

The Secret Life of Patents

Jason Mazzone* & Matthew Moore⁺

I. INTRODUCTION

Secrecy is not a characteristic of the age in which we live. The Internet brings virtually endless information to our laptops and cell phones. Websites make both facts and falsehoods available at a keystroke, often without any indication of which is which. Use of e-mail and instant messaging has eroded physical distances and social barriers. GPS devices help us navigate streets and forests, while enabling other people to know exactly where we are. Computers collect and analyze our online browsing and buying habits. Court cases, property prices, campaign contributions, and other governmental records of our lives are all available for anyone with a web browser and an interest to read. Blogs, chat rooms, and webcams let strangers into our minds and into our homes. With increasing popularity, social networking sites encourage people to volunteer personal information—from their demographic characteristics to their musical tastes—for strangers to peruse.

Most of the time, we welcome and thrive on this kind of openness. Yet just as new technologies allow us to connect and to share with other people, the same technologies also make it more difficult to keep private those things we do not want others to know. Most private information has little value to anyone else—even when the information is vulnerable, no one has an incentive to discover it or tell others about it. However, certain secrets are valuable; in fact, some are worth billions of dollars to their keepers. The secret recipes that built the Coca-Cola Company and PepsiCo are obvious examples. Many other individuals, proprietors, and entities hold commercially valuable secrets, such as a formula or method, a blueprint, a customer list, a database, a developing invention, or the results of clinical trials. Though it is hard to quantify

* Associate Professor of Law, Brooklyn Law School. Professor Mazzone teaches constitutional law and intellectual property law. He is the author of *Copyfraud and Other Abuses of Intellectual Property*, forthcoming from Stanford University Press in 2009.

⁺ J.D. Candidate 2009, Brooklyn Law School. Mr. Moore has worked in the music business for more than a decade. His work has included protection and enforcement of recording artists' royalty rights, music publishing, and various positions at both major and independent record labels in New York and London. The authors are grateful to Tom Volper for his helpful suggestions. This article was supported, in part, by a Dean's Summer Research Stipend from Brooklyn Law School. Gary Miller provided excellent research assistance.

the total value of trade secrets to the United States economy, it is safe to say that corporations consider their trade secrets to be important assets.¹

Enter trade secret law, an amorphous state law doctrine, which offers protection for certain kinds of information that confers value on the person or enterprise keeping the information secret. Secrecy is the touchstone of a trade secret—once information becomes public, the law's protections evaporate. Therefore, the protection trade secret law provides is often only as strong as the ability of the person or enterprise holding the secret to keep it secure. In the digital age, one characterized by openness and the free flow of information, it would not be surprising to find that trade secrets have declining popularity—that, like other kinds of secrets, they are relics of an earlier and less public era. Yet some commentators, notably Professor Karl Jorda,² argue for *greater* reliance upon trade secret law today and in the future.

According to Professor Jorda, trade secret law offers corporations under-utilized protections for their intellectual property.³ As a general matter, he argues that rights stemming from more than one intellectual property doctrine can overlap.⁴ In order to protect their interests, inventors, authors, and their corporate employers should exploit these overlaps.⁵ With respect to corporations that have valuable inventions, Jorda argues that these corporations can—and should—make *simultaneous* use of patent law and trade secret law to protect their intellectual assets.⁶ Rather than view patents and trade secrets as serving different purposes, Jorda contends that corporations should treat patent and trade secret rights as providing complementary and mutually reinforcing protections.⁷ Under this approach, patent law provides core protections for an invention, while trade secret law serves to protect non-patentable knowledge associated with the invention.⁸ According to Professor Jorda, a corporation should make trade secrets a key component of its strategy to protect its assets and to enhance its interests.⁹

This article challenges the claim that trade secret law can and should play an increased role in safeguarding intellectual property today. In our view, although trade secret law will continue to be useful in certain circumstances, it remains—and should remain—of limited sig-

1. See United States Patent and Trademark Office (USPTO), *Are You a Small Business?*, <http://www.uspto.gov/smallbusiness> (last visited Sept. 21, 2008) (noting that theft of intellectual property costs United States businesses roughly \$250 billion annually).

2. See generally Karl F. Jorda, *Patent and Trade Secret Complementariness: An Unsuspected Synergy*, 48 WASHBURN L.J. 1 (2008).

3. *Id.* at 4.

4. *Id.* at 13.

5. *Id.* at 12-15.

6. *Id.* at 15.

7. *Id.* at 18.

8. *Id.* at 18-19.

9. See generally *id.*

nificance. This is for two reasons. First, as a practical matter, the digital age makes trade secrets more vulnerable. It facilitates disclosure by demolishing barriers that once prevented access to and sharing of information. Likewise, the digital age also makes disclosure more costly. In the past, a leak could be contained. Today, mass disclosure, an irreversible loss, is just an e-mail away.

Second, from a policy perspective, greater reliance on trade secrets presents the risk of overreaching; that is, the use of the law to claim protections beyond those the law actually confers. Overreaching, a problem found increasingly in other areas of intellectual property law, upsets the balance between intellectual property rights and the public domain. In arguing against the proposal for increased reliance on trade secrets, this article draws lessons from current trends in copyright law. Specifically, owners of creative works who are dissatisfied with the protections that copyright law confers are increasingly turning to contract law to augment their rights and claim protections beyond those that copyright law itself provides. These actions undermine the public domain. The experience of using contract law to augment copyright law highlights similar public costs that may result from aggressive use of trade secret law to augment patent protections. A diminished role for trade secrets, which is likely in the digital age, would therefore be a welcome development.

More generally, another disadvantage of increased reliance on trade secrets is that trade secret law is not on par with patent law. Federal law, superior to state law, expresses a clear preference for the inventor who discloses an invention to the public and obtains a patent over the inventor who keeps the invention a secret. State trade secret law must not undermine the policy of disclosure that Congress has adopted.

Part II of this article sets out the elements of trade secret and patent law that are relevant to the subsequent discussion. Part III shows why trade secret law faces substantial barriers in the digital age. Drawing on experience in the copyright context, Part IV highlights the risks that an increased reliance on trade secret law presents. Part V discusses the benefits of an integrated approach to intellectual property law while noting the dangers of integrating state trade secret law with federal law.

II. TRADE SECRETS AND PATENTS

Some background on trade secret law helps to set the stage for the claims of this article. This section provides a brief overview of the origins and scope of trade secret protections and contrasts trade secret law with other forms of intellectual property law.

A. Origins

Federal law governs copyrights, patents, and trademarks.¹⁰ Trade secret law, unlike its bigger brothers, is state law.¹¹ Each state, individually, determines whether and how to protect trade secrets, with the result that there is no single body of trade secret law. Within the states, trade secret law originated as common law—judicial decisions by the judges of a state developed a body of trade secret doctrines applicable in that state.¹²

Efforts to impose interstate order have proved challenging. In 1939, the first Restatement of Torts, widely relied upon by state courts, included a section on trade secrets that sought to synthesize the doctrines of trade secret law generated by state judges.¹³ Forty years later, the reporters of the Restatement (Second) of Torts, published in 1979, concluded that trade secrets were not properly a concern of tort law at all and omitted the subject.¹⁴ That same year, with renewed calls to harmonize state practices, the National Conference of Commissioners on Uniform State Laws published the first Uniform Trade Secrets Act (UTSA).¹⁵ Following feedback and criticism, the Conference published a revised Uniform Act in 1985.¹⁶ A decade later, trade secret law found an additional home as part of the Restatement (Third) of Unfair Competition.¹⁷

Meanwhile, efforts to identify the theoretical basis for trade secret

10. See 17 U.S.C. §§ 101 to 810, 1001 to 1101 (2006) (copyrights); 35 U.S.C. §§ 100 to 318 (2000) (patents); 15 U.S.C. §§ 1051 to 1129 (2006) (trademarks). With respect to trademarks, in addition to federal law, states have trademark statutes, deceptive trade practices statutes, and dilution statutes. See generally J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION §§ 22.1–22.10 (4th ed. 2008) (providing an overview of state trademark laws). State copyright laws protect sound recordings made prior to February 15, 1972. See 17 U.S.C. § 301(e) (providing that “[w]ith respect to sound recordings fixed before February 15, 1972, any rights or remedies under the common law or statutes of any State shall not be annulled or limited by this title until February 15, 2067” and that “no sound recording fixed before February 15, 1972, shall be subject to copyright under this title before, on, or after February 15, 2067”).

11. The sole exception is the Economic Espionage Act of 1996, 18 U.S.C. § 1831, which criminalizes the theft of certain kinds of trade secrets. Prosecution under the Act is rare. See U.S. Dep’t of Justice, Computer Crime & Intellectual Property Section, *Economic Espionage Act (EEA) Cases*, <http://web.archive.org/web/20071229062522/http://www.cybercrime.gov/eeapub.htm> (last visited Oct. 16, 2008) (listing cases prosecuted under § 1831 from 1997–2005); Jordan Robertson, *Engineer Is First Sentenced for Economic Espionage*, USA TODAY, June 18, 2008, available at http://www.usatoday.com/tech/products/2008-06-18-4083753379_x.htm (reporting that on June 18, 2008, Xiaodong Sheldon Meng was the first person sentenced under the Economic Espionage Act).

12. The first reported United States decision describing trade secrets appears to be *Peabody v. Norfolk*, 98 Mass. 452, 458 (1868) (“If [a person] invents or discovers, and keeps secret, a process of manufacture, whether a proper subject for a patent or not, he has not indeed an exclusive right to it as against the public, or against those who in good faith acquire knowledge of it; but he has a property in it, which a court of chancery will protect against one who in violation of contract and breach of confidence undertakes to apply it to his own use, or to disclose it to third persons.”).

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

14. See UNIF. TRADE SECRETS ACT, Prefatory Note, 14 U.L.A. 530–32 (2005); RESTATEMENT (SECOND) OF TORTS (1979) (omitting prior-included section on trade secrets).

15. See UNIF. TRADE SECRETS ACT, Historical Notes, 14 U.L.A. 530.

16. See *id.*

17. RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 39–45 (1995).

law also yielded various approaches. While the usual justification for patent protections is that they provide incentives to innovate,¹⁸ such incentives may be only a weak justification for trade secret law.¹⁹ Courts and commentators have therefore offered a variety of other justifications for trade secret law, finding its heritage in contract,²⁰ the tort of unfair competition,²¹ property theory,²² commercial ethics,²³ and privacy.²⁴

18. See U.S. CONST. art. I, § 8 (giving Congress power “[t]o promote the progress of science and useful arts, by securing for limited times to . . . inventors the exclusive right to their respective . . . discoveries”); *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 480 (1974) (“The patent laws promote . . . progress by offering a right of exclusion for a limited period as an incentive to inventors to risk the often enormous costs in terms of time, research, and development.”).

19. Whether trade secret law promotes innovation is disputed. The first Restatement of Torts rejected innovation as a justification for protecting trade secrets:

The patent monopoly is a reward to the inventor. But such is not the case with a trade secret. Its protection is not based on a policy of rewarding or otherwise encouraging the development of secret processes or devices. The protection is merely against breach of faith and reprehensible means of learning another’s secret.

RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939). The Supreme Court has suggested, however, that with respect to innovations not eligible for patent protection, “[t]rade secret law will encourage invention in areas where patent law does not reach, and will prompt the independent innovator to proceed with the discovery and exploitation of his invention. Competition is fostered and the public is not deprived of the use of valuable, if not quite patentable, invention.” *Kewanee Oil*, 416 U.S. at 485; see also RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. a (“[T]he protection of trade secrets has been justified as a means to encourage investment in research by providing an opportunity to capture returns from successful innovations.”). Commentators have expressed different views on this issue. See, e.g., Michael Abramowicz & John F. Duffy, *Intellectual Property for Market Experimentation*, 83 N.Y.U. L. REV. 337, 391 (2008) (arguing that “the goal of trade secret law is not to encourage the production of . . . information so much as the production of . . . business”); Vincent Chiappetta, *Myth, Chameleon or Intellectual Property Olympian? A Normative Framework Supporting Trade Secret Law*, 8 GEO. MASON L. REV. 69, 88–90 (1999) (discussing the weaknesses of treating trade secret law as encouraging innovation); Richard A. Epstein, *The Constitutional Protection of Trade Secrets Under the Takings Clause*, 71 U. CHI. L. REV. 57, 57 (2004) (“[T]he logic for protecting trade secrets parallels that for protecting patents and copyrights. People will not develop certain forms of information at private cost if the benefits of that information can be immediately socialized by the unilateral actions of others.”); Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTEL. PROP. L. REV. 1, 26–27 (2007) (arguing that “creating incentives to innovate is a very minor justification of trade secret law” because, assuming there is no law requiring forced disclosure, owners of valuable information already have an incentive to make investments to keep it secret and so trade secret law does not provide them with any additional reward).

20. See, e.g., Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CAL. L. REV. 241, 283–90 (1998) (arguing that contract is the only viable justification for trade secret law).

21. See, e.g., Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777, 805–08 (2007) (explaining trade secret law as based in unfair competition).

22. See, e.g., 1 ROGER M. MILGRIM, *MILGRIM ON TRADE SECRETS* 73-98 (2006) (describing trade secrets as property).

23. See *Kewanee Oil*, 416 U.S. at 481 (describing the “maintenance of standards of commercial ethics” as a reason for trade secret law).

