, although the Second Circuit's use of intermediate scrutiny was primarily based on the functionality of DeCSS. Corley, 273 F.3d at 450-52. Corley is distinguishable from Bunner in several respects: the injunction in Corley was a permanent injunction after trial on the merits, not a preliminary injunction, *id.* at 436, Corley had posted executable object code rather than source code, *id.* at 438, and the suit against Corley charged him with trafficking in circumvention technologies, not posting of trade secrets or information derived from trade secrets, *id.* at 435.

[FN151]. Bunner III, 75 P.3d at 11 (relying upon, among others, *Ward v. Rock Against Racism*, 491 U.S. 781 (1989) (regulation of decibel levels for outdoor concerts did not violate the First Amendment); *Madsen v. Women's Health Center*, 512 U.S. 753 (1994) (upholding injunction regulating access to abortion clinic against a First Amendment challenge)). Bunner's counsel pointed out that the Supreme Court in *Bartnicki v. Vopper* had characterized a wiretap statute as applied to publication of an illegally intercepted conversation by a person not involved in the misappropriation of the information as a regulation of “pure speech.” *Id.* at 12-13 (discussing

532 U.S. 514 (2000)). However, Justice Brown pointed out that the Court did not say in *Bartnicki* what level of scrutiny it was applying and a majority of the Justices supported less than a strict scrutiny approach. *Id.* at 12-13.

[FN152]. *Id.* at 11 (“Our principal inquiry in determining content neutrality is whether the government has adopted a regulation of speech without reference to the content of the regulated speech.” (quoting *Madsen*, 512 U.S. at 763) (internal quotation marks omitted)).

[FN153]. *Id.* (“The underlying basis for the injunction is the trial court's holding that *Bunner* misappropriated DVD CCA's property--its trade secrets--in violation of California's trade secrecy law.”).

[FN154]. See, e.g., *id.* at 14 (“The First Amendment does not prohibit courts from incidentally enjoining speech in order to protect a legitimate property right.”).

[FN155]. *Id.* at 10-17.

[FN156]. *Id.* at 15-16.

[FN157]. *Id.* at 19.

[FN158]. *Id.* Two Justices stated the holding more narrowly. See *infra* note 160.

[FN159]. Part IV will explain at length why I disagree with this implication of *Bunner III*.

[FN160]. *Bunner III*, 75 P.3d at 21 (Moreno, J., concurring) (“I concur in the majority's narrow holding, which as I understand it, is that the First Amendment does not categorically prohibit preliminary injunctions to enjoin the publication of trade secrets.”); see also *id.* at 21-23 (Moreno, J., concurring) (discussing *Madsen* and other decisions on which Justice Brown had relied). Justice Werdegar also construed the holding in *Bunner III* to mean “that the First Amendment... does not necessarily preclude injunctive relief in trade secret cases.” *Id.* at 20 (Werdegar, J., concurring).

[FN161]. *Id.* at 23 (Moreno, J., concurring).

[FN162]. *Id.*; see also *Volokh*, *supra* note 8, at 702-06 (criticizing *Bunner III*, among other cases, for its analysis of content-neutrality, arguing that injunctions in intellectual property cases are content-based restrictions on speech).

[FN163]. *Bunner III*, 75 P.3d at 24. Yet, a long footnote referred to the Court of Appeal's reasons for distinguishing trade secrets and copyrights vis-à-vis injunctive relief. *Id.* at 23 n.1.

[FN164]. See, e.g., *id.* at 11 (“*Bunner* misappropriated DVD CCA's property....”); *id.* (characterizing trade secrets as a property right and referring to “DVD CCA's statutorily created property right”); *id.* at 12 (“[T]he specific deprivation to be remedied is the misappropriation of a property interest in information.”); *id.* at 13 (characterizing trade secrets as “a constitutionally protected intangible property interest”); *id.* (trade secret law creates “a limited property right in information”); *id.* at 14 (“[T]he right to exclude others is central to the very definition of the property interest.” (internal quotation marks omitted) (quoting *Monsanto*, 467 U.S. at 1011)); see also *supra* notes 150-51.

[FN165]. Bunner III, 75 P.3d at 12 (citing Beckerman-Rodau, *supra* note 8); *id.* at 15 (citing Epstein, *supra* note 8).

[FN166]. See, e.g., *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1003-04 (1984) (holding that reports and data on safety claimed as trade secrets were property for purposes of Fifth Amendment takings analysis).

[FN167]. See, e.g., *Lloyd Corp. Ltd. v. Tanner*, 407 U.S. 551, 568-70 (1972) (holding that mall owner had the right to exclude the distribution of handbills by anti-war protestors from its premises).

[FN168]. See, e.g., *Dallas Cowboy Cheerleaders, Inc. v. Scoreboard Posters, Inc.*, 600 F.2d 1184, 1188 (5th Cir. 1979) (holding that there is no First Amendment right to infringe trademarks).

[FN169]. See, e.g., *Tabor v. Hoffman*, 23 N.E. 12, 13-14 (N.Y. 1889) (finding misappropriation of trade secrets where the defendant abused a confidential relationship by measuring and copying plaintiff's patterns and using the copies to make pipes that competed with plaintiff's pipes).

[FN170]. Restatement (Third) of Unfair Competition §40 (1993).

[FN171]. 244 U.S. 100, 102 (1917).

[FN172]. Restatement of Torts §757 cmt. a (1939).

[FN173]. Restatement (Third) of Unfair Competition §39 cmt. b (1993).

[FN174]. *Id.*; see also Pooley, *supra* note 40, at 1-20.

[FN175]. Restatement (Third) of Unfair Competition §39 cmt. b (1993).

[FN176]. *Id.*

[FN177]. Milgrim, *supra* note 9, §9.02[5][a].

[FN178]. U.S. Const. art. I, §8, cl. 8.

[FN179]. See 17 U.S.C. §106 (2000) (setting forth exclusive rights of copyright); 35 U.S.C. §271 (2000) (setting forth exclusive rights of patent owners).

[FN180]. See, e.g., William B. Stoebuck & Dale A. Whitman, *The Law of Property* §7.1, at 411-13 (3d ed. 2000).

[FN181]. See 17 U.S.C. §102(a).

[FN182]. *Id.* §102(b). The algorithms in CSS would be unprotectable processes or procedures in the program. See, e.g., *Gates Rubber Co. v. Bando Chem. Indus., Ltd.*, 9 F.3d 823, 834-37 (10th Cir. 1993). Under *Gottschalk v. Benson*, 409 U.S. 63 (1972), program algorithms would also be unpatentable as mathematical ideas. Even if one believes that *Benson* is no longer good law, it is fair to say that the CSS algorithms are unpatentable (and hence unprotectable as a matter of federal patent law) because they have been in commercial use for several years. See 35 U.S.C. §102(b). Thus, as a matter of patent law, the CSS algorithms cannot be federally protected property either. They should be protectable as trade secrets only so long as they are secrets, which they no

longer are.

[FN183]. See, e.g., *Feist Pub., Inc. v. Rural Tel. Serv.*, 499 U.S. 340, 349 (1991).

