Denver Law Review

Volume 93
Issue 4 *Symposium - Future World IP: Legal Response to the Tech Revolution*

Article 3

January 2016

Secrecy is Dead - Long Live Trade Secrets

Derek E. Bambauer

Secrecy is Dead - Long Live Trade Secrets

SECRECY IS DEAD – LONG LIVE TRADE SECRETS

DEREK E. BAMBAUER†

ABSTRACT

The future of intellectual property is in trade secrets. Changes to patent law make obtaining a patent more costly in some cases and impossible in others. The relentless spread of networked computing, with its inevitable vulnerabilities, and digital data make non-legal means of maintaining secrecy increasingly unreliable. Innovators will be forced to turn to trade secrets. This newfound prominence for trade secrecy will generate tensions with freedom of speech protections, federalism, and the balance between civil and criminal enforcement. The Article, part of a symposium on the Future World IP by the *Denver Law Review*, closes with a set of testable empirical predictions to evaluate its claims.

TABLE OF CONTENTS

I. INTRODUCTION

The future of intellectual property is in trade secrets.

This Article predicts that innovators will shift to using trade secret law to safeguard advances, rather than filing for patent protection or using contractual and technological self-help to keep inventions confidential. There are two reasons for this coming rise of trade secrets. The first is that other means of keeping advances secret are becoming far less effective in the digital networked era. The second is that obtaining a patent has become more difficult and less certain with recent doctrinal developments. By process of elimination, that leaves trade secret law to fill the

† Professor of Law, James E. Rogers College of Law, University of Arizona. This Article is part of a symposium on *Future World IP: Legal Responses to the Tech Revolution*, hosted by the *Denver Law Review*. Thanks for helpful suggestions and discussion are owed to Jane Bambauer, Dan Hunter, Thinh Nguyen, Simone Sepe, and the participants in the conference on Competition Policy, Innovation, and Procurement, Institute for Advanced Study in Toulouse. The author welcomes comments at derekbambauer@email.arizona.edu.

gap—innovators will rely on relative rather than absolute secrecy. This will lead to development of and pressure on that field's doctrine, raising questions of federalism, enforcement, and conflict with other legal regimes. Normatively, this Article comes neither to praise the rise of trade secret nor to bury it, but to elucidate tensions and issues that will accompany its new prominence.

This Article continues with three additional Parts. The first explains why doctrinal changes have made patents harder to obtain and what technological changes have made secrecy more difficult to maintain. The second explores the changes that increased reliance on trade secret will generate, including pressure on other doctrines, on federalism, and on criminal enforcement of intellectual property. The final Part concludes by making a set of testable predictions about the shift this Article foresees.

II. SECRETS AND DISCLOSURE

A. Two Roads Diverged: Protecting Innovation[1]

Intellectual property scholars typically present the decision on how to protect innovation, such as a new medication or the process used to synthesize it, as a binary choice: apply for a patent, or protect the advance as a trade secret.[2] That framing is inaccurate. The correct way to understand the decision is to contrast patenting, with its concomitant disclosure of the advance to the public, with secrecy.[3] Trade secret law is merely one way of protecting a secret. It is normally called into action when other methods of maintaining secrecy—non-disclosure agreements, encryption, printing on copy-proof pages—have failed or are about to do so.[4] If the precautions to maintain secrecy that are required by the doctrine function as designed, then, there is no reason to call the legal system into action. Trade secret operates in an ex post world, a last ditch effort to prevent information from being revealed or to claw it back once it has been disclosed.[5] The innovator's choice, then, is whether to try to keep the advance secret, or to disclose it in the hope of obtaining a patent, knowing that each road brings risks and costs.

---

1. With apologies to Robert Frost. ROBERT FROST, *The Road Not Taken*, *in* THE ROAD NOT TAKEN AND OTHER POEMS 1, 1 (Stanley Appelbaum ed., 1993).

2. *See, e.g.*, David D. Friedman, William M. Landes & Richard A. Posner, *Some Economics of Trade Secret Law*, 5 J. ECON. PERSP. 61, 62–66 (1991).

3. *See* Derek E. Bambauer & Simone M. Sepe, Top Secret(s) 3 (unpublished manuscript) (on file with author).

4. *See* Robert G. Bone, *The (Still) Shaky Foundations of Trade Secret Law*, 92 TEX. L. REV. 1803, 1818 (2014); Joshua Rivera, *Here's the Extreme Measure Taken to Prevent the 'Star Wars: The Force Awakens' Script from Leaking*, TECH INSIDER (Aug. 12, 2015, 11:16 AM), http://www.techinsider.io/how-star-wars-is-keeping-its-script-secret-2015-8.

5. *See* Elizabeth A. Rowe, *Saving Trade Secret Disclosures on the Internet Through Sequential Preservation*, 42 WAKE FOREST L. REV. 1, 46–47 (2007).