24. See, e.g., *id.* (“The maintenance of standards of commercial ethics and the encouragement of invention are the broadly stated policies behind trade secret law.”); *Pioneer Hi-Bred Int’l v. Holden Foundation Seeds*, 35 F.3d 1226, 1238 n.42 (8th Cir. 1994) (“[B]y labeling certain wrongful, if not actually otherwise illegal, acts ‘improper,’ trade secret law plays an important role in regulating commercial behavior.”); *Burten v. Milton Bradley Co.*, 763 F.2d 461, 467 (1st Cir. 1985) (“The underlying goal of the law which protects trade secrets, like that which protects copyrights and patents, is to encourage the formulation and promulgation of ideas by ensuring that creators of ideas benefit from their creations.”); see also RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39, cmt. a (“[T]he protection afforded under the law of trade secrets against breaches of confidence and improper physical intrusions furthers the interest in personal privacy.”).

B. *The Uniform Trade Secrets Act*

In discussing trade secrets, this article relies principally on the UTSA, adopted by forty-six states, the District of Columbia, and the U.S. Virgin Islands.²⁵ Although not an all-encompassing approach, relying on the UTSA is a useful way to limit and organize the discussion.²⁶ The UTSA defines “trade secret” very broadly as:

[I]nformation, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.²⁷

Rather than provide a definitive catalog of information that qualifies for protection, the UTSA defines a trade secret in terms of the two identified criteria: information that (1) confers at least potential economic value as a result of being kept secret; and (2) is subject to reasonable efforts to keep it secret.²⁸

Assuming information qualifies as a trade secret, the UTSA makes it unlawful to misappropriate the trade secret.²⁹ Here, again, the UTSA takes a broad approach. Under the UTSA, misappropriation occurs in scenarios involving acquisition, use, and disclosure of the trade secret—or some combination of these actions. The UTSA defines “misappropriation” as:

(i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

25. See UNIF. TRADE SECRETS ACT, Table of Jurisdictions Wherein Act Has Been Adopted, 14 U.L.A. 529–30 (2005) (reporting states which have adopted the Act).

26. It is important to keep in mind that the laws of the adopting states are not entirely uniform. See National Conference of Commissioners on Uniform State Laws (NCCUSL), *A Few Facts About the Uniform Trade Secrets Act*, http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-utsa.asp (last visited Oct. 16, 2008) (listing separately the states that adopted the 1979 UTSA and the states that adopted the UTSA with 1985 amendments); NCCUSL, *Why States Should Adopt the Uniform Trade Secrets Act*, http://www.nccusl.org/nccusl/uniformact_why/uniformacts-why-utsa.asp (last visited Oct. 16, 2008) (noting that “[s]tates without the UTSA now depend on the common law to resolve disputes over misappropriation of trade secrets”). Some states adopted the 1979 version of the UTSA and some adopted the 1985 version, while others adopted a “homemade” combination of the two. Individual states have also customized provisions of the Act to suit their own tastes. UNIF. TRADE SECRETS ACT, General Statutory Note, 14 U.L.A. 533–35 (2005). In addition, the first Restatement of Torts continues to influence the law of trade secrets in some states. See *id.* at 531 (noting that “[t]he Uniform Act codifies the basic principles of common law trade secret protection”). States that have not adopted the Act rely on common law standards, which are articulated in the Restatement. Cf. *id.* These states are Massachusetts, New Jersey, North Carolina, and Texas. See *A Few Facts, supra*. Further, in codifying common law rules, the Act relied heavily on the Restatement itself; courts therefore use the Restatement to interpret the Uniform Act.

27. UNIF. TRADE SECRETS ACT § 1(4), 14 U.L.A. 538.

28. Some states that have adopted the Uniform Act omit the requirement that the information not be “readily ascertainable.” See, e.g., CAL. CIV. CODE § 3426.1 (West 1997). In California, a defendant in a misappropriation action can assert as a defense that the information was readily ascertainable so long as the defendant ascertained the information lawfully. *Sargent Fletcher, Inc. v. Able Corp.*, 3 Cal. Rptr. 3d 279, 287 (Cal. Ct. App. 2003).

29. UNIF. TRADE SECRETS ACT §§ 2–3, 14 U.L.A. 619, 633–34.

(ii) disclosure or use of a trade secret of another without express or implied consent by a person who

(A) used improper means to acquire knowledge of the trade secret; or

(B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was

(I) derived from or through a person who had utilized improper means to acquire it;

(II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or

(III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or

(C) before a material change of his position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.³⁰

Several of the above provisions require the use of “improper means” to trigger liability. Under the UTSA, “‘improper means’ include theft, bribery, misrepresentation, breach, or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means.”³¹

It therefore follows that under the UTSA, three general categories of behavior give rise to liability. First, acquiring a trade secret with actual or imputed knowledge that the secret was obtained from the owner by improper means violates the statute. Second, a party is liable for disclosing or using a trade secret if the party knew or should have known one of three things: (a) the party’s knowledge of the trade secret derives from a person who used improper means to acquire the secret; (b) the party acquired the secret by virtue of a duty to keep it secret or limit its use; or (c) the secret was derived from someone else who owed a duty to the owner of the trade secret. Third, a party is liable for using or disclosing the secret if the party knew or should have known that the secret was mistakenly or accidentally disclosed. Under the UTSA, a trade secret owner can seek injunctive relief to prevent actual or threatened misappropriation,³² as well as compensatory damages for misappropriation.

30. *Id.* § 1(2), 14 U.L.A. 537.

31. *Id.* § 1(1), 14 U.L.A. 537.

32. *See id.* § 2(a), 14 U.L.A. 619 (providing that “[a]ctual or threatened misappropriation may be enjoined”). Consistent with the requirement of secrecy for trade secret protection, the provision further provides that “[u]pon application to the court, an injunction shall be terminated when the trade secret has ceased to exist, but the injunction may be continued for an additional reasonable period of time in order to eliminate commercial advantage that otherwise would be derived from the misappropriation.” *Id.*; *see also* *Morlife, Inc. v. Perry*, 66 Cal. Rptr. 2d 731, 733–34 (Cal. Ct. App. 1997) (enjoining misappropriation of an employer’s customer list after it was used by former employees to solicit customers for their new business); *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1271 (7th Cir. 1995) (holding that an employer may prove a claim of trade secret misappropriation by demonstrating that an employee’s new job will inevitably lead her to rely on her former employer’s trade secrets, even if she has not yet done so).

tion,³³ and, in some circumstances, punitive damages.³⁴

C. Lawful Uses of Trade Secrets

Although the UTSA defines trade secrets broadly and creates liability under several different circumstances, the statute's reach also has some significant limitations. Many uses of trade secrets do not give rise to liability for misappropriation. Consider a hypothetical individual—we will call her Vanessa—who acquires a trade secret. She does so in a way that does not constitute improper means under the statute and without violating a duty she owed to the trade secret owner. Vanessa has not misappropriated the trade secret so long as her acquisition meets two additional conditions: (1) she did not acquire the secret from someone she knows used improper means or breached a duty in obtaining or disclosing the secret; and (2) she did not know the secret was inadvertently made available. The most important practical effect is that Vanessa, or any other person who comes across a trade secret while accessing the Internet, is not likely to be liable under the Act. In other words, once a trade secret is distributed by mass e-mail or is posted on a publicly accessible blog or web page, the secret is available for others to use.³⁵

33. UNIF. TRADE SECRETS ACT § 3(a), 14 U.L.A. 633-34 (providing that “[d]amages can include both the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss,” and that “[i]n lieu of damages measured by any other methods, the damages caused by misappropriation may be measured by imposition of liability for a reasonable royalty for a misappropriator's unauthorized disclosure or use of a trade secret”); *see, e.g.*, EFCO Corp. v. Symons Corp., 219 F.3d 734, 741-42 (8th Cir. 2000) (awarding damages to a manufacturer based on evidence of general revenue erosion coinciding with competitor's increased revenues, evidence of sales lost to competitor, and evidence of losses in revenues from a particular product that coincided with the introduction of competitor's rival product, which was developed using the manufacturer's trade secrets).

34. UNIF. TRADE SECRETS ACT § 3(b), 14 U.L.A. 634 (“If willful and malicious misappropriation exists, the court may award exemplary damages in an amount not exceeding twice any award made under subsection (a) [governing compensatory damages]”); *see, e.g.*, Boeing Co. v. Sierracin Corp., 738 P.2d 665, 680-81 (Wash. 1987) (awarding punitive damages to designer where aircraft window supplier engaged in massive efforts to disguise its copying of designer's drawings with knowledge its conduct was illegal).

35. *See, e.g.*, Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 1368 (E.D. Va. 1995) (“Once a trade secret is posted on the Internet, it is effectively part of the public domain Although the person who originally posted a trade secret on the Internet may be liable for trade secret misappropriation, the party who merely down loads [sic] Internet information cannot be liable for misappropriation because there is no misconduct involved in interacting with the Internet.”); Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., 923 F. Supp. 1231, 1256 (N.D. Cal. 1995) (“Although a work posted to an Internet newsgroup remains accessible to the public for only a limited amount of time, once that trade secret has been released into the public domain there is no retrieving it.”); DVD Copy Control Ass'n, Inc. v. Bunner, 75 P.3d 1, 27 (Cal. 2004) (Moreno, J., concurring) (“Courts that have considered the matter have agreed that, generally speaking, a party not involved in the initial misappropriation of a trade secret cannot be prosecuted under trade secret law for downloading and republishing proprietary information posted on the Internet, primarily because the information is in the public domain and is no longer secret.”). Other cases in which courts have denied trade secret status have involved materials posted on the Internet as well as available from other sources. *See, e.g.*, Inflight Newspapers, Inc. v. Magazines In-Flight, LLC, 990 F. Supp. 119, 129 (E.D.N.Y. 1997) (holding that customer lists were not trade secrets because they could be determined through the use of trade directories, telephone books, the Internet, trade shows, and magazines); State *ex rel.* Lucas

D. Trade Secret Law Compared to Patent Law

This brings us then to some key ways in which trade secret law differs from patent law. In contrast to the broad sweep of the UTSA, the Patent Act limits its protections to inventions that meet very specific requirements.³⁶ To be eligible for patent protection, an invention must fall within the designated subject matter of the Patent Act³⁷ and the invention must be novel,³⁸ adequately disclosed,³⁹ non-obvious,⁴⁰ and useful.⁴¹ In addition, a patent only exists and can only be asserted when the United States Patent and Trademark Office (USPTO) issues it, following review and approval of the application.⁴² There is, by contrast, no government office that prospectively reviews whether information can be designated a trade secret; therefore, only if there is litigation is the validity of a claim to trade secret status tested.⁴³ Finally, patents have a limited duration—generally twenty years—while a trade secret can last indefinitely, assuming it is not disclosed beyond those authorized to know it and duty-bound to keep it.⁴⁴

Patent law requires novelty and grants exclusive nationwide rights to the patent holder.⁴⁵ A patent confers a right to exclude others from making, using, selling, offering for sale, and importing the patented invention.⁴⁶ By contrast, trade secret law does not require that the secret information be novel, only that it confers economic value. Nor does trade secret law grant an exclusive right to own or use the information. Assuming there is no misappropriation, multiple parties can own and make use of the same trade secret, even in a single state. This point takes on particular importance with respect to independent discovery and reverse engineering. Under trade secret law, someone who independently discovers a trade secret owns the trade secret and is free to use it. If, for example, the authors of this article happen upon an appealing combination of ingredients that gives us the recipe for a black

County Bd. of Comm'rs v. Ohio EPA, 724 N.E.2d 411, 418–19 (Ohio 2000) (citing the general rule that “where the identity of the customers is readily ascertainable through ordinary business channels or through classified business or trade directories, the courts refuse to accord to the list the protection of a trade secret”).

36. See 35 U.S.C. §§ 101 to 103, 112 (2000).

37. See *id.* § 101 (authorizing the issuance of patents for “any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof”).

38. *Id.* § 102.

39. *Id.* § 112.

40. *Id.* § 103.

41. *Id.* § 101.

42. *Id.* § 111.

43. The validity of a patent issued by the USPTO can also be tested in litigation.

44. 35 U.S.C. § 154(a)(2) (providing that a patent lasts “for a term beginning on the date on which the patent issues and ending 20 years from the date on which the application for the patent was filed in the United States or, if the application contains a specific reference to an earlier filed application or applications . . . from the date on which the earliest such application was filed”). Design patents last for fourteen years. *Id.* § 173.

45. *Id.* § 271(a).

46. *Id.*

cola, we own the recipe and we can use it to make and sell cola—even if the recipe is the very same that produces Coca-Cola. Likewise, a trade secret acquired through reverse engineering can be freely used: we are free to perform a chemical analysis to reverse engineer the Coca-Cola recipe and use the formula thereafter to make our own product.⁴⁷ By contrast, if a patent protects something, independent discovery and reverse engineering have no effect on the patent holder’s monopoly; anyone who wishes to make or use the patented invention needs the patent holder’s permission.⁴⁸ Indeed, an inventor’s newly acquired patent prevents the owner of even a pre-existing trade secret from using the secret in ways that infringe the patent.⁴⁹

Trade secret law protects secret information.⁵⁰ This too sets trade secret law apart from patent law. The Patent Act requires disclosure of specific information about the invention⁵¹ in order to obtain a patent on it.⁵² Secrecy also makes trade secret law unusual among the species of intellectual property law. While a copyright owner is not required to

47. See *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 476 (1974) (“A trade secret law . . . does not offer protection against discovery by . . . so-called reverse engineering, that is by starting with the known product and working backward to divine the process which aided in its development or manufacture.”); *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 178 (7th Cir. 1991) (discussing reverse engineering as an appropriate means of discovering a trade secret).