[FN184]. See, e.g., *id.* at 349 (characterizing the unprotectability of facts as “the essence of copyright and a constitutional requirement” (citations omitted)); *Harper & Row Publishers v. Nation Enters.*, 471 U.S. 539, 559-60 (1985) (noting that copyright law does not conflict with the First Amendment because copyright doesn't protect ideas and facts). Many commentators regard facts and ideas as constitutionally protected elements of the public domain. See generally Pamela Samuelson, *Enriching Discourse on Public Domains*, 55 *Duke L.J.* 783 (2006) (discussing concepts of the constitutionally protected public domain that includes ideas and information).

[FN185]. See *supra* note 184 and accompanying text (concerning preemption and First Amendment concerns arising when trade secret law is strengthened).

[FN186]. See *supra* note 171 and accompanying text.

[FN187]. 467 U.S. 986, 986 (1984) (applying Fifth Amendment takings analysis to legislation regulating uses that could be made of safety data submitted to the Environmental Protection Agency in connection with approval of fungicides).

[FN188]. *Id.* at 1002.

[FN189]. *Id.* at 1002-04. Other intangible interests, such as a materialman's lien and contracts, have been treated as “property” for purposes of assessing Fifth Amendment takings claims. *Id.* at 1003. 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* of trade secrets as property and the mischief this characterization might wreak unless narrowly construed).

[FN190]. The challenged provisions were part of the Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA). The data-consideration rules were in §3(c)(1)(D) of FIFRA.

[FN191]. See 7 U.S.C. §136g (2000); see *id.* §136a(c)(2)(A) (containing the data-disclosure provisions).

[FN192]. *Ruckelshaus*, 467 U.S. at 998-99 (noting that Monsanto alleged that all of the challenged provisions were unconstitutional takings and sought injunctive relief against the EPA's use of those provisions and asserted the uses permitted were for private, rather than public, purposes).

[FN193]. *Id.* at 1004-08. Prior to 1972, FIFRA was silent on whether the EPA could use or disclose this data. The Court construed this silence too as giving Monsanto no investment-backed expectation of non-use or non-disclosure. *Id.* at 1008-10.

[FN194]. *Id.* at 1006.

[FN195]. *Id.* at 1010-12.

[FN196]. *Id.* at 1012-16.

[FN197]. *Id.* at 1016-19 (holding that Monsanto could seek compensation under the Tucker Act in the Court of Claims).

[FN198]. See, e.g., Beckerman-Rodau, *supra* note 8, at 21 n.95.

[FN199]. Ruckelshaus, 476 U.S. at 1014-16.

[FN200]. 44 Cal. Rptr. 3d 72, 112 (Ct. App. 2006).

[FN201]. *Id.*

[FN202]. *Id.*

[FN203]. *Id.* In *Intel Corp. v. Hamidi*, the California Supreme Court rejected arguments based on analogizing unauthorized email communications by former employee to current employees of Intel as akin to trespass to real property. 71 P.3d 296, 308-12 (Cal. 2003). The court considered the free speech implications of enjoining unauthorized emails as trespasses to computers in ruling against Intel. *Id.* at 311-12. Justice Brown's dissent in that case emphasized the desirability of protecting property rights. *Id.* at 313-25 (Brown, J., dissenting).

[FN204]. O'Grady, 44 Cal. Rptr. 3d at 112.

[FN205]. *Id.* Third party disclosure of trade secrets is discussed *infra* Part IV.E.

[FN206]. Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 *Stan. L. Rev.* 1049, 1063 (2000). Volokh points out that characterizing Sullivan's interest in his reputation as 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 United States change the First Amendment implications of flag burning. *Id.* at 1063-64; see also Volokh, *supra* note 8, at 700 (giving examples of strategic uses of the property metaphor to try to change outcomes in First Amendment cases); Lemley & Volokh, *supra* note 8, at 182-85 (critical of view that designating copyright as property is a basis for ruling that the First Amendment has no application).

[FN207]. See, e.g., *ETW Corp. v. Jireh Pub'g, Inc.*, 332 F.3d 915, 937 (6th Cir. 2003) (holding that First Amendment overrides publicity rights claim as to print of Tiger Woods); *Mattel, Inc. v. MCA Records, Inc.*, 296 F.3d 894, 901, 904 (9th Cir. 2002) (holding that First Amendment limits trademark and dilution law to permit expressive uses of marks such as song about Barbie dolls); *Cardtoons L.C. v. Major League Baseball Players Ass'n*, 95 F.3d 959, 969 (10th Cir. 1996) (holding that First Amendment interests of maker of parody baseball cards outweighed players' publicity rights interests); *L.L. Bean, Inc. v. Drake Publishers, Inc.*, 811 F.2d 26, 29 (1st Cir. 1987), cert. denied, 483 U.S. 1013 (1987) (holding that the First Amendment limits the scope of dilution law as applied to sexual parody of catalog); *Stop the Olympic Prison v. United States Olympic Comm.*, 489 F. Supp. 1112, 1125 (S.D.N.Y. 1980) (holding that First Amendment speech interests supported allowing use of Olympic symbol in protest against building a prison on a former Olympic site); *Hicks v. Casablanca Records*, 464 F. Supp. 426, 433 (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).

[FN208]. See *infra* note 212 and accompanying text.

[FN209]. Lemley & Volokh, *supra* note 8, at 182-84.

[FN210]. 537 U.S. 186, 221 (2003), reh'g denied, 538 U.S. 916 (2003).

[FN211]. 510 U.S. 1315, 1317 (1994).

[FN212]. See, e.g., *Procter & Gamble Co. v. Bankers Trust Co.*, 78 F.3d 219, 224-25 (6th Cir. 1996) (holding preliminary injunction against *Business Week's* publication of information derived from documents said to constitute trade secrets and confidential information to be an unconstitutional prior restraint); *Ford Motor Co. v. Lane*, 67 F. Supp. 2d 745, 750 (E.D. Mich. 1999) (denying Ford's motion for preliminary injunction against disclosure of trade secret information as prior restraint); *Religious Tech. Ctr. v. Lerma*, 897 F. Supp. 260, 262 (E.D. Va. 1995) (denying preliminary injunction in trade secrecy and copyright infringement against *Washington Post*, characterizing requested injunction as a prior restraint); *State ex rel. Sports Mgmt. News, Inc. v. Nachtigal*, 921 P.2d 1304, 1308 (Or. 1996) (overturning preliminary injunction as a prior restraint against publication of information by newsletter that had been disclosed in breach of employee confidence); *Garth v. Staktek Corp.*, 876 S.W.2d 545, 549-50 (Tex. App. 1994) (holding preliminary injunction was prior restraint, but showing adequate to overcome this restraint); see also *Bridge C.A.T. Scan Assocs. v. Technicare Corp.*, 710 F.2d 940, 945-46 (2d Cir. 1983) (holding no exception from prior restraint doctrine for trade secrets). But see *Bunner III*, 75 P.3d 1, 18 (Cal. 2003) (opining that a preliminary injunction against public dissemination of alleged trade secrets was not a prior restraint on speech).

[FN213]. 510 U.S. at 1316.

[FN214]. *Id.*

[FN215]. *Id.*

[FN216]. *Id.*

[FN217]. *Id.* at 1317 (internal citations omitted).

[FN218]. *Id.* at 1318.