The trade-offs between patents and trade secrets are well-known. Patents last for twenty years from the date of filing; secrets (including trade secrets) last as long as sufficient secrecy is maintained. Patents protect against everyone who makes, uses, sells, offers to sell, or imports the patented invention in the United States (and some who engage in specified extraterritorial conduct)[6]; trade secret law protects only against those who procure the information through improper means or who are in specified relationships with a misappropriator.[7] Trade secret offers broader subject matter coverage.[8] Its protection occurs immediately, while patent rights are enforceable, with minor exceptions, only after examination and registration by the Patent Office.[9] Patents provide greater notice of the boundaries of the owner's rights, as defined by the claims, while the scope of a trade secret is determined entirely during litigation.[10] And, patents enjoy a statutory presumption of validity, such that challengers in litigation must prove invalidity by a clear and convincing standard, while trade secret owners bear the burden of establishing validity during suits.[11] Patent enforcement is entirely private, while

6. 35 U.S.C. § 271(f)–(g) (2012).

7. The counterpart to the strength of these rights is the availability of defenses. Patent law has very few defenses. The experimental use defense is effectively non-existent under the Federal Circuit's jurisprudence. *See* Madey v. Duke Univ., 307 F.3d 1351, 1361–63 (Fed. Cir. 2002). There are a few industry-specific statutory defenses, such as for doctors performing patented surgical methods, prior business users performing patented business methods, and generic pharmaceutical manufacturers making patented compounds as part of applying to the Food and Drug Administration. *See* 35 U.S.C. § 287(c) (2012) (surgical methods); 35 U.S.C. § 271(e)(1) (pharmaceuticals); 35 U.S.C. § 273 (2012) (business methods). By contrast, trade secret includes broader defenses, including independent discovery, reverse-engineering, and insufficient knowledge on the part of a third-party regarding the existence of an acquired secret. *See* UNIF. TRADE SECRETS ACT § 1 (amended 1985) (NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS 1986) (describing proper means); *id.* § 1(2) (describing third-party liability); Robert G. Bone, *Secondary Liability for Trade Secret Misappropriation: A Comment*, 22 SANTA CLARA COMPUTER & HIGH TECH L.J. 529, 532–33 (2006).

8. *See* Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 317 (2008).

9. 35 U.S.C. § 154(d)(4)(A) (2012) (establishing provisional rights).

10. This point can be overstated. The meaning of claim language is determined by the court during litigation. Markman v. Westview Instruments, Inc., 517 U.S. 370, 388–90 (1996); *see also* Mark A. Lemley, *The Changing Meaning of Patent Claim Terms*, 104 MICH. L. REV. 101, 111 (2005); Peter S. Menell, Matthew D. Powers & Steven C. Carlson, *Patent Claim Construction: A Modern Synthesis and Structured Framework*, 25 BERKELEY TECH. L.J. 711, 717–18 (2010). Even then, certainty is elusive, as the Federal Circuit reverses district court decisions in roughly one-quarter to one-third of its cases. *See* J. Jonas Anderson & Peter S. Menell, *Informal Deference: A Historical, Empirical, and Normative Analysis of the Standard of Appellate Review for Patent Claim Construction*, 108 NW. U. L. REV. 1, 38–39 (2013); *see also* Christian A. Chu, *Empirical Analysis of the Federal Circuit's Claim Construction Trends*, 16 BERKELEY TECH. L.J. 1075, 1104 (2001) (noting a 44% reversal rate in an approximately two-year sample); Kimberly A. Moore, Markman *Eight Years Later: Is Claim Construction More Predictable?*, 9 LEWIS & CLARK L. REV. 231, 239 (2005) (finding a 34.5% reversal rate after a de novo appeal). *But see* Ted Sichelman, *Myths of (Un)Certainty at the Federal Circuit*, 43 LOY. L.A. L. REV. 1161, 1178 (2010).

11. 35 U.S.C. § 282(a) (2012); *see also* Microsoft Corp. v. i4i Ltd. P'ship, 564 U.S. 91, 100–02 (2011).

trade secret misappropriation can result in both state[12] and federal[13] criminal penalties. Finally, relative costs vary widely and are indeterminate. The cost of obtaining a patent depends upon the technology, claims, and skill of the drafter, among other variables;[14] two 2013 surveys estimate the prosecution cost for a moderately complex patent at roughly $10,000.[15] The cost of protecting a secret includes the expense of precautions, such as drafting non-disclosure agreements and installing physical safeguards, and also the expense of litigation if the precautions fail.[16]

Innovators facing the choice between disclosure and secrecy must thus consider a number of factors and then balance them. In some circumstances, there may be only one plausible choice. For example, if the inventor has been selling a product or service embodying the innovation for more than a year, obtaining a patent is not possible, since those sales can be cited as disqualifying prior art against an application.[17] Similarly, the invention may be too small an advance relative to the state of the art in its field, such that an application would be rejected on obviousness grounds.[18] There are also considerations pressing in the other direction: the innovation may be readily discovered on inspection of the product or by reverse-engineering it, such that trade secret protection would be evanescent.[19]

Patenting may also be more valuable for business reasons. Once a patent application has been filed, innovators can rely on it to protect their invention (assuming that the application will be granted in time). Thus, they can disclose details of the invention covered by the patent to potential partners, investors, potential acquirers, and the like, since there is little risk of expropriation.[20] By contrast, innovators relying on secrecy must use devices such as contractual restrictions to ensure that limited disclosure does not destroy the innovation's value. Patents may be easier

12. *See, e.g.*, CAL. PENAL CODE § 499c(b)–(c) (West 2011); MASS. GEN. LAWS ch. 266, § 30(4) (2016); NEV. REV. STAT. § 600A.035 (2015); TEX. PENAL CODE ANN. § 31.05(b) (West 2015).