48. See *Kewanee Oil*, 416 U.S. at 489–90 (“Trade secret law provides far weaker protection in many respects than the patent law. While trade secret law does not forbid the discovery of the trade secret by fair and honest means, *e.g.*, independent creation or reverse engineering, patent law operates ‘against the world,’ forbidding any use of the invention for whatever purpose for a significant length of time.”). In *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, the Supreme Court stated:

[T]he competitive reality of reverse engineering may act as a spur to the inventor, creating an incentive to develop inventions that meet the rigorous requirements of patentability. The Florida statute substantially reduces this competitive incentive, thus eroding the general rule of free competition upon which the attractiveness of the federal patent bargain depends. The protections of state trade secret law are most effective at the developmental stage, before a product has been marketed and the threat of reverse engineering becomes real. During this period, patentability will often be an uncertain prospect, and to a certain extent, the protection offered by trade secret law may ‘dovetail’ with the incentives created by the federal patent monopoly.

489 U.S. 141, 160–61 (1989) (citation omitted) (holding that federal patent law preempted a Florida statute prohibiting duplication of boat hulls by using an original hull to create a mold).

49. See *W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1549–50 (Fed. Cir. 1983).

50. *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1002 (1984) (“Information that is public knowledge or that is generally known in an industry cannot be a trade secret.”).

51. 35 U.S.C. § 112 (2000) (setting out the disclosure requirements); see *infra* notes 92–96 and accompanying text (discussing these requirements).

52. See, *e.g.*, *J.E.M. Ag Supply, Inc. v. Pioneer Hi-Bred Int’l, Inc.*, 534 U.S. 124, 142 (2001) (“The disclosure required by the Patent Act is ‘the *quid pro quo* of the right to exclude.’”). Note that there is a difference between a patent application and the publication of the patent. In applying for a patent, the patent owner is required to disclose to the USPTO trade secrets that are part of the claimed patent. Patent applications are published eighteen months after the filing date. 35 U.S.C. § 122. Publication destroys any trade secret in the information expressed in the patent, leaving intact trade secrets in related information that are not part of the patent. The publication requirement does not apply if the applicant submits a statement that the application will not be filed in a foreign country that provides for eighteen-month publication. *Id.* In addition, the following are exempt from the publication rule: provisional applications; applications for reissue; design applications; and applications that implicate certain national security issues. *Id.* About ten percent of patent applications are not published. NATIONAL RESEARCH COUNCIL, A PATENT SYSTEM FOR THE TWENTY-FIRST CENTURY 4 (Stephen A. Merrill et al. eds., 2004), available at http://books.nap.edu/openbook.php?record_id=10976&page=1.

disclose a work in order to benefit from the protections of copyright law, disclosure does not alter those protections. Similarly, the owner of a trademark is not required to keep a trademark secret. Indeed, the largest financial gains made from inventions and creative works protected by these federal intellectual property doctrines derive from maximizing and capitalizing on controlled disclosure and dissemination.

E. The Relational Aspect of Trade Secrets

Although general disclosure destroys the status of a trade secret, owners of trade secrets often do disclose the secret to key people in order to manufacture their goods, run their businesses, and otherwise derive value from the information. Accordingly, as the provisions of the UTSA governing misappropriation reflect, many trade secret claims arise from a contractual or other privileged relationship in which the trade secret owner has disclosed the secret to a party who has a duty to keep the information confidential. Such relationships include: a nondisclosure or confidentiality agreement in which a party agrees to keep information secret;⁵³ a relationship in which there are fiduciary duties or duties of loyalty, such as those between a supplier and customer,⁵⁴ a licensor and licensee,⁵⁵ an employer and employee;⁵⁶ or some other confidential relationship in which parties disclose sensitive and valuable information.⁵⁷ Patent, trademark, and copyright claims can arise against parties who are in a contractual or other relationship with the patent, trademark, or copyright owner. However, in these other fields of intellectual property law, the presence of such a relationship is of no special

53. See, e.g., *Tax Track Sys. Corp. v. New Investor World, Inc.*, 478 F.3d 783, 787 (7th Cir. 2007) (noting that courts will enforce contracts when the information is confidential and subject to reasonable security measures). Note, however, that contracts alone cannot be used to turn information into a trade secret; the information must meet the trade secret standards. See RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 41 cmt. d.

54. See, e.g., *Tubular Threading, Inc. v. Scandaliato*, 443 So. 2d 712, 715 (La. Ct. App. 1983) (involving a customer who asked supplier to design a pipe-handling system and then sought to use the supplier's design to build a similar system to sell to another company).

55. See, e.g., *Roton Barrier, Inc. v. The Stanley Works*, 79 F.3d 1112, 1118-19 (Fed. Cir. 1996) (affirming finding of trade secret misappropriation and award against prospective licensee); *Bell Helicopter Textron, Inc. v. Tridair Helicopters, Inc.*, 982 F. Supp. 318, 319-20 (D. Del. 1997) (involving misappropriation claim against licensee by manufacturer of kits for converting single engine helicopters into twin-engine helicopters).

56. See, e.g., *Davis v. Eagle Prods., Inc.*, 501 N.E.2d 1099, 1102-03 (Ind. Ct. App. 1986) (involving trade secret misappropriation by former employees who misappropriated employer's pet food formula and started their own company).

57. See *Nadel v. Play-By-Play Toys & Novelties, Inc.*, 208 F.3d 368, 371-72 (2d Cir. 2000) (involving inventor's claim that manufacturer used his idea for a vibrating and spinning plush toy, expressed in a monkey prototype, to develop a similar Tasmanian Devil toy called "Tornado Taz" without compensating the inventor); *Lamb-Weston, Inc. v. McCain Foods, Ltd.*, 941 F.2d 970, 972 (9th Cir. 1991) (allowing trade secret claim against independent contractor); *Heyman v. AR. Winarick, Inc.*, 325 F.2d 584, 587 (2d Cir. 1963) ("As the prospective buyer is given the information for the limited purpose of aiding him in deciding whether to buy [a business], he is bound to receive the information for use within the ambit of this limitation. He may not in good conscience accept the information; terminate negotiations for the sale; and then, using vital data secured from the would-be seller, set out on a venture of his own.").

significance; many parties bring patent, trademark, and copyright claims against opposing parties with no prior relationship at all to the holder of the relevant intellectual property rights. In essence, it is fair to say that trade secrets mostly provide protection against wrongdoing by people whom the owner of the trade secret knew and trusted. Patent, copyright, and trademark provide the opposite—protection from strangers.

III. TRADE SECRETS IN THE DIGITAL AGE

With these aspects of trade secret law laid out, the discussion turns now to the role of trade secrets today. This section examines the difficulties of protecting trade secrets in the digital age.

A. Vulnerabilities

Trade secrets face substantial difficulties in the digital age. For one, digital technology makes the preservation of many kinds of trade secrets increasingly precarious.⁵⁸ Technology's biggest achievements are also its largest threats to trade secret law.⁵⁹ In particular, digital technology allows people to access and steal trade secrets kept in digital form. This is true because devices commonly carried today by ordinary people—cell phones, iPods, laptops, Universal Serial Bus (USB) drives,⁶⁰ Personal Digital Assistants (PDAs),⁶¹ and so forth—provide the means to copy, store, and transport massive quantities of information a company relies on being kept secret. Thieves may also send files containing trade secrets from within the company via e-mail or upload them to portable devices or external websites.⁶² Moreover, a trade secret thief need not even be on site. Digital files can be hacked by outsiders half a world away from the company's headquarters. Beyond the risk of theft, digital technology also increases the opportunities for trade

58. See ASIS INT'L, TRENDS IN PROPRIETARY INFORMATION LOSS: SURVEY REPORT 34 (Aug. 2007), <http://www.asisonline.org/newsroom/surveys/spi2.pdf> (reporting on a study of corporations' costliest trade secret losses, finding that in most cases the information was accessed electronically).

59. See *Religious Tech. Ctr. v. Netcom On-Line Comm'n Servs.*, 923 F. Supp. 1231, 1256 (N.D. Cal. 1995) (“[O]ne of the Internet’s virtues, that it gives even the poorest individuals the power to publish to millions of readers . . . can also be a detriment to the value of intellectual property rights. The anonymous (or judgment proof) defendant can permanently destroy valuable trade secrets, leaving no one to hold liable for the misappropriation.” (internal citations omitted)).

60. A USB drive is a flash memory card, small enough to put on a keychain, that plugs into a computer’s USB port and operates like a disk drive, allowing for the copying of data.

61. A PDA is a handheld computer for managing contacts and appointments; wireless versions offer e-mail, Internet connections, and cellular phone service.

62. See *United States v. Martin*, 228 F.3d 1, 19 (1st Cir. 2000) (involving trade secrets e-mailed outside the company); *United States v. Genovese*, 409 F. Supp. 2d 253, 254 (S.D.N.Y. 2005) (involving Microsoft source code posted on the Internet); *Four Seasons Hotels & Resorts B.V. v. Consorcio Barr. S.A.*, 267 F. Supp. 2d 1268, 1280 (S.D. Fla. 2003) (involving penetration of intranet and transfer of files), *aff’d in part, rev’d in part*, 138 Fed. Appx. 297 (11th Cir. 2005); *Ford Motor Co. v. Lane*, 67 F. Supp. 2d 745, 747 (E.D. Mich. 1999) (involving Ford secrets posted on the Internet); *Liebert Corp. v. Mazur*, 827 N.E.2d 909, 918 (Ill. App. Ct. 2005) (involving employee who burned zip files to a compact disc).

secrets to be lost through carelessness. Employees might mistakenly attach sensitive files to e-mails, misplace flash drives, store information on unsecure laptops, access e-mail on vulnerable networks, forget to log-off a hotel computer, and so on. Numerous incidents in recent years have illustrated the vulnerability of information kept in digital form.⁶³

B. Remedies

Trade secret law provides the owner of a trade secret with remedies against those who misappropriate the secret. However, just as digital technology makes trade secrets vulnerable to access, when combined with the unique features of trade secret law discussed above, digital technology also undermines the possibility of successfully obtaining remedies for disclosure. Information in digital form can reach millions of people via the Internet in a matter of seconds. A disclosed trade secret is therefore able to flow to users who are not liable for accessing or using the information because they owed no duty of confidentiality, and they did not knowingly receive improperly acquired information, as required for liability under the UTSA.

With the aid of technology, the owner of the trade secret might be able to identify who was responsible for the initial disclosure. In terms of a remedy, however, this might not do the trade secret owner much good. Along with disclosures by former employees seeking to profit from knowledge they obtained on the job, most trade secret violations stem from current employees accidentally disclosing information they

63. See Press Release, ASIS International, U.S. Companies Lost up to \$59 Billion in Proprietary Information and Intellectual Property (Sept. 30, 2002), available at <http://www.asisonline.org/newsroom/pressReleases/093002trends.xml> (reporting that in a one-year period United States businesses lost \$59 billion in intellectual property theft and that forty percent of respondents reported incidents involving trade secret theft, including research and development data, customer lists, financial data, strategic plans, merger/acquisition data, product specifications, and manufacturing data); Karen W. Arenson, *Princeton Pries into Website for Yale Applicants*, N.Y. TIMES, July 26, 2002, available at <http://query.nytimes.com/gst/fullpage.html?res=9C0CE2DA1E38F935A15754C0A9649C8B63&sec=&spon=&pagewanted=1> (“[Princeton’s admissions director] acknowledged that he had entered the Yale [web]site by using the birth dates and Social Security numbers of Princeton applicants who had also applied to Yale.”); Gay Bryant et al., *Who’s Stealing Your Business?*, FORTUNE SMALL BUS., May 2008, at 68, 68 (reporting on hackers who broke into a supermarket chain’s database and stole customers’ credit card information); Thomas Frank, *TSA Seeks Hard Drive, Personal Data for 100,000*, USA TODAY, May 5, 2007, available at http://www.usatoday.com/tech/news/computersecurity/2007-05-04-harddrive-tsa_n.htm?loc=interstitialskip (reporting potential accidental disclosure of employees’ personal and financial records stored electronically by Transportation Security Administration); Brian Krebs, *Data Breaches Have Surpassed Level for All of ‘07, Report Finds*, WASH. POST, Aug. 26, 2008, at D01 (reporting that as of the date of the article, 449 U.S. businesses, government agencies, and universities had reported a loss or theft of consumer data in 2008); Brian Krebs, *Justice Breyer Is Among Victims in Data Breach Caused by File Sharing*, WASH. POST, July 9, 2008, at A1 (reporting that investment firm’s records of 2,000 clients, including Supreme Court Justice Stephen Breyer, were exposed on the Internet after an employee of the firm used an online file-sharing network at his office); Brad Stone, *11 Charged in Theft of 41 Million Card Numbers*, N.Y. TIMES, Aug. 6, 2008, available at http://www.nytimes.com/2008/08/06/business/06theft.html?_r=1&scp=1&sq=11%20Charged%20in%20Theft%20of%2041%20Million%20Card%20Numbers&st=cse&oref=slogin (reporting on use of “sniffer programs” to tap into retailers’ networks for processing credit cards to intercept customers’ stored PINs and debit and credit numbers).

possess by virtue of their employment.⁶⁴ Accidental disclosure does not constitute misappropriation under the UTSA and even if it did, there would be little point in trying to collect damages from an employee. Further, careless disclosures by employees may provide evidence that the owner did not take adequate security precautions to safeguard his or her secret, thereby precluding it from the protection of trade secret law.