[FN219]. *Id.*

[FN220]. *Id.*

[FN221]. *Id.*; accord *Dietemann v. Time Inc.*, 449 F.3d 245, 249 (9th Cir. 1971) (“The First Amendment has never been construed to accord newsmen immunity from torts or crimes committed during the course of news-gathering. The First Amendment is not a license to trespass, to steal, or to intrude by electronic means into the precincts of another's home or office.”)

[FN222]. See 403 U.S. 713, 759-63 (1971) (Blackmun, J., dissenting). Justice Blackmun's principal concern was that the case had been adjudicated in haste and with pressure, panic, and sensationalism that did not allow for proper judicial consideration. *Id.* at 760-61. He would have remanded the case for expeditious proceedings after some discovery and an orderly presentation of evidence and argumentation. *Id.* at 761-62. He also expressed concern about the harm that publication of the Pentagon Papers might do to the lives of soldiers. *Id.* at 762-63. Justice Blackmun also joined Justice Harlan's dissent. *Id.* at 752.

[FN223]. See *infra* notes 394-95 and accompanying text for further discussion of this point.

[FN224]. *Bunner III*, 75 P.3d 1, 18 (Cal. 2003). Justices Werdegar and Moreno concurred in the court's judg-

ment but took issue with Justice Brown's prior restraint analysis. See *id.* at 20-28 (Werdegar & Moreno, JJ., concurring).

[FN225]. Justice Brown opined that as long as the law under which the injunction was issued was content-neutral and the defendant violated that law, the injunction should be regarded as a content-neutral restriction on speech, not a prior restraint. *Id.* at 17-18 (majority opinion) (citing *Thomas v. Chicago Park Dist.*, 534 U.S. 316, 321-22 (2002) (holding that licensing scheme was not a prior restraint because it was “not subject matter censorship, but content-neutral time, place, and manner regulation”) and *Schenck v. Pro-Choice Network of W. N.Y.*, 519 U.S. 357, 374 n.6 (1997) (holding that preliminary injunction regulating protests outside of abortion clinic was not unconstitutional because it was issued “not because of the content of petitioners' expression... but because of their prior unlawful conduct”)).

[FN226]. *Bunner III*, 75 P.3d. at 18.

[FN227]. *Id.*

[FN228]. See e.g., *id.* at 23 n.1 (Moreno, J., concurring) (citing *Metropolitan Opera Ass'n, Inc. v. Local 100, Hotel & Rest. Employees Int'l Union*, 239 F.3d 172, 176 (2d Cir. 2001) (preliminary injunction against publication treated as a prior restraint in litigation between private parties)); see also *CBS, Inc. v. Davis*, 510 U.S. 1315, 1318 (1994) (granting emergency stay of preliminary injunction against broadcast of videotape found to contain trade secret information as unconstitutional prior restraint); *Org. for a Better Austin v. Keefe*, 402 U.S. 415, 419-20 (1971) (temporary injunction against leafleting in private litigation for invasion of privacy held to be unconstitutional prior restraint); *Bridge C.A.T. Scan Assocs. v. Technicare Corp.*, 710 F.2d 940, 946 (2d Cir. 1983) (improperly issued protective order in private litigation was unconstitutional prior restraint on speech); *Lemley & Volokh*, *supra* note 8 (citing cases and analyzing policies underlying prior restraint law). Justice Brown's treatment of the prior restraint doctrine is inconsistent with prior decisions by the California Supreme Court. See *Aguilar v. Avis Rent a Car Sys., Inc.*, 980 P.2d 846, 859-62 (Cal. 1999) (upholding permanent injunction forbidding use of racial epithets after trial on the merits, but recognizing that preliminary injunctions in civil litigations may be unconstitutional prior restraints); *Wilson v. Superior Court*, 532 P.2d 116, 120 (Cal. 1975) (preliminary injunction against distribution of newsletter held to be an unconstitutional prior restraint in libel case).

[FN229]. See *Bunner III*, 75 P.3d at 21-22 (Moreno, J., concurring) (discussing these cases).

[FN230]. See *supra* note 221 and accompanying text.

[FN231]. Douglas Lichtman, Professor, University of Chicago Law School, Comments at the Berkeley Center for Law & Technology Trade Secrecy Workshop (Oct. 13, 2006). Prof. Lichtman has suggested that perhaps liability for misappropriation in such cases should turn on whether it was really necessary for the information to be revealed as part of the news story. *Id.* However, there will be times, and the CBS tape of Federal's plant may be one of them, in which disclosure of some secret may be incidental to an otherwise significant news story. In addition, necessity often may be hotly debated. To reveal details may add credibility to a story that would otherwise seem too vague about the threat to public health or other social interest.

[FN232]. Commercial use in competition with the trade secret developer is, of course, not a necessary element for trade secret misappropriation, so the mere absence of competitive uses should not, of itself, lead courts to deny preliminary injunctions. See Restatement (Third) of Unfair Competition §40 cmt. c (1993). Yet, the ab-

sence of competitive use makes these kinds of trade secret cases different from the ordinary claim and so closer scrutiny of the claim and the injunction being sought is warranted.

[FN233]. See, e.g., *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 493 (1974); see also Epstein, *supra* note 8, at 1036-38. I agree with Professor Epstein that First Amendment “exceptionalism” should not lead courts to deny preliminary injunctions in ordinary trade secret cases.

[FN234]. This exception is akin to that which Professors Lemley and Volokh proposed for straightforward copyright infringement cases (e.g., literal copying of the whole work or unauthorized public performance where fair use is not a plausible defense). See Lemley & Volokh, *supra* note 8, at 151. *CBS, Inc. v. Davis* proposes a further exception from the prior restraint doctrine if the defendant engaged in criminal activity. See *supra* note 221 and accompanying text.

[FN235]. 876 S.W.2d 545 (Tex. App. 1994); accord *Cherne Indus., Inc. v. Grounds & Assoc., Inc.*, 278 N.W.2d 81 (Minn. 1979) (rejecting First Amendment defense in trade secret case because of defendant's breach of a confidential relationship obligation).

[FN236]. Garth, 876 S.W.2d at 547.

[FN237]. *Id.*

[FN238]. *Id.* at 549.

[FN239]. *Id.*

[FN240]. *Id.*

[FN241]. *Id.* at 550.

[FN242]. *Id.*

[FN243]. Restatement (Third) of Unfair Competition §45 cmt. c (1993) (“If a trade secret has already entered the public domain, an injunction may be appropriate to remedy any head start or other unfair advantage acquired by the defendant as a result of the misappropriation.”).

[FN244]. *Religious Tech. Ctr. v. Lerma*, 908 F. Supp. 1362, 1368 (E.D. Va. 1995) (distinguishing a preliminary injunction against a direct misappropriator from that against third party recipients, such as the Washington Post); see also *Underwater Storage, Inc. v. United States Rubber Co.*, 371 F.2d 950, 955 (D.C. Cir. 1966) (endorsing injunction against a direct misappropriator despite general publication).

[FN245]. Courts should, for example, take into account whether someone who obtains a secret by wrongful means intends to publish the secret as an act of revenge against a firm or for other wrongful purposes.

[FN246]. *CBS, Inc. v. Davis*, 510 U.S. 1315, 1318 (1994). Justice Blackmun indicated that he would recognize an exception to the prior restraints doctrine for criminal acts. *Id.* at 1316. Justice Blackmun did not explain why he made this distinction, but criminal wrongdoing may change the public interest calculus in preliminary injunction analysis. See also *State ex rel. Sports Mgmt. News, Inc. v. Nachtigal*, 921 P.2d 1304, 1309 n.8 (Or. 1996) (criminal acts might alter whether a preliminary injunction was an unconstitutional prior restraint).

[FN247]. Volokh, *supra* note 8, at 741. Yet, Volokh argued elsewhere that “as a general matter, preliminary injunctions justified by the possibility that the defendant's speech breaches a contract are no more warranted than preliminary injunctions justified by the possibility that the defendant's speech is libelous.” Lemley & Volokh, *supra* note 8, at 232. Post would seem to take issue with this position. See, e.g., Post, *supra* note 13, at 715.

[FN248]. Volokh, *supra* note 8, at 741.

[FN249]. 921 P.2d at 1309 n.8; accord *Ford Motor Co. v. Lane*, 67 F. Supp. 2d 745, 750 n.6 (E.D. Mich. 1999).

[FN250]. 501 U.S. 663 (1991); accord *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 31 (1984) (rejecting First Amendment challenge to order requiring the Times not to disclose newsworthy information disclosed under seal during discovery); *Snepp v. United States*, 444 U.S. 507, 510 (1980) (upholding injunction enforcing contract not to disclose secrets obtained during governmental service in the CIA because “Snepp's employment with the CIA involved an extremely high degree of trust”). But see *Penguin Books USA, Inc. v. Walsh*, 756 F. Supp. 770, 786-88 (S.D.N.Y. 1991) (holding that former government lawyer could publish a book on his experiences as a prosecutor notwithstanding a prepublication agreement to submit drafts for clearance by government agency; distinguishing *Snepp*).

[FN251]. *Cowles Media*, 501 U.S. at 665-66.

[FN252]. *Id.* at 671.

[FN253]. *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. *Id.* at 670. Justices Blackmun, Marshall, Souter and O'Connor dissented. *Id.* at 670 (Blackmun, J., dissenting); *id.* at 676 (Souter, J., dissenting).

[FN254]. The dissenters objected to the “talismanic” invocation of the content-neutrality of promissory estoppel, saying that “such laws may restrict First Amendment rights just as effectively as those directed specifically at speech itself,” and it was “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 (Souter, J., dissenting). But see Epstein, *supra* note 8, 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).

[FN255]. The Supreme Court has 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.” *Freedman v. Maryland*, 380 U.S. 51, 58 (1965) (striking down a motion picture licensing regime because of long delays before judicial review of decision by censorship board). 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. *Kingsley Books, Inc. v. Brown*, 354 U.S. 436, 440 (1957). Decisions such as *Kingsley* suggest that the Court would find preliminary injunctions in trade secret cases to be generally justifiable as long as standards for issuance of preliminary injunctions in trade secret cases are clear and procedures are suitably expeditious. However, these decisions predate *New York Times Co. v. United States*, 403 U.S. 713 (1971), and its progeny, and their continued precedential significance is unclear.

[FN256]. Cf. *Penguin Books USA Inc. v. Walsh*, 756 F. Supp. 770, 787 (S.D.N.Y. 1991) (concluding that un-

reasonable delays and demands for excising material by government office that was contractually entitled to pre-publication review writings of former employee about his work conflicted with the First Amendment).

[FN257]. See, e.g., Garfield, *supra* note 62, at 264-65. Jeffrey Wigand, who leaked data from Brown & Williamson Tobacco Company, is an example of this kind of informant.

[FN258]. See, e.g., *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1004-05, 1016 (1984) (holding health and safety data on fungicides to be trade secrets, although allowing the government to disclose them if necessary to inform the public about risks).

[FN259]. See *Nicholson v. McClatchy Newspapers*, 223 Cal. Rptr. 58, 63-66 (Ct. App. 1986) (holding against liability for publication of bar association evaluation of a judicial candidate, even though someone had disclosed his name to the newspapers in violation of law). The court found First Amendment protection for ordinary news-gathering activities such as “asking persons questions, including those with confidential or restricted information.” *Id.* The court ruled that conclusory allegations of conspiracy with wrongdoer “cannot serve to transform privileged behavior of the media defendants into tortious behavior.” *Id.*

[FN260]. 78 F.3d 219 (6th Cir. 1996).

[FN261]. *Id.* at 222-23.

[FN262]. Procter & Gamble learned of the impending publication when a BW reporter called to get comments on the story it was about to print. See *id.* at 224.

[FN263]. *Id.* at 222-23.

[FN264]. *Id.* The trial court's order was faxed to McGraw Hill, parent company of Business Week. *Id.* at 222.

[FN265]. *Id.*

[FN266]. *Id.* at 225. In ruling that the First Amendment did not forbid the injunction, the trial court relied on *Seattle Times Co. v. Rhinehart*, 467 U.S. 20 (1974), in which the Court upheld an order forbidding public disclosure of newsworthy information obtained during discovery. The Sixth Circuit pointed out that reliance on *Seattle Times* was “misplaced” because it concerned the rights of parties to the litigation to disseminate (or not) information obtained under a protective order during discovery, not the rights of third party journalists to publish this information. 78 F.3d at 225.

[FN267]. *Id.* (alteration in original) (quoting *In re Providence Journal Co.*, 820 F.2d 1342, 1345 (1st Cir. 1986)).

[FN268]. *Id.*

[FN269]. *Id.* at 225-26. The trial court had not even given BW notice of the hearings or an opportunity to be heard about its First Amendment interests in publication, thereby depriving BW of its due process as well as its First Amendment rights. *Id.* at 226-27. The Sixth Circuit also questioned the adequacy of the court's supervision of discovery. *Id.* at 227. One judge dissented on the ground that the matter was moot because Business Week had by then published the article. *Id.* at 229 (Brown, J., dissenting).

[FN270]. 921 P.2d 1304 (Or. 1996).

[FN271]. *Id.* at 1308-10. The Oregon Supreme Court overturned the lower court's order based on its interpretation of 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.* at 1307 n.6.

[FN272]. *Id.* at 1306.

[FN273]. *Id.* at 1308.

[FN274]. 67 F. Supp. 2d 745 (E.D. Mich. 1999). *O'Grady v. Superior Court* is factually similar to *Ford*, in that *O'Grady* published on his website information about forthcoming Apple products that Apple claimed as trade secrets, although Apple did not name *O'Grady* as a defendant. 44 Cal. Rptr. 3d 72, 80-82 (Ct. App. 2006).

[FN275]. *Ford*, 67 F. Supp. 2d at 754.

[FN276]. *Id.* at 748. The same allegation was apparently made in *Sports Management News*, although the Oregon Supreme Court did not expressly say so. See 921 P.2d at 1305-06.

[FN277]. *Ford*, 67 F. Supp. 2d at 753. The trial court in *Ford* relied heavily on *Procter & Gamble* and the substantially higher threshold it set for preliminary injunctions against third party publishers of trade secrets. *Id.* at 751-53.

[FN278]. Epstein, *supra* note 8, at 1035-46; see also Goldberg, *supra* note 8, at 271.

[FN279]. Epstein, *supra* note 8, at 1037.

[FN280]. *Id.*

[FN281]. *Ford*, 67 F. Supp. 2d at 753.

[FN282]. *Id.* at 747; see *BlueOvalNews.com*, <http://www.blueovalnews.com> (last visited Mar. 1, 2007).