In addition, state trade secret law is likely of limited value in responding to disclosures that occur outside a contractual or other confidential relationship.⁶⁵ Espionage, hacking, and other external threats are increasingly likely in the digital age, and their harm can be great. Current employees normally cooperate with efforts to minimize accidental leaks out of either loyalty or fear; in many cases, an employer can trace a leak by an employee back to the employee. An outside hacker presents quite a different problem. A hacker could be outside the United States and beyond the purview of American courts. Indeed, some such threats come from foreign governments that seek to benefit from American technology.⁶⁶

C. Disclosure on the Internet

Owners of trade secrets encounter an additional problem in the digital age. Once disclosed on the Internet, a trade secret normally loses its status as a trade secret, and nothing will make the information secret again.⁶⁷ Although the resulting loss of trade secret status will not be a

64. See ASIS INT'L, *supra* note 58, at 28, tbl.12 (reporting on a survey of corporations that suffered threats to their trade secrets, twenty-three respondents reported a threat from an employee inadvertently e-mailing information, nineteen respondents reported deliberate disclosure by an employee, and thirteen reported unauthorized access by outsiders to information systems). See, e.g., *Navigant Consulting, Inc. v. Wilkinson*, 508 F.3d 277, 280 (5th Cir. 2007) (involving a former employee seeking to profit by divulging employer's trade secrets); *Conseco Fin. Servicing Corp. v. N. Am. Mortgage Co.*, 381 F.3d 811, 815 (8th Cir. 2004) (involving solicitation of a competitor's former employees who possessed customer lists); *Rohm & Haas Co. v. Adco Chem. Co.*, 689 F.2d 424, 430 (3d Cir. 1982) (involving the recruiting of competitors' employees with knowledge of trade secrets); *Bus. Designs v. Midnational Graphics*, No. 2-085/01-1087, 2002 Iowa App. LEXIS 524, at *2 (Iowa Ct. App. May 15, 2002) (involving competing business using former employer's design documents).

65. Two federal statutes respond to the threats digital technology makes to trade secret protection. The Economic Espionage Act of 1996 criminalizes the theft of certain kinds of trade secrets, although it does not provide for a private cause of action. 18 U.S.C. § 1831 (2006). The Computer Fraud and Abuse Act, passed in 1986 and amended in 2001 as part of the PATRIOT Act, criminalizes certain forms of computer hacking. *Id.* § 1030.

66. See FEDERAL BUREAU OF INVESTIGATION, STRATEGIC PLAN 2004-2009 § 1 (2004), *available at* <http://www.fbi.gov/publications/strategicplan/stategicplantext.htm> ("The cyber threat to our national security stems from two groups: (1) non-state actors such as terrorist groups and hackers; and (2) foreign governments that have developed cyber espionage or information warfare programs to target U.S. networks. The number of foreign governments and non-state actors exploiting computer networks and developing their cyber capabilities is on the rise."). A survey of United States corporations reports that in efforts to gain unauthorized access to their trade secrets, foreign individuals, entities, or governments were more than twice as likely as domestic actors to be the intended beneficiaries. See ASIS INT'L, *supra* note 58, at 23.

67. See, e.g., *DVD Copy Control Ass'n, Inc. v. Bunner*, 10 Cal. Rptr. 3d 185, 192-93 (Cal. Ct. App. 2004) (explaining that injunctive relief may be appropriate where a posting 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 eco-

defense available to a party sued for an initial misappropriation, anyone else will be able to use the information legally in the future. Some courts have taken the position that, even when posted on a website, a trade secret can maintain trade secret status if the owner of the secret took remedial action before the general public had an opportunity to access the information.⁶⁸ Yet remedial action, in particular if the trade secret owner seeks injunctive relief, can itself be the thing that drives additional disclosure and destroys the secret. For example, when a trade group sent cease-and-desist letters demanding that websites remove the code for overwriting copyright protection on Blu-ray and high-definition DVDs, the letters unintentionally prompted Internet users to disseminate the code widely.⁶⁹

D. A Comparison to Copyright

A comparison to copyright sharpens the point. Digital technology, as courts and commentators have observed, facilitates infringement of copyrights.⁷⁰ In the same way that digital technology allows for the mass distribution of trade secrets without the owner's permission, it also allows for the mass distribution of copyrighted works without the consent of the copyright owner. Yet dissemination does not alter the status of a copyrighted work; however widely distributed, the owner still possesses a copyrighted work. The copyright owner can seek damages against the first individual making the illegal copy as well as against the millionth individual who obtains it illegally. In contrast to trade secret law, copyright law requires no pre-existing contractual or fiduciary duty in order for there to be infringement, and liability exists regardless of the intent or knowledge of the infringer. Further distinguishing copyright from trade secret law, the more widespread the distribution of a copyrighted work, the greater the number of potential defendants, and the higher the potential cumulative damages available to the copyright owner.⁷¹ Consider in this respect the well-known example of unauthorized

conomic value").

68. See, e.g., *Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc.*, 923 F. Supp. 1231, 1255–56 (N.D. Cal. 1995) (holding that secrecy was destroyed when information was posted to a newsgroup likely visited by interested individuals). One state has passed a law that preserves the secrecy of information posted on the Internet if the trade secret owner acts quickly to enjoin the posting. See NEV. REV. STAT. § 600A.055 (Supp. 2008).

69. Brad Stone, *In Web Uproar, Antipiracy Code Spreads Wildly*, N.Y. TIMES, May 3, 2007, at A6.

70. See generally *MGM Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005) (noting that the volume of file-sharing enabled by peer-to-peer networks inevitably enhances opportunity for infringement); Symposium, *Interdisciplinary Conference on the Impact of Technological Change on the Creation, Dissemination, and Protection of Intellectual Property*, 70 ALB. L. REV. 1151 (2007).

71. See 17 U.S.C. § 504(b)–(c) (2006) (providing for recovery of actual damages and profits or, at the election of the copyright owner, statutory damages up to \$30,000 per infringement or \$150,000 per infringement in the case of willful infringement).

downloading and sharing of copyrighted music files.⁷² By contributing to declining sales, these activities have had a serious impact on the recording industry, yet never altered the copyright status of the compositions or recordings—a point driven home to the thousands of individuals sued by the Recording Industry Association of America (RIAA), in some cases for very substantial damages.⁷³ Trade secret law provides no comparable remedy against digital distribution.

Moreover, the digital environment creates new opportunities for owners of creative works to protect their interests, which are unavailable to owners of trade secrets. Thus, in addition to enforcing its copyrights, the recording industry has responded to unauthorized copying with technology-based “self-help” measures.⁷⁴ In particular, record labels have responded to piracy by encrypting CDs and commercial digital music with digital rights management (DRM) technology,⁷⁵ backed up by a federal anti-circumvention law.⁷⁶ These kinds of strategies are also not available to the trade secret owner. Although trade secret owners may utilize encryption technology, they do so to control access, not distribution, which is the very thing that undermines the value of their information. Additionally, while technology that tracks disclosure is useful to copyright owners because it allows them to identify infringers, such technology is of less value to trade secret owners, who depend heavily on prevention.

IV. THE COSTS OF SECRECY

The digital age does not render all trade secrets vulnerable to the point of ineffectiveness. Some owners do not keep trade secrets in digital form, therefore those secrets are not vulnerable to the distribution capability of digital technology. Some owners of trade secrets will respond successfully to the threats that digital technology poses by in-

72. Not surprisingly, the recording industry was the first to feel the sting of piracy because the relatively small size of compressed digital song files allowed for easy dissemination of music even in the days of dial-up Internet connections. The early attacks on the music business provided a warning to movie studios and other creative industries, which used the lead time to develop an encryption system before the commercial release of any digital copies of films. A digital rights management (DRM) system known as Content Scramble System (CSS), developed for the first commercial releases of DVDs, remains the industry standard despite the fact that hackers broke the encryption and distributed the decrypting code, known as DeCSS. See TARLETON GILLESPIE, WIRED SHUT: COPYRIGHT AND THE SHAPE OF DIGITAL CULTURE 169-78 (2007) (tracing the development of CSS).

73. See Marc Fisher, *Download Uproar: Record Industry Goes After Personal Use*, WASH. POST, Dec. 30, 2007, at M05 (reporting that the RIAA has filed 20,000 lawsuits for sharing copyrighted music; while most cases have settled, in October 2007, in the first case a jury decided, the RIAA won a judgment of \$220,000 against a defendant who shared twenty-four songs online).

74. See WILLIAM W. FISHER III, PROMISES TO KEEP: TECHNOLOGY, LAW AND THE FUTURE OF ENTERTAINMENT 51-54 (2004).

75. DRM technology limits the ways consumers can use audio files. Limitations include how many copies may be made, whether or not a file will play on more than one computer or portable device, and even on which devices it will and will not play.

76. See the Digital Millennium Copyright Act of 1998 (DMCA), which, inter alia, made the circumvention of digital copyright management systems illegal. 17 U.S.C. § 1201(a).

creasing their security efforts. This section turns to a normative assessment of the call for a greater use of trade secrets. Drawing on recent experiences in the realm of copyright law, it shows how an increased reliance on trade secret law would pose a risk to the public domain.

A. *Contract and Copyright*

The call for increased use of trade secrets to fill gaps in patent law protection shares a familial relationship with a striking development in our system of copyright in recent years. Owners of creative works, dissatisfied with the protection that copyright law provides them, have increasingly turned to state contract law to enhance and augment their rights. A vendor conditions access to a database upon an agreement not to copy or distribute the materials without the vendor's permission, even though copyright law might allow copying and distribution.⁷⁷ Archives restrict access to their collections to people who agree to forego copying that the Copyright Act would otherwise permit.⁷⁸ Websites impose terms of use involving assertions of rights beyond those permitted by copyright law.⁷⁹ Online music sites sell downloads under restrictive terms.⁸⁰ Software publishers license rather than sell their works, with

77. See, e.g., *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1449 (7th Cir. 1996) (involving a "shrinkwrap" license agreement prohibiting a user of a CD-ROM containing public domain business telephone listings from copying the CD); *Forest2Market, Inc. v. Am. Forest Mgmt.*, No. 3:05cv423, 2008 U.S. Dist. LEXIS 33185, at *3-*4 (W.D.N.C. Apr. 21, 2008) (involving a database of information about timber prices and availability, provided for a fee and contingent upon the user's agreement not to redistribute); *Telerate Sys., Inc. v. Caro*, 689 F. Supp. 221, 223 (S.D.N.Y. 1988) (involving database owner's reliance on contract law to prevent the redistribution of its collected financial market price listings).

78. See, e.g., Columbia Univ. Libraries, *The Papers of John Jay: Copyright and Use*, <http://www.columbia.edu/cu/lweb/digital/jay/copyright.html> (last visited Oct. 17, 2008) ("[M]uch of the material may be in the public domain," but "[t]he University does not authorize any use or reproduction whatsoever for commercial purposes.>").

79. For example, the terms and conditions accompanying U.S. News & World Report's ranking of colleges provides:

The materials contained on the Web site are provided by *U.S. News* as a service to you for your noncommercial, personal use on an "as is, as available" basis and may be used by you for information purposes only. . . . All materials published on the Web site are protected by copyright laws, and may not be reproduced, republished, distributed, transmitted, resold, displayed, broadcast, or otherwise exploited in any manner without the express written permission of [] *U.S. News*.

U.S. News & World Report, *Terms & Conditions of Use and Privacy Policy*, <http://www.usnews.com/usnews/usinfo/terms.htm> (last visited Oct. 17, 2008). The New York Public Library's (NYPL) website states the following conditions of use:

NYPL Digital Gallery contains hundreds of thousands of digital images of historical materials from the Research Libraries' and Branch Libraries' original, rare, and specialized holdings. Images may be freely downloaded for personal, research, and study purposes only. As the physical rights holder of this material, most of which is in the public domain for copyright purposes, the Library charges a usage fee to license an image for commercial use (defined above). The usage fee is not a copyright fee. You are free to obtain a copy of these images from a source other than NYPL. Usage fees help ensure that the Library is able to continue to acquire, preserve and provide access to its collections.

NYPL Digital Gallery, *User's Guide*, http://digitalgallery.nypl.org/nypldigital/dghelp_using.cfm#conditions (last visited Oct. 16, 2008).

80. See, e.g., Amazon.com, *Amazon MP3 Music Service: Terms of Use*, <http://www.amazon.com/gp/help/customer/display.html?nodeId=200154280> (last visited October 30, 2008) (speci-

licensing terms that exceed the rights the publisher would be entitled to under copyright law.⁸¹ Although paper books can be loaned and re-sold, e-books come with licensing terms that prohibit such actions.⁸² State contract law, rather than federal copyright law, increasingly determines the scope of rights held by owners of creative works and sets the limits on uses of those works. By giving content owners protections beyond those that copyright law permits, these practices upset the balance between copyrighted works and the public domain.⁸³ Yet, so far, courts have tended to uphold contracts that enhance the interests of content owners.⁸⁴

fyng that “you agree that you will not redistribute, transmit, assign, sell, broadcast, rent, share, lend, modify, adapt, edit, sub-license or otherwise transfer or use the Digital Content.”).