[FN283]. Mainstream news organizations, such as the *Wall Street Journal*, have sometimes been threatened by trade secret litigation when they publish non-public information about companies. In one documented instance, *Procter & Gamble* persuaded Ohio law enforcement officials to undertake a criminal investigation over leaked information. See Terry M. Dworkin & Elletta S. Callahan, *Employee Disclosures to the Media: When is a "Source" a "Sorcerer" ?*, 15 *Hastings Comm. & Ent. L.J.* 357, 358 (1993).

[FN284]. Volokh, *supra* note 8, at 741. Volokh would have courts apply strict scrutiny to third party publisher cases. See *id.*

[FN285]. See, e.g., *O'Grady v. Superior Court*, 44 Cal. Rptr. 3d 72, 113-14 (Ct. App. 2006).

[FN286]. The classic Supreme Court prior restraint decisions other than *New York Times Co. v. United States* include: *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539 (1976); *Freedman v. Maryland*, 380 U.S. 51 (1965); *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58 (1963); *Near v. Minnesota*, 283 U.S. 697 (1931).

[FN287]. 403 U.S. 713 (1971). Many trade secret and free speech cases cite to the *Pentagon Papers* case. See, e.g., *CBS, Inc. v. Davis*, 510 U.S. 1315, 1317-18 (1994); *Procter & Gamble Co. v. Bankers Trust Co.*, 78 F.3d 219, 225 (6th Cir. 1996); *Ford*, 67 F. Supp. 2d at 751; *Religious Tech. Ctr. v. Lerma*, 897 F. Supp. 260, 263

(E.D. Va. 1995); *Bunner II*, 113 Cal. Rptr. 2d 338, 351 (2001). The Sports Management News decision was the only trade secret and 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. *State ex rel. Sports Mgmt. News, Inc. v. Nachtigal*, 921 P.2d 1304, 1307 n.6 (Or. 1996).

[FN288]. 532 U.S. 514 (2001).

[FN289]. *Id.* at 533-35.

[FN290]. The documents consisted of a classified study entitled “History of U.S. Decision-Making Process on Viet Nam Policy.” *Pentagon Papers*, 403 U.S. at 714.

[FN291]. See Floyd Abrams, *The Pentagon Papers a Decade Later*, N.Y. Times, June 7, 1981, §6 at 22.

[FN292]. See *Pentagon Papers*, 403 U.S. at 760 (Blackmun, J., dissenting).

[FN293]. *Id.* A three-paragraph per curiam decision preceded the nine opinions by the Justices. *Id.*

[FN294]. 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. *Id.* at 714, 720, 727, 730 (Black, J., concurring; Douglas, J., concurring; Stewart, J., concurring; White, J., concurring). Justice Harlan wrote a dissenting opinion which Chief Justice Burger and Justice Blackmun joined. *Id.* at 752 (Harlan, J., dissenting).

[FN295]. *Id.* at 714-24 (Black, J., concurring). Holding that the publication of news can be enjoined, Justice Black thought, “would make a shambles of the First Amendment.” *Id.* at 715.

[FN296]. *Id.* at 726. (Brennan, J., concurring). Justice Brennan would only have found such a restraint justified 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.* at 726-27.

[FN297]. *Id.* at 725-26.

[FN298]. *Id.* at 731-33 (White, J., concurring).

[FN299]. *Id.* at 741-43 (Marshall, J., concurring).

[FN300]. *Id.* at 743-47.

[FN301]. *Id.* at 749-51 (Burger, C.J., dissenting); *id.* at 754 (Harlan, J., dissenting).

[FN302]. *Id.* at 748-62 (Burger, C.J., Harlan & Blackmun, JJ., dissenting).

[FN303]. See, e.g., Greene, *supra* note 8, at 543-51.

[FN304]. See, e.g., *Pentagon Papers*, 403 U.S. at 762 (Blackmun, J., dissenting) (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” (quoting *United States v. Wash. Post Co.*, 446 F.2d 1327, 1330 (D.C. Cir. 1971) (Wilkey, J., dissenting))).

[FN305]. *Religious Tech. Ctr. v. Lerma*, 897 F. Supp. 260, 263 (E.D. Va. 1995); see also *Procter & Gamble Co. v. Bankers Trust Co.*, 78 F.3d 219, 225 (6th Cir. 1996); *Ford Motor Co. v. Lane*, 67 F. Supp. 2d 745, 751 (E.D. Mich. 1999).

[FN306]. In *O'Grady*, the California Court of Appeal ducked the question whether bloggers should be accorded the same degree of First Amendment protection as journalists and traditional publishers. 44 Cal. Rptr. 3d 72, 103 n.21 (Ct. App. 2006). The court declined the “implicit invitation to embroil ourselves in questions of what constitutes ‘legitimate journalis[m].’” *Id.* at 1457 (alteration in original).

[FN307]. The Uniform Trade Secrets Act provides that “[a]ctual or threatened misappropriation may be enjoined.” *Unif. Trade Secrets Act §2(a)* (amended 1985), 14 U.L.A. 619 (2005).

[FN308]. 532 U.S. 514 (2001).

[FN309]. *Id.* at 518-19.

[FN310]. *Id.* at 519.

[FN311]. *Id.* at 518-19.

[FN312]. *Id.* at 519.

[FN313]. 18 U.S.C. §2511(1)(c) (2000).

[FN314]. *Bartnicki*, 532 U.S. at 520.

[FN315]. *Id.* at 519.

[FN316]. *Id.* at 521.

[FN317]. *Id.* at 522. The cases in conflict were *Peavy v. WFAA-TV, Inc.*, 221 F.3d 158 (5th Cir. 2000), *Bartnicki v. Vopper*, 200 F.3d 109 (3d Cir. 1999), and *Boehner v. McDermott*, 191 F.3d 463 (D.C. Cir. 1999). *Bartnicki*, 532 U.S. at 521-22.

[FN318]. *Bartnicki*, 532 U.S. at 524-25.

[FN319]. *Id.* at 525.

[FN320]. *Id.* (citation omitted). Chief Justice Rehnquist and Justices Scalia and Thomas would have upheld the lower court and applied intermediate scrutiny in *Bartnicki*, under which

[t]hese 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 cellular phones. It is hard to imagine a more narrowly tailored prohibition on the disclosure of illegally intercepted communications....

Id. at 548 (Rehnquist, C.J., dissenting). The dissent characterized the “matter of ‘public concern’” limitation as “an amorphous concept that the Court does not even attempt to define.” *Id.* at 542.

[FN321]. *Id.* at 526 (plurality opinion).

[FN322]. *Id.* at 526-27 (alteration in original) (quoting *Bartnicki v. Vopper*, 200 F.3d 109, 120 (3d Cir. 1999)).

[FN323]. *Id.* at 527-28 (citing *Florida Star v. B.J.F.*, 491 U.S. 524 (1989) (no civil liability for publishing the name of a rape victim); *Smith v. Daily Mail Publ'g Co.*, 443 U.S. 97 (1979) (striking down law criminalizing publication of the name of a juvenile defendant); *Landmark Commc'ns, Inc. v. Virginia*, 435 U.S. 829 (1978) (striking down law criminalizing publication of information from confidential proceedings of state judicial review committee)). Justice Stevens also invoked *New York Times Co. v. United States* 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 (citing 403 U.S. 713 (1971)). The dissent objected to the Court's reliance on these precedents, distinguishing the first three cases from *Bartnicki* because the information there had already been publicly available and the Court's concern was about press “timidity and self-censorship.” *Id.* at 545-47 (Rehnquist C.J., dissenting) (quoting *Florida Star*, 491 U.S. at 535). In addition, the dissent found the Court's reliance on *New York Times* “mystifying” given that it involved an attempted prior restraint on speech by the government, not an action for damages. *Id.* at 555.

[FN324]. *Bartnicki*, 532 U.S. at 528 (alteration in original) (quoting *Smith*, 443 U.S. at 103).

[FN325]. *Id.* at 535, 540 (Breyer, J., concurring). Justice Breyer gave examples of situations in which disclosures of intercepted communications would not satisfy the public concern standard. *Id.* at 540.

[FN326]. None of the trade secret/First Amendment cases, for example, mentioned the public/private concern distinction. It would be inconsistent with their rulings to impose such a requirement. But the public/private concern distinction has had significance in cases involving damage awards. See, e.g., *Dun & Bradstreet, Inc. v. Greenmoss Builders*, 472 U.S. 749, 763 (1985) (holding that there was no First Amendment impediment to award of damages against non-media defendant for issuing a credit report falsely claiming that plaintiff had filed for bankruptcy, as it pertained to matters of private concern); *Connick v. Myers*, 461 U.S. 138, 140-42 (1983) (public employee seeking damages for wrongful termination after speaking out on matters the Court deemed to be of private concern); *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 334 (1974) (need for showing actual malice to justify award damages for defamation as to issues of public concern to be consistent with the First Amendment). For further discussion of damage issues, see *infra* Part V.A.

[FN327]. *Volokh*, *supra* note 8, at 747; see also *id.* at 743 (“Every time the Court has decided that certain speech is not on a matter of public concern, it has erred.”).

[FN328]. *Id.* at 747.

[FN329]. *Bunner III*, 75 P.3d 1, 15-16 (Cal. 2003) (emphasis omitted). Justice Brown pointed to dicta in *Bartnicki* that listed trade secrets among the categories of information that are matters of private concern. *Id.* at 15 (citing *Bartnicki*, 532 U.S. at 533). But as Professor *Volokh* has pointed out, some trade secrets are matters of public concern. *Volokh*, *supra* note 8, at 747-48.

[FN330]. *Bunner III*, 75 P.3d at 16.

[FN331]. Declaration of David Wagner, *Bunner I*, No. CV786804 (Super. Ct. Cal. Jan. 14, 2000), available at http://www.eff.org/IP/Video/DVDCCA_case/20000107-pi-motion-wagnerdec.html.

[FN332]. See, e.g., *Eaton-Salners*, *supra* note 101, at 284; *Touretsky*, *supra* note 94.

[FN333]. Eaton-Salners, *supra* note 101, at 282-83; Volokh, *supra* note 8, at 746-47.

[FN334]. Bunner IV, 10 Cal. Rptr. 3d 185, 189 (Ct. App. 2004) (footnote omitted).

[FN335]. See Declaration of Andrew Bunner at ¶¶ 6-8, Bunner I, No. CV786804 (Super. Ct. Cal. Jan. 14, 2000), available at http://www.eff.org/IP/Video/DVDCCA_case/20000107-pi-motion-bunnerdec.html [hereinafter Bunner Declaration].

[FN336]. *Id.* ¶ 10.

[FN337]. See Eaton-Salners, *supra* note 101, at 273, 283-84 (discussing protests related to DeCSS); see also *id.* at 284 n.110 (discussing other public policy goals served by public disclosure of CSS).

[FN338]. *United States v. Microsoft Corp.*, 253 F.3d 34, 47 (D.C. Cir. 2001).

[FN339]. See, e.g., Case COMP/C-3/37.792, *Comm'n v. Microsoft Corp.*, 2004 E.C. 299, available at <http://europa.eu.int/comm/competition/antitrust/cases/decisions/37792/en.pdf>.

[FN340]. See, e.g., James Kanter & Ken Belson, European Panel Investigates DVD-Standards Rivalry, *N.Y. Times*, Aug. 9, 2006, at C3.

[FN341]. *O'Grady v. Superior Court*, 44 Cal. Rptr. 3d 72, 114 (Ct. App. 2006) ("Apple's commitment to such a product could prove to be an important step in democratizing the production and publication of music.").

[FN342]. *Id.*

[FN343]. Bunner did not himself misappropriate CSS. See Bunner Declaration, *supra* note 335, ¶¶ 3, 7-14. He got DeCSS from one of the many public postings of this program on the Internet. See *id.* He 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. See *id.* 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. See *id.*

Even though *Bartnicki* obviously involves a very different legal claim than Bunner--violation of federal wiretap laws rather than 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 on the initial receipt and possession of it. See *Bartnicki*, 532 U.S. 514, 519 (2001); *Bunner III*, 75 P.3d 1, 7-9 (Cal. 2003). Defendants in both cases were charged as secondary wrongdoers. *Bartnicki*, 532 U.S. at 519; *Bunner IV*, 10 Cal. Rptr. 3d 185, 188-89 (Ct. App. 2004). 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. *Bartnicki*, 532 U.S. at 519-20; *Bunner III*, 75 P.3d at 7-9. 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. *Bartnicki*, 532 U.S. at 519-20; *Bunner III*, 75 P.3d 1, 7-9.

In addition, 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. Holding *Bunner* and others liable for republishing DeCSS source code will no more

deter youngsters from reverse engineering encryption software 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 at issue in Bunner was a preliminary injunction. See *supra* note 326 and accompanying text. 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. See *Bunner III*, 75 P.3d at 6-8. 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. *Id.* 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.

[FN344]. *Shoen v. Shoen*, 5 F.3d 1289, 1293 (9th Cir. 1993) (alteration in original) (quoting *von Bulow v. von Bulow*, 811 F.2d 136, 144 (2d Cir. 1987)).

[FN345]. See *United States v. Genovese*, 409 F. Supp. 2d 253, 256 (S.D.N.Y. 2005) (rejecting First Amendment defense to Economic Espionage Act (EEA) prosecution for trade secret misappropriation for posting Microsoft source code on the Internet and charging a fee for sharing it with others); see also Press Release, Microsoft, Statement from Microsoft Regarding Illegal Posting of Windows 2000 Source Code (Feb. 12, 2004), <http://www.microsoft.com/presspass/press/2004/feb04/02-12windowssource.mspx> (announcing illegal postings of Windows source code).

[FN346]. There is some risk that this standard would facilitate the "laundering" of misappropriated information. That is, 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. Yet, in cases like this, courts would likely consider X and Y to be in league as direct misappropriators. The Court rejected a similar line of reasoning in *Bartnicki*. See 532 U.S. at 529-31. If courts require the information to be newsworthy and there is a risk of civil or criminal liability for wrongfully publishing trade secrets, the laundering risk should be minimal.

[FN347]. *Lemley & Volokh*, *supra* note 8, at 230.