81. See John A. Rothchild, *The Incredible Shrinking First-Sale Rule: Are Software Resale Limits Lawful?*, 57 RUTGERS L. REV. 1, 22–50 (2004) (describing how software publishers circumvent the first-sale doctrine with contractual terms that: declare those who acquire copies of the software “licensees” and therefore are not “owners”; limit distributors’ authority to transfer title of software copies; and, in the form of clickwrap licenses, create restrictions that travel with the software copies).

82. See Randall Stross, *First It Was Song Downloads. Now It’s Organic Chemistry*, N.Y. TIMES, July 27, 2008, available at <http://www.nytimes.com/2008/07/27/technology/27digi.html?scp=1&sq=first%20it%20was%20song%20downloads.&st=cse> (describing publishers’ increased use of digital versions of textbooks that are rented rather than sold to students); Amazon.com, *Amazon Kindle: License Agreement and Terms of Use*, www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=200144530 (last visited Oct. 17, 2008) (“Restrictions. You may not sell, rent, lease, distribute, broadcast, sublicense or otherwise assign any rights to the Digital Content or any portion of it to any third party.”).

83. See Jason Mazzone, *Copyfraud*, 81 N.Y.U. L. REV. 1026, 1056–57 n.142 (2006) (discussing uses of contracts to restrict use of public domain works); Kathleen K. Olson, *Preserving the Copyright Balance: Statutory and Constitutional Preemption of Contract-Based Claims*, 11 COMM. L. & POL’Y 83, 84 (2006) (“Because of the difficulty in enforcing copyright in a digital age, some copyright owners have abandoned the current system in favor of private rights management and contract law, protecting their intellectual property through licensing agreements that, in some cases, take away the rights given by copyright law regarding fair use and other public interest safeguards.”); J.H. Reichman & Jonathan A. Franklin, *Privately Legislated Intellectual Property Rights: Reconciling Freedom of Contract with Public Good Uses of Information*, 147 U. PA. L. REV. 875, 878 (1999) (“In the networked environment . . . routine validation of mass-market access contracts and of non-negotiable constraints on users would tend to convert standard form licenses of digitized information goods into functional equivalents of privately legislated intellectual property rights. Firms possessing any degree of market power could thereby control access to, and use of, digitized information by means of adhesion contracts that alter or ignore the balance between incentives to create and free competition that the Framers recognized in the Constitution and that Congress has progressively codified in statutory intellectual property laws.”); Hannibal Travis, Comment, *Pirates of the Information Infrastructure: Blackstonian Copyright and the First Amendment*, 15 BERKELEY TECH. L.J. 777, 828 (2000) (describing as a form of “copyright grab,” “the transformation . . . of sales of copyrighted works, currently governed by the public law of copyright and governed by courts, into licenses for the use of those works, strictly limited in duration and scope by standard form contract language and seamlessly implemented by mechanisms of technological self-help.”).

84. Language from two 1964 United States Supreme Court cases suggests that state laws conferring rights beyond those the Copyright Act provides are preempted. See *Compco Corp. v. Day-Brite Lighting, Inc.*, 376 U.S. 234, 237 (1964) (“[W]hen an article is unprotected by a patent or a copyright, state law may not forbid others to copy that article. To forbid copying would interfere with the federal policy, found in . . . the Constitution and in the implementing federal statutes, of allowing free access to copy whatever the federal patent and copyright laws leave in the public domain.”); *Sears, Roebuck & Co. v. Stiffel Co.*, 376 U.S. 225, 232–33 (1964) (invalidating state unfair competition law preventing copying of unpatented work, stating that “a State may not, when the article is unpatented and uncopyrighted, prohibit the copying of the article itself or award damages for such copying”). However, more recent courts have upheld such contracts. See, e.g., *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1449 (7th Cir. 1996) (holding that “shrinkwrap” license agreement prohibiting user of CD-ROM containing public domain business telephone listings from copying CD was enforceable against user); *Howard v. Sterchi*, 974 F.2d 1272, 1277 (11th Cir. 1992) (“Although enforcement of this con-

Developments in the recording industry are especially notable. With encryption and DRM leading to consumer backlash,⁸⁵ the recording industry has turned to a novel means of distribution—that of streaming music to subscribers bound by licensing agreements.⁸⁶ Whereas consumers previously purchased physical records and CDs, consumers accessing streamed music receive no physical or digital file. Essentially, streaming is on-demand radio. The consumer owns nothing other than the right to stream the music; there is nothing for an infringer to copy and transfer to someone else. These arrangements allow record labels largely to prevent infringement of their copyrights, as well as to claim rights and remedies beyond those that are available under copyright law if set out in the agreement with the subscriber. For example, streamed music comes with terms of use conditions that prohibit reproductions by the subscriber, including reproductions that would be permissible fair use under the Copyright Act.⁸⁷

tractual limitation would make [the defendant] subject to limitations with respect to . . . materials that are in the public domain, this contractual restriction is clearly stated in the contract and plaintiffs would not receive the benefit of their bargain if the restriction is not enforced.”). *But see* Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 270 (5th Cir. 1988) (holding that state law licensing provision prohibiting adaptation of licensed computer program by decompilation or disassembly was preempted by the Copyright Act and was therefore unenforceable). Commentators have expressed a range of views as to whether parties should be permitted to use contracts to impose restrictions unavailable under copyright law. *See* Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239, 1264 (1995) (arguing that the Uniform Commercial Code should not allow for enforcement of “unbargained shrinkwrap license provisions that reduce or eliminate the rights granted to licensees by the federal intellectual property laws”); Michael J. Madison, *Legal-Ware: Contract and Copyright in the Digital Age*, 67 FORDHAM L. REV. 1025, 1134, 1139 (1998) (writing that “information law [should] be a . . . federal preserve,” and suggesting that Congress assign to federal courts power to make federal common law governing copyright and contract); David Nimmer et al., *The Metamorphosis of Contract into Expand*, 87 CAL. L. REV. 17, 76 (1999) (“[A]ttempts to rework, alter, or eviscerate aspects of copyright through the vehicle of state contract law are illegitimate.”); Maureen A. O’Rourke, *Drawing the Boundary Between Copyright and Contract: Copyright Preemption of Software License Terms*, 45 DUKE L.J. 479, 482 (1995) (“[T]here are many circumstances in which the law should not preempt parties’ agreements to surrender decompilation rights, despite the fact that such agreements contract around the [Copyright] Act’s background rules.”).

85. *See* Jefferson Graham, *Firestorm Rages Over Lockdown on Digital Music*, USA TODAY, Nov. 14, 2005, at 1B (reporting on reactions to Sony BMG’s use of copy protection on twenty CD titles). With DRM technology protected under the DMCA, works that are only available with DRM protection cannot be used to make a fair use of the existing work. *See* Fred von Lohmann, *Fair Use and Digital Rights Management: Preliminary Thoughts on the (Irreconcilable?) Tension Between Them*, http://w2.eff.org/IP/DRM/fair_use_and_drm.html (last visited Oct. 17, 2008) (“While it may be too early to draw final conclusions, it is plain that DRM technologies, backed by laws like the DMCA, pose a serious potential threat to fair use. While technical refinements may address or minimize some of the social costs that stem from an erosion of fair use, it is unlikely that they will entirely resolve the tension.”).

86. Streaming is a digital delivery process similar to terrestrial radio stations: a signal is broadcast to the listener, but at no time is a tangible or digital copy of the work in the possession of the listener. Streamed content can either be consumer- or provider-driven. Consumer-driven streaming is essentially on-demand access to streaming songs selected by the listener.

87. According to the Terms of Use at Rhapsody, one service that provides streaming audio: The Services available through the Application, and the Application itself (including the Content), are the property of Rhapsody or its licensors and are protected by copyright and other intellectual property laws. The Services provided through the Application may be used for your personal, non-commercial use only. You agree not to (i) reproduce, record, retransmit, redistribute, disseminate, sell, rent, lend, broadcast, publicly perform, adapt, sub-license or circulate the Application or any Content received through the Application or any Service (including music content) to any third party, (ii) exploit any such Content or

B. Trade Secrets, Patent Law, and the Public Domain

Just as state contract law distorts federal copyright law, state trade secret law can distort federal patent law and undermine the public domain. To understand this problem, one needs to consider the effects of aggressive use of trade secret law in the context of the current patent system.

1. Problems in Patent Issuance

Current problems with the patent approval system are legendary.⁸⁸ The USPTO suffers from a shortage of qualified patent examiners, particularly in fields with new technologies, often resulting in a lengthy period between the USPTO's receipt of a patent application and an examiner's decision to grant or deny the patent. These delays compound the application backlogs that have grown significantly in recent years.⁸⁹ The filing process is also often expensive for inventors, thereby favoring well-financed applicants. Fees paid by applicants and annual maintenance fees from patent holders fund the USPTO; this funding system creates an incentive for the USPTO to approve patents liberally, so that applicants file new applications in greater numbers. Studies show that as a result of these factors, the USPTO has been overly generous, granting patents on inventions that should not qualify for protection because,

the Application for commercial purposes without the express prior written consent of Rhapsody, or (iii) to share your password with any third party. You may not make any unauthorized copies of the Application or the Content obtained through the Services, and may only make such copies as are reasonably necessary for your personal, non-commercial use. Because the Services are designed for personal use, you are not allowed to use any automated system for the selection or streaming of files. You further agree to indemnify and hold harmless Rhapsody for your failure to comply with this section. Rhapsody and its licensors retain exclusive ownership of the Application, the Content, the Services, and all intellectual property rights associated therewith. Except as expressly provided herein, you are not granted any rights or license to patents, copyrights, trade secrets or trademarks with respect to the Services, the Application or their contents. Rhapsody and its licensors reserve all rights not expressly granted hereunder. You shall promptly notify Rhapsody in writing upon your discovery of any unauthorized use or infringement of the Services (or their contents) or any patent, copyright, trade secret, trademarks or other intellectual property rights of Rhapsody or its licensors.

Rhapsody, *Rhapsody Service Terms and Conditions*, <http://rhapreg.real.com/rhapsody/freeform?freeformname=RhapC%20Terms> (last visited on Oct. 17, 2008).

88. See generally FED. TRADE COMM'N, TO PROMOTE INNOVATION: THE PROPER BALANCE OF COMPETITION AND PATENT LAW AND POLICY (2003), available at <http://www.ftc.gov/os/2003/10/innovationrpt.pdf>; NATIONAL RESEARCH COUNCIL, *supra* note 52, at 4.

89. See United States Patent and Trademark Fee Modernization Act of 2003: Hearing on H.R. 1561 Before the Subcomm. on Courts, the Internet, and Intellectual Prop. of the H. Comm. on the Judiciary, 108th Cong. 7 (2003) (statement of the Honorable James E. Rogan, Under Sec'y of Commerce for Intellectual Prop. and Dir. of the USPTO), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_house_hearings&docid=f86267.wais (“[W]ithout fundamental changes to the way the USPTO operates, the quality of the patents . . . we issue likely will deteriorate, and the time it takes for an application to be reviewed will skyrocket. . . . [T]hese problems are a greater threat to the health of America's intellectual property system than ever.”); U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-05-720, INTELLECTUAL PROPERTY: USPTO HAS MADE PROGRESS IN HIRING EXAMINERS, BUT CHALLENGES TO RETENTION REMAIN 1 (2005) (“USPTO's resources have not kept pace with the rising number and complexity of patent applications it must review.”).

for example, they are not sufficiently novel.⁹⁰ The social and economic costs of these faulty patents are enormous—patents allow their holders to charge consumers monopoly prices and otherwise to thwart competition and innovation that could benefit society as a whole. Faulty patents are especially problematic in key industries like software and biotechnology.⁹¹ More generally, every time the USPTO issues a faulty patent, unless and until a court finds it invalid, the patent holder monopolizes an invention that as a matter of federal law should be in the public domain.

2. Secrecy and Patent Quality

Increased use of trade secret law will exacerbate the problems the patent system faces. The quality of patents depends greatly on the information made available to patent examiners in making their determinations. The Patent Act establishes disclosure requirements, designed to ensure that members of the public have notice of the scope of the patentee's rights and to disseminate the knowledge that is the basis for the invention.⁹² The first two paragraphs of section 112 of the Patent Act set out the disclosure requirements:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.⁹³

There are four separate requirements: (1) the written description; (2) the enablement; (3) the best mode; and (4) the distinct claim.⁹⁴ Failure to comply with any of them is grounds for denying a patent application and for invalidating an issued patent.⁹⁵ Of these four, the enablement and best mode requirements are particularly relevant to the focus

90. See FED. TRADE COMM'N, *supra* note 88, at 6 (noting that perhaps as many as forty-five to forty-six percent of all patents litigated to final results are held invalid). Patents that others challenge in court, however, are probably not representative of all patents issued.

91. See *id.* at Executive Summary, 6–7 (noting that in industries characterized by incremental innovation in which “firms can require access to dozens, hundreds, or even thousands of patents to produce just one commercial product, . . . [q]uestionable patents . . . frustrate competition”).