[FN348]. 410 F. 2d 701 (D.C. Cir. 1968). Drew Pearson and Jack Anderson, the columnists, were aware that the documents had been purloined. *Id.* at 705. The D.C. Circuit also reversed the trial court's ruling that the columnists were liable for conversion of the documents on the ground that the columnists had received copies of the documents, not the originals which were returned to Dodd's office. *Id.* at 708. *Boehner v. McDermott*, another D.C. Circuit decision, is arguably in conflict with *Pearson*. 441 F.3d 1010 (D.C. Cir. 2006). In its first *Boehner* decision, *Boehner v. McDermott*, the D.C. Circuit rejected Congressman McDermott's First Amendment defense to a claim for damages arising from wiretap charges for McDermott's public disclosure of the contents of a cell-phone conversation that he received from the private citizens who intercepted it. 191 F.3d 463, 475-78 (D.C. Cir. 1999). In the call, *Boehner* and other Republican leaders discussed ethics violation charges against Newt Gingrich and whether Gingrich should accept a reprimand without a hearing being held on the charges. *Id.* at 465. The Supreme Court reversed the D.C. Circuit and remanded *Boehner* for further consideration in light of

Bartnicki. *Boehner v. McDermott*, 532 U.S. 1050 (2001). On remand, McDermott was ordered to pay \$60,000 in damages and more than half a million dollars in attorney fees. See *Boehner v. McDermott*, 441 F.3d 1010, 1011 (D.C. Cir. 2006). The D.C. Circuit, with a 2-1 split, affirmed. *Id.* at 1017. Judge Sentelle dissented on the ground that the ruling was inconsistent with Bartnicki:

Under the rule proposed by Representative Boehner, no one in the United States could communicate on this topic of public interest because of the defect in the chain of title. I do not believe the First Amendment permits this interdiction of public information either at the stage of the newspaper-reading public, of the newspaper-publishing communicators, or at the stage of Representative McDermott's disclosure to the news media.

Id. at 1022 (Sentelle, J., dissenting). The D.C. Circuit has agreed to rehear the case en banc. *Boehner v. McDermott*, No. 04-7203 (D.C. Cir. June 23, 2006).

[FN349]. See *Florida Star v. B.J.F.*, 491 U.S. 524, 532 (1989) (holding that First Amendment shielded newspaper from liability for damages for publishing the name of a crime victim in violation of a law protecting the anonymity interests of crime victims because the newspaper obtained the name from a police bulletin board that negligently revealed the name); *Food Lion v. Capital Cities/ABC*, 194 F.3d 505, 510 (4th Cir. 1999) (affirming dismissal of fraud and unfair trade practices claims against ABC for assigning agents to become employees of a food handling firm in order to obtain information about its practices for a news story, but allowing claim for damages for breach of employees' duty of loyalty to proceed). But see Epstein, *supra* note 8, at 1018-23 (criticizing Desnick and Food Lion).

[FN350]. See *supra* note 333 and accompanying text.

[FN351]. 472 U.S. 749, 763 (1985).

[FN352]. *Id.* at 751.

[FN353]. *Id.* at 752.

[FN354]. *Id.* *Dun & Bradstreet* relied on *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 334 (1974) (showing of actual malice necessary to justify award damages for defamation). The Court ruled that the *Gertz* actual malice standard only applied when the defamation pertained to matters of public concern. *Dun & Bradstreet, Inc.*, 472 U.S. at 760.

[FN355]. *Dun & Bradstreet, Inc.*, 472 U.S. at 757-61.

[FN356]. *Bunner III*, 75 P.3d 1, 15 (Cal. 2003) (quoting *Bartnicki v. Vopper*, 532 U.S. 514, 533 (2001)).

[FN357]. *Id.* Volokh is critical of Bartnicki for its characterization of trade secrets as matters of private concern, noting that “[i]t would be a shame if the Court's casual, offhanded dictum led lower courts to quickly uphold the ban on third-party publication of trade secrets based on an unsupported assertion about their inherent ‘private concern’ status.” Volokh, *supra* note 8, at 743.

[FN358]. Bartnicki, 532 U.S. at 539 (Breyer, J., concurring) (citing Restatement (Third) of Unfair Competition §40 cmt. c (1993)).

[FN359]. Yet, the Court in *Cohen v. Cowles Media Co.* ruled that the First Amendment permits damage awards to persons harmed by the breach of a promise not to disclose newsworthy secret information. 501 U.S. 663, 668-72 (1991). The Court did so without regard to the public/private concern distinction. See *supra* notes 240-42

and accompanying text.

[FN360]. 44 Cal. Rptr. 3d 72 (Ct. App. 2006). Exhaustion of alternative sources was a factor in the balancing test. *Id.* at 109-13.

[FN361]. *Id.* at 77-78.

[FN362]. *Id.* at 80.

[FN363]. *Id.* at 79.

[FN364]. *Id.* at 80. Apple implied that O'Grady might be a misappropriator but did not name him as a defendant. *Id.*

[FN365]. *Id.* at 80-81.

[FN366]. *Id.* at 81.

[FN367]. *Id.* at 76.

[FN368]. *Id.* at 82-116 (also ruling that disclosure would violate the Stored Communications Act, 18 U.S.C. §§2701-2712 (2000), and the California reporter "shield" law).

[FN369]. *Id.* at 105.

[FN370]. *Id.* at 106. An amicus brief asserted that bloggers had equally strong claims to be treated as traditional journalists. *Id.* at 103 n.21. The court did not find it necessary to decide this question, although it did distinguish O'Grady's regular publication from blogging. *Id.*

[FN371]. *Id.* at 106-08.

[FN372]. See 690 P.2d 625, 631-34 (Cal. 1984). Mitchell was a libel action in which the California Supreme Court ruled that reporters, editors, and publishers had a conditional privilege not to disclose confidential sources and unpublished information provided by the sources; it set forth factors to be weighed in determining whether the privilege should shield the disclosure. *Id.* at 629-34.

[FN373]. O'Grady, 44 Cal. Rptr. 3d at 106-07.

[FN374]. *Id.* at 107.

[FN375]. *Id.* at 107-08.

[FN376]. *Id.* at 108. The information could, for instance, have been sent to O'Grady anonymously. *Id.*

[FN377]. *Id.* at 109.

[FN378]. *Id.* (quoting Mitchell, 690 P.2d at 633-34).

[FN379]. *Id.* at 109.

[FN380]. *Id.* at 110.

[FN381]. *Id.*

[FN382]. *Id.* at 112.

[FN383]. *Id.*

[FN384]. *Id.* (questioning the categorical proposition); *id.* at 114 (explaining why Asteroid was not only news-worthy but a matter of public concern).

[FN385]. *Id.* at 112-13.

[FN386]. *Id.* at 115.

[FN387]. *Id.*

[FN388]. *Id.*

[FN389]. See, e.g., Lemley & Volokh, *supra* note 8, at 158-65 (discussing the general standard). Courts sometimes also consider various other factors in determining whether to issue injunctions in trade secret cases. See Restatement (Third) of Unfair Competition §44(2) (1993).

[FN390]. *CBS, Inc. v. Davis*, 510 U.S. 1315, 1316 (1994).

[FN391]. *Greene*, *supra* note 8, at 553-54.

[FN392]. *Id.* at 553-55.

[FN393]. See *supra* notes 211-12 and accompanying text.

[FN394]. *CBS, Inc.*, 510 U.S. at 1317.