92. See *Markman v. Westview Instruments, Inc.*, 517 U.S. 370, 390 (1996) (explaining that “[t]he limits of a patent must be known for the protection of the patentee, the encouragement of the inventive genius of others and the assurance that the subject of the patent will be dedicated ultimately to the public”).

93. 35 U.S.C. § 112 (2000).

94. *Id.*

95. See *Consol. Aluminum Corp. v. Fosco, Inc.*, 910 F.2d 804, 807 (Fed. Cir. 1990); *Union Carbide Corp. v. Borg-Warner*, 550 F.2d 355, 363–64 (6th Cir. 1977).

of this article.⁹⁶

The enablement provision, requiring a description sufficient to allow a person skilled in the art to make and use the invention, represents the bargain between the government and the inventor. In exchange for the right to exclude, which a patent confers, the inventor must disclose to the public how to make and use the invention. Although the applicant need not disclose every method,⁹⁷ case law interpreting this provision requires that the inventor provide a sufficiently detailed disclosure to enable someone skilled in the art to practice the invention without undue experimentation.⁹⁸ The enablement must also be commensurate with the scope of the patentee's claims.⁹⁹

The best mode provision requires the specification to set forth the best mode contemplated by the inventor of carrying out the invention. This requirement prevents an applicant from obtaining a patent while revealing to the public only an embodiment of the invention that does not represent the best embodiment known to the inventor. As the United States Court of Appeals for the Federal Circuit has explained, "The best mode requirement creates a statutory bargained-for-exchange by which a patentee obtains the right to exclude others from practicing the claimed invention for a certain time period, and the public receives knowledge of the preferred embodiments for practicing the claimed invention."¹⁰⁰

Greater reliance upon trade secrets encourages patent applicants to avoid complying with the enablement and best mode requirements.

96. The other two requirements also serve important functions. The United States Court of Appeals for the Federal Circuit has explained that the written description, in addition to giving notice to others of the scope of the invention (apart from what is claimed), ensures that the inventor was in possession of the claimed subject matter at the time of filing. It is therefore separate and distinct from the enablement requirement. *See Vas-Cath, Inc. v. Mahurkar*, 935 F.2d 1555, 1563-64 (Fed. Cir. 1991) ("The purpose of the 'written description' requirement is broader than to merely explain how to 'make and use'; the applicant must convey with reasonable clarity to those skilled in the art that, as of the filing date sought, he or she was in possession of *the invention*." (emphasis in original)). The written description plays a particularly important role when the applicant amends claims after filing; amended claims are limited by the specification. *See id.* at 1560. The claim requirement provides notice of what the patentee is actually claiming. *See Bancorp Servs., L.L.C. v. Hartford Life Ins. Co.*, 359 F.3d 1367, 1371 (Fed. Cir. 2004) (explaining that the claim is sufficiently definite if "those skilled in the art would understand what is claimed when the claim is read in light of the specification").

97. *See Spectra-Physics, Inc. v. Coherent, Inc.*, 827 F.2d 1524 (Fed. Cir. 1987) (holding that failure to disclose other methods by which the claimed invention may be made does not render a claim invalid under 35 U.S.C. § 112); *In re Fisher*, 427 F.2d 833, 839 (C.C.P.A. 1970) (holding that as long as the specification discloses at least one method for making and using the claimed invention that bears a reasonable correlation to the entire scope of the claim, then the enablement requirement is satisfied).

98. *See also United States v. Telectronics, Inc.*, 857 F.2d 778, 785 (Fed. Cir. 1988) ("The test of enablement is whether one reasonably skilled in the art could make or use the invention from the disclosures in the patent coupled with information known in the art without undue experimentation.").

99. *See, e.g., In re Vaecck*, 947 F.2d 488, 496 (Fed. Cir. 1991) ("[T]here must be sufficient disclosure . . . to teach those of ordinary skill how to make and how to use the invention as broadly as it is claimed.").

100. *Eli Lilly & Co. v. Barr Labs., Inc.*, 251 F.3d 955, 963 (Fed. Cir. 2001).

Patent applicants already face temptations to reap the benefits of patent protection while being less than forthcoming in their disclosures in order to maintain a competitive advantage. Corporations that aggressively protect information they deem a trade secret and who “file early [and] file often,”¹⁰¹ will be inclined to file bare-bones or misleading patent applications and to resist requests from examiners to supplement their files.¹⁰² This can only add to the current problems in patent determinations.

The current system does not easily root out failures to meet the enablement and best mode requirements during the examination stage. Federal law provides that “[e]ach individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the [USPTO], which includes a duty to disclose to the [USPTO] all information known to that individual to be material to patentability.”¹⁰³ However, the USPTO takes the position that “[a] court, with subpoena power, is presently the best forum to consider duty of disclosure issues,” and therefore the USPTO “does not investigate and reject original or reissue applications” for failure to comply with this duty.¹⁰⁴

It follows that rejections for failure to comply with the enablement and best mode requirements of section 112 are rare.¹⁰⁵ With respect to the enablement requirement, the patent examiner bears the burden of establishing a reasonable basis for questioning why the enablement requirement has not been satisfied.¹⁰⁶ However, the examiner, who does not actually try to make and use the invention, is not necessarily in a position to know whether there has been sufficient disclosure to enable a person skilled in the relevant art to make and use the invention without undue experimentation.

Nor can the examiner normally tell from the application whether the applicant has disclosed the best mode known to the inventor or

101. Jorda, *supra* note 2, at 19.

102. *Cf. id.* at 20 (describing “rudimentary lab or shop experiments done and samples or prototypes obtained and a mode of carrying out the inventions”); GALE R. PETERSON, TRADE SECRET PROTECTION IN AN INFORMATION AGE § 5.6 (1997) (advising that “the disclosure in the application be limited to that disclosure necessary to ‘support’ the claims . . . and that every effort be taken to maintain the remainder of the system as a trade secret”).

103. 37 C.F.R. § 1.56 (2007).

104. USPTO, MANUAL OF PATENT EXAMINING PROCEDURE § 2010 (8th ed., rev. 2008), *available at* <http://www.uspto.gov/web/offices/pac/mpep/mpep.htm>; *see also* FED. TRADE COMM’N, *supra* note 88, Executive Summary, at 9 (“The PTO’s resources also appear inadequate to allow efficient and accurate screening of questionable patent applications.”).

105. *See generally* FED. TRADE COMM’N, *supra* note 88, ch. 5, at 10 (“Even when examiners develop a *prima facie* case against patentability, they often lack the ability to probe behind the expert affidavit filed by the applicant in response, and the PTO may be compelled to accept the affidavit’s opinions and assertions.”).

106. *In re Wright*, 999 F.2d 1557, 1561–62 (Fed. Cir. 1993) (holding that in rejecting a claim, the examiner must provide a reasonable explanation as to why the patent specification does not meet the enablement requirement).

some less preferred mode for carrying out the invention. The examiner will not typically know about other modes, and if the examiner does, there will be little basis for making an independent determination of which mode is best.¹⁰⁷ The fact that the relevant question is the inventor's knowledge at the time of filing creates additional barriers to denying an application for failure to comply with the best mode requirement. The examiner is not in a position to determine the full scope of the inventor's knowledge. Moreover, in reviewing a patent application it is irrelevant whether others, including those working in the same corporation as the inventor, know of a better mode.¹⁰⁸ As a result, the Manual of Patent Examining Procedure states as follows:

The examiner should assume that the best mode is disclosed in the application, unless evidence is presented that is inconsistent with that assumption. It is extremely rare that a best mode rejection properly would be made in *ex parte* prosecution. The information that is necessary to form the basis for a rejection based on the failure to set forth the best mode is rarely accessible to the examiner, but is generally uncovered during discovery procedures in interference, litigation, or other *inter partes* proceedings.¹⁰⁹

To be sure, a court might later determine a patent is invalid because of a failure to meet the disclosure requirements. Yet even in litigation, proving that the applicant withheld the best mode known to the inventor might be difficult. When a party challenging the patent demonstrates a better mode, the patent holder can claim the inventor did not know about that better mode at the time of filing; rather, additional use and development of the invention revealed the better mode. Because the inventor's knowledge at the time of filing is what matters, the applicant generally need not update a pending application if the inventor becomes aware of a better mode before the patent issues.¹¹⁰ Case law also cre-

107. The Federal Circuit has explained:

[A] proper best mode analysis has two components. The first is whether, at the time the inventor filed his patent application, he knew of a mode of practicing his claimed invention that he considered to be better than any other. This part of the inquiry is wholly subjective, and resolves whether the inventor must disclose any facts in addition to those sufficient for enablement. If the inventor in fact contemplated such a preferred mode, the second part of the analysis compares what he knew with what he disclosed—is the disclosure adequate to enable one skilled in the art to practice the best mode or, in other words, has the inventor “concealed” his preferred mode from the “public”? Assessing the *adequacy* of the disclosure, as opposed to its *necessity*, is largely an objective inquiry that depends upon the scope of the claimed invention and the level of skill in the art. Notwithstanding the mixed nature of the best mode inquiry, and perhaps because of our routine focus on its subjective portion, we have consistently treated the question as a whole as factual.

Chemcast Corp. v. Arco Indus. Corp., 913 F.2d 923, 927–28 (Fed. Cir. 1990) (emphasis in original).

108. See *Glaxo, Inc. v. Novopharm, Ltd.*, 52 F.3d 1043, 1050 (Fed. Cir. 1995) (noting that “there was no violation of the best mode requirement of § 112 by reason of knowledge of the *purported* best mode on the part of a [corporation’s] employees, *other than the inventor*, in the manufacturing group when the inventor did not know of or conceal this best mode” (emphasis in original)).

109. USPTO, *supra* note 104, § 2165.03.

110. See *Transco Prods., Inc. v. Performance Contracting, Inc.*, 38 F.3d 551, 557 & n.6 (Fed. Cir. 1994) (holding that the “the date for evaluating a best mode disclosure in a continuing application is the date of the earlier application with respect to common subject matter,” but noting that “if a claim

ates an additional incentive for applicants to leave out information from the best mode description. The Federal Circuit has held that there is no general requirement to disclose production details—such as the names of specific materials and their suppliers, manufacturing processes, or specific techniques—so long as the description provided is sufficient for enablement in light of what a person skilled in the arts would already know.¹¹¹

It is impossible to know how many patent applicants fail to comply fully with the enablement and best mode requirements, and yet still obtain a patent.¹¹² The case law, of course, tells us only about the instances where another party challenges the validity of a patent on the ground that the applicant did not meet the enablement and best mode standards.¹¹³ Many more instances likely escape detection or litigation.¹¹⁴

3. How Patent Holders Use Undisclosed Information

Patent holders who disclose less to the USPTO than is required can

in a continuation-in-part application recites a feature which was not disclosed or adequately supported by a proper disclosure under 35 U.S.C. 112 in the parent application, but which was first introduced or adequately supported in the continuation-in-part application such a claim is entitled only to the filing date of the continuation-in-part application”).

111. *Wahl Instruments, Inc. v. Acvious, Inc.*, 950 F.2d 1575, 1580 (Fed. Cir. 1991); *Randomex, Inc. v. Scopus Corp.*, 849 F.2d 585, 590 (Fed. Cir. 1988); *In re Gay*, 309 F.2d 769, 774 (C.C.P.A. 1962).

112. How-to manuals advise patent applicants to limit disclosure. *See, e.g.*, ALAN L. DURHAM, *PATENT LAW ESSENTIALS: A CONCISE GUIDE* 74 (1999) (“Although a patent specification must reveal the inventor’s best mode . . . the level of detail that must be included is not unlimited. . . . It need not . . . disclose all of the . . . information that a factory foreman would need . . . for production. Such detailed information would . . . be an unnecessary gift to . . . competitors.”); JAMES L. ROGERS, *THE COMPLETE PATENT KIT* 33 (2005) (“The more that is known in the prior art about the nature of your invention . . . the less information needs to be explicitly stated in your specification.”).

113. *See Enzo Biochem, Inc. v. Calgene, Inc.*, 188 F.3d 1362, 1377 (Fed. Cir. 1999) (holding that claims in two patents directed to genetic antisense technology were invalid because the breadth of enablement was not commensurate in scope with the claims); *Great N. Corp. v. Henry Molded Prods.*, 94 F.3d 1569, 1574 (Fed. Cir. 1996) (holding invalid, for failure to disclose the best mode, a patent which disclosed a structure for protectively supporting and spacing rolls of web material in a multi-layer stack); *U.S. Gypsum Co. v. Nat’l Gypsum Co.*, 74 F.3d 1209, 1214–16 (Fed. Cir. 1996) (holding that the best mode requirement was not met with respect to a patent for joint compound); *In re Goodman*, 11 F.3d 1046, 1053–54 (Fed. Cir. 1993) (holding that the enablement requirement was not met with respect to the claimed method of producing protein in plant cells by expressing a foreign gene); *In re Wright*, 999 F.2d 1557, 1564 (Fed. Cir. 1993) (holding that the enablement requirement was not met with respect to vaccines against retroviruses); *Consol. Aluminum Corp. v. Foseco Int’l Ltd.*, 910 F.2d 804, 807–15 (Fed. Cir. 1990) (holding a patent unenforceable because of the patentee’s inequitable conduct consisting of the substitution in one patent’s specification of a fictitious, inoperable mode for the patentee’s contemplated best mode).