[FN395]. See, e.g., *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 342 (1974) (clear and convincing evidence needed in public figure libel cases); Lemley & Volokh, *supra* note 8, at 215-16 (arguing that heightened standards of proof should be required in prior restraint cases).

[FN396]. 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 whose consequences resemble those of not enjoining disclosure of trade secrets on First Amendment grounds).

[FN397]. U.S. Const. art. I, §8, cl. 8.

[FN398]. But see *Religious Tech. Ctr. v. Netcom On-line Commc'n Servs., Inc.*, 923 F. Supp. 1231, 1257-58 (N.D. Cal. 1995) (applying generally applicable standard, but finding against a likelihood of success on the merits in case involving republication of secrets on the Internet by non-misappropriating third party who raised First Amendment defense).

[FN399]. *Bunner III*, 75 P.3d 1, 20 (Cal. 2003). Justices Werdegar and Moreno agreed about the need for appellate courts to undertake an independent review of the record to ensure that the “factual predicates for injunctive

relief truly exist.” *Id.* at 20-21 (Werdegar & Moreno, JJ., concurring).

[FN400]. Another aspect of First Amendment due process that should be followed in trade secrecy cases where preliminary injunctions implicate First Amendment rights is expeditious appellate review. More than four years passed between the trial court's issuance of preliminary injunction against Bunner's posting of DeCSS on the Internet and the reversal of the preliminary injunction by the Court of Appeal. Given that the injunction was erroneously granted, it seems unjust that Bunner had to wait such a long time to be vindicated. See, e.g., Lemley & Volokh, *supra* note 8, at 179-80 (stressing importance of prompt appellate review of preliminary injunctions against publication).

[FN401]. Bunner III, 75 P.3d at 20.

[FN402]. *Id.* (citing *Bose Corp. v. Consumers Union of the U.S., Inc.*, 466 U.S. 485 (1984)) (holding that to comport with the First Amendment, appellate courts should undertake independent review of constitutionally relevant facts pertinent to a trade libel allegedly committed by Consumer Reports as to Bose products). The California Supreme Court did not use the term “First Amendment due process,” but the term is a useful way of understanding the nature of this principle. See Henry P. Monaghan, *First Amendment “Due Process”*, 83 *Harv. L. Rev.* 518 (1970).

[FN403]. Eugene Volokh & Brett McDonnell, *Freedom of Speech and Independent Judgment Review in Copyright Cases*, 107 *Yale L.J.* 2431, 2437 (1998); *id.* at 2432 (“As courts see more cases of a particular type, they refine the line between protected speech (such as non-obscene art, innocent error, or copying of ideas) and unprotected speech (such as obscenity, punishable libel, or copying of expression).”).

[FN404]. *Id.* at 2432.

[FN405]. Bunner III, 75 P.3d at 20.

[FN406]. Bunner IV, 10 *Cal. Rptr. 3d* 185, 196 (Ct. App. 2004).

[FN407]. *Id.*

[FN408]. *Id.*; accord Bunner III, 75 P.3d at 24 (Moreno, J., concurring) (“The majority recognizes that a preliminary injunction against the disclosure of an alleged trade secret without sufficient evidentiary support is an unlawful prior restraint.”).

[FN409]. The Court of Appeal in Bunner IV did not mention the preliminary or permanent injunction against posting of DeCSS in *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 436 (2d Cir. 2001), let alone its view on the consistency of either injunction with First Amendment principles. See *supra* note 94 for a distinction between the injunctions in Bunner and Corley.

[FN410]. See, e.g., *Kewanee Oil Co. v. Bircon Corp.*, 416 U.S. 270, 474 (1974).

[FN411]. See, e.g., Bunner I, No. CV 786804, 2000 WL 48512 (Super. Ct. Cal. Jan. 21, 2000) (preliminary injunction lacked a limiting provision about Bunner's right to disclose CSS secrets revealed in DeCSS if this information became public).

[FN412]. See, e.g., *Conmar Prod. Corp. v. Universal Slide Fastener Co.*, 172 F.2d 150, 156-57 (2d Cir. 1949)

(injunction unavailable once trade secrets have been disclosed in a patent).

[FN413]. See, e.g., *Bridge C.A.T. Scan Assocs. v. Technicare Corp.*, 710 F.2d 940, 945-47 (2d Cir. 1983) (overturning order forbidding disclosure of information claimed as trade secret, but gathered by the plaintiff from independent sources on grounds that plaintiff had First Amendment rights to disclose this information and that court order was unjustifiable as a prior restraint).

[FN414]. Restatement (Third) of Unfair Competition §44 cmt. f (1993).

[FN415]. See, e.g., J.H. Reichman, *Legal Hybrids Between the Patent and Copyright Paradigms*, 94 Colum. L. Rev. 2432, 2438-39 (1994) (discussing the lead time functions of trade secrecy law).

[FN416]. See, e.g., *Syntex Ophthalmics, Inc. v. Tsuetaki*, 701 F.2d 677 (7th Cir. 1983) (enjoining misappropriation for time necessary to obtain information by proper means).

[FN417]. See, e.g., Restatement (Third) of Unfair Competition §44 cmt. f (1993) (“[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.”).

[FN418]. See, e.g., *Bunner I*, No. CV 786804, 2000 WL 48512, at *3 (Super. Ct. Cal. Jan. 21, 2000). Judge Elfving did not explain his reasons for the unlimited duration of the injunction. Perhaps he accepted DVD CCA's contention that reverse engineering of CSS could not be done lawfully anywhere 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. But this is highly contestable.

[FN419]. In rare circumstances, courts may believe the secret cannot be lawfully obtained by proper means, but a court should have to justify any injunction lacking in durational limits or limiting use or disclosure in excess of the estimated time it would take to acquire the secrets by proper means.

[FN420]. See, e.g., *Computer Assoc. Int'l v. Altai, Inc.*, 982 F.2d 693 (2d Cir. 1992) (establishing clean room established after former Computer Associates employee misappropriated Computer Associate's code while working for Altai).

[FN421]. See, e.g., *Bd. of Tr. of Stanford Univ. v. Sullivan*, 773 F. Supp. 472, 474 (D.D.C. 1991) (“[T]he First Amendment protects scientific expression and debate just as it protects political and artistic expression.”); Joseph P. Liu, *The DMCA and the Regulation of Scientific Research*, 18 Berkeley Tech. L.J. 501, 504 (2003) (to protect scientific inquiry, DMCA anti-circumvention rules should be construed narrowly).

[FN422]. See *supra* Part II.B concerning the enforceability of anti-reverse engineering clauses in license agreements.

[FN423]. The European Union 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). This aspect of the Directive could not be enforced in the United States consistent with the First Amendment.

[FN424]. See *supra* notes 25-30 (discussing *Chicago Lock Co. v. Fanberg*, 676 F.2d 400 (9th Cir. 1981)).

[FN425]. 103 S.W.3d 478 (Tex. Ct. App. 2003).

[FN426]. *Id.* at 480.

[FN427]. *Id.* at 481.

[FN428]. *Id.* at 483.

[FN429]. *Id.* at 481.

[FN430]. *Id.*

[FN431]. *Id.*

[FN432]. *Id.* at 483.

[FN433]. 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 8, at 1046. However, trade secrecy law is more limited in its reach than Epstein is willing to admit. 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.

58 Hastings L.J. 777

END OF DOCUMENT