114. *See* FED. TRADE COMM’N, *supra* note 88, ch. 4, at 41 (“Several panelists argued that business method patents, which frequently encompass software-automated or online processes, are not enabling”); *Competition and Intellectual Property Law and Policy in the Knowledge-Based Economy: Hearing Before the Fed. Trade Comm’n* 53 (Mar. 20, 2002) (statement of Daniel McCurdy, President and CEO of ThinkFire), *available at* <http://www.ftc.gov/opp/intellect/020320trans.pdf> (“[I]n spite of what the Constitution tells us and the body of law teaches us, the fact is that patents seldom teach enough so that someone can actually go out and actually do the invention without some additional work. . . . [T]hey are extraordinarily complicated innovations and so frequently what happens in modern licensing practice is that increasingly companies will actually license know-how.”); Dan L. Burk & Mark A. Lemley, *Is Patent Law Technology-Specific?*, 17 *BERKELEY TECH. L.J.* 1155, 1195–96 (2002) (suggesting that narrower patents resulting from more stringent disclosure requirements might better promote innovation in a software industry characterized by incremental improvements).

use the undisclosed information to their advantage. For example, they can elect to make it confidentially available to preferred licensees of the patented invention who are willing to pay a premium.¹¹⁵ Patent holders can also use the information to prevent competition. In particular, patent holders can make use of contract law to license their products to users who agree to licensing terms that expand the licensor's rights. In exchange for access to the product, the licensee might be required to agree not to reverse engineer the patented invention and thereby discover the non-disclosed information. In the case of integrated systems containing patented and non-patented components, a licensee might have to agree contractually not to reverse engineer non-patented components. Patent holders might use contracts to prevent licensees from lawfully developing or selling alternative, but non-infringing, products. Although licensing terms that run afoul of antitrust law constitute patent misuse,¹¹⁶ courts have upheld non-compete clauses in licenses to use patented inventions.¹¹⁷ Licensors might also use contracts to prevent licensees from lawfully developing interoperable products.¹¹⁸ Contractual terms that prohibit reverse engineering for interoperability purposes are common in software licensing,¹¹⁹ which is traditionally protected by copyright and

115. See JAMES D. HAMILTON & WILLIAM E. BEAUMONT, LICENSING PATENTS AND TRADE SECRETS § 1.01 (June 2000), available at <http://www.oblon.com/media/index.php?id=53> (“[I]t is often beneficial to the licensor to suggest that a license agreement incorporate both patent and trade secret rights, so as to thus constitute a hybrid agreement, or to alternatively separately license the trade secrets and to make available the nonpatented information within the knowledge of the owner of the patent and its employees who have become familiar with the use of the patented technology.”).

116. See *County Materials Corp. v. Allan Block Corp.*, 502 F.3d 730, 734–36 (7th Cir. 2007) (describing the doctrine of patent misuse and its limitations).

117. See, e.g., *id.* at 736–39 (rejecting a patent misuse claim and upholding a contract in which the licensee obtained exclusive rights to manufacture licensor's patented concrete blocks and agreed not to sell non-infringing competing products for eighteen months in a specified market if it stopped making the product).

118. See generally Daniel Laster, *The Secret Is Out: Patent Law Preempts Mass Market License Terms Barring Reverse Engineering for Interoperability Purposes*, 58 BAYLOR L. REV. 621, 624–26 (2006) (providing examples of mass market software licensing terms prohibiting reverse engineering of software, and arguing that patent law should preempt use of licenses to prohibit reverse engineering to develop interoperable products).

119. See, e.g., ProQuest, *Terms and Conditions*, <http://www.csa.com/csallumina/termsandconditions.php> (last visited Oct. 17, 2008) (“By accessing the Product(s), you, the Institution listed on the Order Form, agree that you and your Authorized Users are bound as follows: . . . 10. Access and Use. a. ProQuest® CD-ROM Products may include software to be used in connection with the Products. It may not be reverse engineered or used for any other purpose.”). Courts have upheld contracts that prohibit reverse engineering. See, e.g., *Davidson & Assocs. v. Jung*, 422 F.3d 630, 638–39 (8th Cir. 2005) (concerning software users' reverse engineering of software to create interoperable program, holding that a licensing agreement not to reverse engineer the software was valid and not preempted by federal copyright law); *Bowers v. Baystate Techs., Inc.*, 320 F.3d 1317, 1325–26 (Fed. Cir. 2003) (noting that “private parties are free to contractually forego the limited ability to reverse engineer a software product under the exemptions of the Copyright Act,” and upholding a shrinkwrap contract that prevented reverse engineering of computer-aided design programs that were both copyrighted and patented). By contrast, in *Vault v. Quaid Software Ltd.*, 847 F.2d 255 (5th Cir. 1988), the Fifth Circuit invalidated a state law authorizing contracts that prohibited “any process by which computer software is converted from one form to another form which is more readily understandable to human beings, including without limitation any decoding or decrypting of any computer program which has been encoded or encrypted in any manner.” *Id.* at 268–70 (quoting LA. REV. STAT. ANN. § 51:1962(3) (1987)). The court found the state law in conflict with 17 U.S.C. § 117, which permits a computer program owner to make an adaptation of a program provided that the ad-

is increasingly the subject of patent protection.¹²⁰

4. The Erosion of Trade Secrets' Traditional Limits

Viewed from a different angle, contracts can also undermine the traditional contours of trade secrets. With patentees licensing, rather than selling, their products and licensing terms restoring protections that are normally lost through public disclosure of information as a matter of trade secret law, contracts can allow corporations to enjoy the benefits of patent protection while also limiting the flow of information to the public domain.¹²¹ Contracts prohibiting reverse engineering and development of non-infringing products present a problem that is quite different from the one the United States Supreme Court dealt with in *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*¹²² In that case, a state statute prohibited reverse engineering of a public domain work, and the Court held that federal law preempted state law.¹²³ A contract in which a party has agreed to refrain from doing something permissible under federal intellectual property law is a different scenario. Absent a similar finding of preemption, or an extension of misuse doctrines, the combination of minimal disclosure to the USPTO and restrictive licensing terms threatens to upset the balance Congress has set between patent protection and the public domain.¹²⁴ The emergence of this combined threat also puts into question the traditional assumption by courts that limited state law protections for trade secrets are compatible with federal intellectual property laws.¹²⁵ More generally, trade secret law is not

aptation is either created as an essential step in the utilization of the computer program in conjunction with a machine or is for archival purpose only. *Id.* at 270. Courts have recognized a fair use defense to copyright infringement for decompiling and reverse engineering software “solely in order to discover the functional requirements for compatibility.” *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1522 (9th Cir. 1993); *see also* *Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596, 602–04 (9th Cir. 2000) (holding that intermediate copying to access unprotected functional elements of a software program to achieve interoperability was fair use); *Atari Games Corp. v. Nintendo of Am., Inc.*, 975 F.2d 832, 843 (Fed. Cir. 1992) (holding that “reverse engineering object code to discern the unprotectable ideas in a computer program is a fair use”). The Digital Millennium Copyright Act of 2000 generally prohibits circumvention of technological safeguards, yet permits the use of circumvention technology for the purpose of achieving interoperability. 17 U.S.C. § 1201(f) (2006).

120. Bradford L. Smith & Susan O. Mann, *Innovation and Intellectual Property Protection in the Software Industry: An Emerging Role for Patents?*, 71 U. CHI. L. REV. 241, 242 (2004).

121. Laster, *supra* note 118, at 642 (“[W]hat had until recently been a state law right in trade secrets circumscribed by the doctrine of permissible . . . [reverse engineering] of mass distributed products has now potentially expanded effectively by contract law (including choice of law terms) into a nation-wide property right without any of the limitations built into other IP regimes, such as novelty, nonobviousness, experimental use, first sale, fair use, or misuse.”).

122. 489 U.S. 141 (1989); *see supra* note 48 and accompanying text.

123. *Bonito Boats*, 489 U.S. at 166.

124. Caution is warranted in relying upon preemption or misuse in the context discussed in this section. *See* Reichman & Franklin, *supra* note 83, at 920 (describing the limitations of preemption and misuse doctrine and concluding that “these doctrines as currently administered give courts no solid foundation for coping with the downside social risks inherent in an unprecedented meshing of federal intellectual property policies with state-enforced contracts of adhesion”).

125. Although the discussion has focused on licensing agreements and trade secrets, corporations might use other kinds of contracts to claim additional rights. For example, some courts have upheld

on par with patent law. Federal law is superior to state law, and it expresses a clear congressional policy preference for the disclosure of inventions.¹²⁶ As the Federal Circuit has explained, “As between a prior inventor who benefits from a process by selling its product but suppresses, conceals, or otherwise keeps the process from the public, and a later inventor who promptly files a patent application . . . the law favors the latter.”¹²⁷ Increased use of trade secrets can undermine the policy choice that Congress has made.¹²⁸

Congress could act to deal with these problems in order to protect its policy preferences. This section has focused on inadequate fulfillment of the enablement and best mode requirements under section 112, as undermining the purposes of the patent laws by contributing to faulty patents and allowing the collateral licensing of undisclosed information. Congress could strengthen the enablement and best mode requirements in ways that promote disclosure. For example, rather than an undue experimentation and reasonableness standard, Congress could require the enablement to provide sufficient information so that, with a clear degree of certainty, a person skilled in the relevant art could make and use the invention. Congress could provide for randomized testing to determine if the enablement requirement is met, for example by engaging a consultant with the relevant skill to review the enablement or, in appropriate circumstances, to actually make and use the invention or some part

employment contracts that prevent employees from disclosing information beyond trade secrets. *See, e.g.,* Simplified Telesys, Inc. v. Live Oak Telecom, L.L.C., 68 S.W.3d 688, 693–94 (Tex. App. 2000) (finding it irrelevant in breach of confidentiality action whether information was a trade secret “[b]ecause the written confidentiality agreements prohibit unauthorized use of any kind of ‘Confidential Information’ . . . whether entitled to trade-secret status or not”). Other courts have allowed unfair competition claims based on a breach of a confidentiality agreement even though the disclosed information did not qualify as a trade secret. *See, e.g.,* Imax Corp. v. Cinema Techs., Inc., 152 F.3d 1161, 1169 (9th Cir. 1998) (“Under California law a plaintiff can maintain a common law unfair competition claim regardless of whether it demonstrates a legally protectable trade secret.”).

126. *See, e.g.,* Scott Paper Co. v. Marcalus Mfg. Co., 326 U.S. 249, 255 (1945) (“The aim of the patent laws is not only that members of the public shall be free to manufacture the product or employ the process disclosed by the expired patent, but also that the consuming public at large shall receive the benefits of the unrestricted exploitation, by others, of its disclosures.”).

127. *W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1550 (Fed. Cir. 1983).

128. We therefore disagree with Professor Jorda’s argument that a “good case can be made . . . that the trade secret owner has a de facto prior user right to continue the practice of his trade secret,” notwithstanding the grant of a patent, based on common law rights, principles of equity, and the Due Process and Takings Clauses of the Constitution. Jorda, *supra* note 2, at 26. This effort to elevate trade secret protections over patent protections is unpersuasive. The Patent Act and the relevant case law make clear that if an inventor eschews patent protection and relies upon trade secret law, the trade secret will not act as prior art to prevent a later inventor from patenting the same invention and excluding the trade secret holder. *See* 35 U.S.C. § 102 (2000) (“A person shall be entitled to a patent unless . . . (g)(1) during the course of an interference . . . another inventor involved therein establishes . . . that before such person’s invention thereof the invention was made by such other inventor and not abandoned, suppressed, or concealed, or (2) before such person’s invention thereof, the invention was made in this country by another inventor who had not abandoned, suppressed, or concealed it.”); *W.L. Gore & Assocs., Inc.*, 721 F.2d at 1550. Equitable principles provide stronger justification for prior user right in first-to-file systems than in the first-to-invent system in place in the United States. It is exceedingly unlikely that the Supreme Court would hold the prior art provisions of the Patent Act unconstitutional on due process or takings grounds.

of it. Similarly, Congress could strengthen the best mode requirement by mandating disclosure of all modes known to the inventor, along with a designation of which mode is the best. Likewise, Congress could require disclosure of modes known to anyone working in the same corporation as the inventor and of any additional modes that come to light during the pendency of the application.¹²⁹ Congress could also empower officials in the USPTO to subpoena, in borderline cases, information from the inventor and the inventor's employer.

Whether any of these particular changes are viable—some would be very costly—or ultimately effective, the general point remains that Congress has the power to alter the section 112 requirements in order to promote additional disclosure to the USPTO prior to the issuance of the patent. Nonetheless, relying on Congress to respond to whatever problems trade secret law produces is far from a perfect fix.

Creating an overall system of intellectual property that strikes a desirable balance between the rights of private parties and the public domain is far from easy. This point brings us to the subject of the next section: the benefits and risks of an integrated approach to intellectual property law.

V. INTEGRATION AND ITS LIMITS

As Professor Jorda rightly notes, intellectual property law is a poorly defined and poorly integrated field.¹³⁰ Universal reliance on the term “intellectual property law” to unify patents, trademarks, and copyrights, is a relatively recent development.¹³¹ Even today, the field of intellectual property law defies easy categorization. It exists as a collection of legal doctrines protecting intangibles that perhaps one should not even think of as “intellectual”¹³² or as “property.”¹³³ Currently, the

129. *Cf.* *Plant Genetic Sys., N.V. v. DeKalb Genetics Corp.*, 315 F.3d 1335, 1343–44 (Fed. Cir. 2003) (holding that the district court properly used post-filing work to test whether patent claims were enabled).

130. *See* Jorda, *supra* note 2, at 18.

131. Professor Mark Lemley contends that “[t]he modern use of the term intellectual property as a common descriptor of the field probably traces to the foundation of the World Intellectual Property Organization (WIPO) by the United Nations [in 1967].” Mark A. Lemley, *Property, Intellectual Property, and Free Riding*, 83 TEX. L. REV. 1031, 1033 n.4 (2005). The historical record is probably more complex. Numerous nineteenth-century commentators used the term “intellectual property.” *See, e.g.*, R.R. BOWKER, COPYRIGHT: ITS LAW AND ITS LITERATURE 2 (1886) (describing copyright as intellectual property); N.S. SHALER, THOUGHTS ON THE NATURE OF INTELLECTUAL PROPERTY AND ITS IMPORTANCE TO THE STATE (1878) (discussing patents and copyrights as intellectual property); LYSANDER SPOONER, THE LAW OF INTELLECTUAL PROPERTY (1855) (discussing the rights of authors and inventors as intellectual property). Nonetheless, the term was not universal. *See* Paris Convention for the Protection of Industrial Property, art. 1, § 2, Mar. 20, 1883, 21 U.S.T. 1583 (providing that *industrial property* includes “patents, utility models, industrial designs, trademarks, service marks, trade names, indications of source or appellations of origin, and the repression of unfair competition.”) (emphasis added).

132. In particular, it is hard to see the right of publicity as protecting something that is intellectual in the same way as a book, an invention, or a mark, which are products of the mind. Casebooks reflect this difficulty. *See, e.g.*, ROCHELLE COOPER DREYFUSS & ROBERTA ROSENTHAL KWALL,

field of intellectual property law exists as three major sub-fields: copyright, patent, and trademark. All are now the province of federal law, while state laws govern trade secrets and rights of publicity. Despite efforts to approach the sub-fields holistically and to consider how they inform one another, they remain largely distinct.¹³⁴ In law schools, aside from a basic survey course, the three major sub-fields exist as distinct areas of study and the responsibility of different faculty members; some intellectual property courses and programs omit state laws of trade secret and rights of publicity entirely. In practice, intellectual property lawyers tend to specialize in one or two of the major sub-fields. Clients with a trademark issue look for a trademark lawyer, not an intellectual property lawyer. There is a particularly strong distinction between patent lawyers on the one hand and copyright and trademark lawyers on the other. Conferences, bar committees, and continuing legal education programs likewise reflect a basic separation in intellectual property law among the specialties and the specialists.

It makes considerable sense to examine, as Professor Jorda urges, how different intellectual property laws can protect the same subject matter. Rather than a single form of intellectual property safeguarding the interests of a creator or an inventor, the best source of protection often depends upon the particular context, and so can shift from one situation to another. Consider, for example, the case of sound recordings. Everyone knows today—in no small part because recent industry lawsuits against individuals who illegally share copyrighted music files have put the issue in the news—that federal copyright law protects sound recordings. The longer history of protections for sound recordings sheds light on modern practices. Sound recordings have been protected from unauthorized duplication since Thomas Edison unveiled the first commercial audio playback device in 1877.¹³⁵ However, federal copyright law did not protect sound recordings until the passage of the Sound Re-

INTELLECTUAL PROPERTY: CASES AND MATERIALS ON TRADEMARK, COPYRIGHT AND PATENT LAW 538–63 (2d ed. 2004) (omitting rights of publicity from the casebook title but including two principal cases on the issue).

133. See Cory Doctorow, “*Intellectual Property*” Is a Silly Euphemism, THE GUARDIAN, Feb. 21, 2008, available at <http://www.guardian.co.uk/technology/2008/feb/21/intellectual.property> (“[T]he phrase ‘intellectual property’ is, at root, a dangerous euphemism that leads us to all sorts of faulty reasoning about knowledge.”); Mark A. Lemley, *Property, Intellectual Property and Free Riding*, *supra* note 131, at 1033 (commenting that while “intellectual property” is a “sexy” term, the rhetoric and theory behind real property law is not necessarily compatible with the intangibles it describes).

134. See, e.g., JAY DRATLER, JR. & STEPHEN M. MCJOHN, 1 INTELLECTUAL PROPERTY LAW: COMMERCIAL, CREATIVE, AND INDUSTRIAL PROPERTY vii (1991); ROBERT P. MERGES, PETER S. MENELL, & MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE xxi–xxii (4th ed. 2006).

135. See WILLIAM F. PATRY, PATRY ON COPYRIGHT § 1.70 (2008) (discussing the history of intellectual property protections for sound recordings); Sidney A. Diamond, *Sound Recordings and Phonorecords: History and Current Law*, 1979 U. ILL. L.F. 337, 345–51 (1979) (observing that “the profitability of unauthorized duplication of sound recordings has attracted the technical ingenuity of ‘pirates’ from the earliest days of the recording industry,” and tracing the early legal protections for sound recordings).

cordings Amendment Act of 1971.¹³⁶ That law passed, in large part, to ward off home duplication of commercial sound recordings available to average consumers for the first time with the introduction of the recordable audiocassette in the 1960s. For almost one hundred years previously, the intellectual property interests in sound recordings were protected primarily by technological barriers to consumer copying, patents on playback and recording devices—including Edison’s patent on the phonograph—and various state common law copyright rules.

Today, another shift is occurring, with trademark and branding playing an increasingly important role in the music industry. After a sound recording enters the public domain, the recording can retain commercial value to the prior copyright holder, typically a record label, which can parlay its brand and associated reputation into new sales. In the United Kingdom, because of a shorter copyright period for sound recordings than exists in the United States, many popular jazz, pop, and early rock ‘n’ roll standards have already entered the public domain and continue to do so with each passing year.¹³⁷ Yet original labels continue to sell and profit from many of these works because distributors and consumers place a premium on the authenticity and quality the label provides.¹³⁸ This is true even though other vendors are able to provide the same recording with the same quality more cheaply.

Trademark and branding can also play a role where copyright, though available, does not adequately serve an artist’s or a label’s interests. For example, in October 2007, the alternative rock band Radiohead released its album, *In Rainbows*, directly to consumers via Internet download, without the support of a record label and at whatever price

136. Sound Recordings Amendment Act of 1971, Pub. L. No. 92-140, 85 Stat. 391 (1971) (codified as amended in scattered sections of 17 U.S.C.).

137. In the United Kingdom, sound recordings are protected for fifty years. Copyright, Designs and Patents Act, 1988, c. 48, § 13A(1) (Eng.). In the United States, the protection runs for the life of the author plus seventy years. 17 U.S.C. § 302(a) (2006).

138. One example of the phenomenon is Capitol Jazz/Blue Note’s continued sales of Miles Davis’ 1949 album, *Birth of the Cool*. Though the album entered the public domain in the United Kingdom in 1999, Blue Note, the original label, issued a re-mastered double disc set as *The Complete Birth of the Cool* in 1998, and another single disc remastered edition of the original release with a booklet of essays in 2001. See Blue Note Records, *Miles Davis Discography*, <http://www.bluenote.com/ArtistDiscography.aspx?ArtistId=902304> (last visited Oct. 17, 2008) (providing a catalog of Miles Davis’ recordings). Sales in the United Kingdom remain strong for the Capitol Jazz/Blue Note releases. At Amazon’s U.K. site, the single disc remastered release is the number-one seller for Capitol, and it is ranked number two in the category of Jazz/Instruments/Trumpet and ranked 2,126 of all music sales. See Amazon.co.uk, http://www.amazon.co.uk/Birth-Cool-Miles-Davis/dp/B00005614M/ref=sr_1_1?ie=UTF8&s=music&qid=1221715237&sr=8-1 (last visited Oct. 17, 2008). At the U.K. iTunes Store, the single and double disc versions released by Capitol Jazz/Blue Note are in the top six sellers for Miles Davis albums out of a total of 225 listings; no third-party versions are available. See Apple iTunes, www.apple.com/uk/itunes (results obtained by searching for “Miles Davis” in the “Search iTunes store” box, clicking on “Miles Davis” under “Artists and More,” and then selecting the option to sort albums retrieved by “bestsellers”) (last visited Oct. 17, 2008). The popular U.K. music sites, HMV and Zavvi, carry the Capitol Jazz/Blue Note versions and list third-party versions as unavailable. See HMV, <http://hmv.com> (search for “Birth of the Cool”) (last visited Oct. 17, 2008); Zavvi, <http://www.zavvi.co.uk> (search for “Birth of the Cool”) (last visited Oct. 17, 2008).

individual consumers chose to pay for the album, including an option to pay nothing at all.¹³⁹ Though the band, previously signed to EMI/Capitol Records, took a financial risk in making the new album available in this manner, it received substantial marketing benefits and enhanced the value of its brand. Making music available for free attracted widespread press coverage; consumers who downloaded the album had to enter their names and e-mail addresses, thereby building a massive fan database. The high volume of traffic on the band's website increased public awareness of the band and its other albums and future projects. In the spring of 2008, Radiohead began a sold-out world tour, with record turnouts resulting from the band's enhanced reputation and increased fan base.¹⁴⁰ Radiohead elected to forego payments it was entitled to under copyright law, but it enhanced the value of its mark.

While an integrated approach to intellectual property law makes general sense, it does not follow that all efforts by private parties to use multiple forms of intellectual property law to protect their creations and inventions are necessarily desirable. Each assertion of an intellectual property right should lead us to ask whether recognizing it would promote the creativity that underlies intellectual property laws.¹⁴¹ On this score, integrating trade secret law with patent law, as Professor Jorda advocates, presents some special risks.

Trade secret law is a peculiar branch of intellectual property law in that it is state law. At the federal level, in creating detailed laws of copyright, trademark, and patent, Congress has created a careful balance between specified intellectual property rights conferred upon authors and inventors and the public domain. Congress can, and does, alter the assignment of rights when it concludes that the system is out of balance.¹⁴² Making state-governed trade secret law part of the overall

139. See Press Release, ComScore, For Radiohead Fans, Does "Free"+"Download"= "Free-load"?, (Nov. 5, 2007), <http://www.comscore.com/press/release.asp?press=1883> (last visited Oct. 17, 2008) (reporting that although around sixty percent of fans in the United States paid nothing for the album, the remaining forty percent chose to contribute an average of \$8.05 per download). The CD, released three months after the album was available for free downloading, hit number one on the charts within a week. Jeff Leeds, *Radiohead Finds Sales, Even After Downloads*, N.Y. TIMES, Jan. 10, 2008, at E1, available at http://www.nytimes.com/2008/01/10/arts/music/10radio.html?_r=1&scp=1&sq=Radiohead%20Finds%20Sales,%20Even%20After%20Downloads&st=cse&oref=slogin.

140. See Eliot Van Buskirk, *New In Rainbows Numbers Offer Lessons for Music Industry*, WIRED, July 31, 2008, available at <http://blog.wired.com/music/2008/07/new-in-rainbows.html> ("Radiohead's strategy was a success . . . contributing to the album topping the charts in both the UK and United States and a successful worldwide tour.").

141. See U.S. CONST. art. I, § 8 (giving Congress power "to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries").

142. See *Eldred v. Ashcroft*, 537 U.S. 186, 222 (2003) (noting that "[a]s we read the Framers' instruction, the Copyright Clause empowers Congress to determine the intellectual property regimes that, overall, in that body's judgment, will serve the ends of the Clause," and rejecting a constitutional challenge to the Copyright Term Extension Act of 1998); *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 429 (1984) ("[I]t is Congress that has been assigned the task of defining the scope of the limited monopoly [rights] that should be granted to authors or to inventors in order

balance, however, is not so easy.

Congress has power to preempt state trade secret law it considers undesirable, and federal legislation can take account of the nature and degree of state law protections. For instance, strengthening the enablement and best mode requirements of section 112 could counteract the problems discussed in this article of inadequate disclosures to the USPTO and the licensing of access to undisclosed information. However, it remains more difficult to maintain a desired balance between rights and the public domain when the balance can be altered through lawmaking by another sovereign or, as in our federal system of government, by fifty other sovereigns. Moreover, because state law cannot cut back on federal intellectual property rights, it is likely to alter the balance by enhancing the interests of owners of intellectual property. Increased use of state trade secret law is, therefore, likely to have the effect of reducing the public domain. Integrating trade secret law with federal intellectual property law is likely to lead to a recalibration of Congress' intellectual property balance in a way that reduces what is available to the public.

VI. CONCLUSION

The Americans who wrote and ratified the United States Constitution could not have predicted that the "Progress of Science"¹⁴³ would lead to the technological marvels of the digital age. Nonetheless, the founding generation placed a high value on public access to knowledge and would celebrate the flow of information that digital technology enables. Consistent with this vision, the Constitution empowered Congress to create a system of intellectual property laws that incentivize invention and disseminate the fruits of progress. Secret knowledge is not knowledge shared. State trade secret law can undermine, rather than complement, the value of public access that the Constitution reflects and that Congress has sought to pursue. In the digital age, as in the age of the founding generation, efforts to lock up valuable knowledge should be met with vigilance and skepticism.

to give the public appropriate access to their work product.").

143. U.S. CONST. art. I, § 8.