13. Economic Espionage Act of 1996 § 101(a), 18 U.S.C. §§ 1831–1832 (2012).

14. *See* Stephen Yelderman, *Improving Patent Quality with Applicant Incentives*, 28 HARV. J.L. & TECH. 77, 92 n.79 (2014).

15. Brian J. Love, *Do University Patents Pay Off? Evidence from a Survey of University Inventors in Computer Science and Electrical Engineering*, 16 YALE J.L. & TECH. 285, 310 n.76 (2014).

16. *See* Friedman, Landes & Posner, *supra* note 2, at 63.

17. 35 U.S.C. § 102(a)(1), (b)(1) (2012).

18. 35 U.S.C. § 103 (2012); *see also* KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398, 406 (2007).

19. *See* Andrew A. Schwartz, *The Corporate Preference for Trade Secret*, 74 OHIO ST. L.J. 623, 639 (2013).

20. There could be exceptions. The application's disclosure may be greater than the coverage of the claims, or the mere existence of the application could provide useful information to a competitor about how to design its products. But patent is no worse than trade secret here, since an innovator could always use similar mechanisms (such as non-disclosure agreements) to reinforce its rights.

to value than secrets, since they are readily inspected after publication,[21] and the market may treat patents as a proxy for an innovating firm's value since they act as costly screens.[22] Thus, patents may be treated as honest signals by investors, making innovators more likely to select disclosure over secrecy.

This Article's focus is on changes that shift the equilibrium between secrecy and disclosure. Some changes are industry-specific, such as exclusions from patentable subject matter,[23] and some sweep across all fields, such as the falling cost of disseminating information.[24] In the aggregate, these changes will push innovators away from patent and away from absolute secrecy, towards the relative secrecy of trade secret law.

B. Disclosure and Patents

The conventional wisdom for both innovators and scholars is that patenting is preferable to secrecy. While the road to patenting is costly and long, it rewards an inventor with strong property rights at the successful conclusion of the journey. The shorter duration of patent protection is seen as outweighed by the strength of those rights and by the greater ease of valuing the patent.[25] Patents help innovators exclude competitors, since neither independent discovery nor use after reverse-engineering operate as defenses to liability for infringement. Scholars see the disclosure from patents as driving follow-on innovation and diffusing knowledge.[26]

Regardless of whether one agrees with the conventional wisdom, innovators are likely to use trade secrets more and patents less in the future, due in part to changes in the Patent Act and doctrine that make obtaining a patent more difficult. First, both the text of the statute and judicial interpretations of it have narrowed the scope of patent-eligible subject matter relative to trade secret. The Patent Act protects only four categories of inventions: processes, machines, manufactures, and compositions of matter.[27] Furthermore, with the America Invents Act (AIA), Congress acted to exclude one category of innovation—inventions de-

21. *See* Kenneth J. Arrow, *Economic Welfare and the Allocation of Resources for Invention*, *in* THE RATE AND DIRECTION OF INVENTIVE ACTIVITY: ECONOMIC AND SOCIAL FACTORS 609 (1962).

22. *See* David Fagundes & Jonathan S. Masur, *Costly Intellectual Property*, 65 VAND. L. REV. 677, 679–82 (2012).

23. *See* Mark A. Lemley, Michael Risch, Ted M. Sichelman & R. Polk Wagner, *Life After* Bilski, 63 STAN. L. REV. 1315, 1317, 1325 (2011).

24. *See* Derek E. Bambauer, *Middlemen*, 64 FLA. L. REV. F. 64, 64 (2012).

25. *See generally* Schwartz, *supra* note 19, at 626–42.

26. *See, e.g.*, Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241, 266 (1998) ("If an inventor chooses trade secret instead of patent, others will be denied ready access to the information, access that would exist under patent law."). The disclosure function is disputed, though—Mark Lemley notes that many firms do not read patents and do not perform prior art searches before developing new products. Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 333 n.89 (2008).

27. 35 U.S.C. § 101 (2012).

signed to reduce income tax liability—from patentability, but by treating such inventions as uniformly within the prior art rather than by deeming them ineligible subject matter.[28] Some defenses, such as prior user rights[29] and lack of liability for physicians who practice patents covering surgical methods,[30] mean that while an innovator may formally hold a patent, she may not be able to protect her invention effectively against all those who make, use, or sell it. And, for inventions that may implicate U.S. national security, government entities can prevent inventors from obtaining patents (with the resulting disclosure of sensitive information) via administrative orders.[31]

Courts have grafted a set of exceptions onto the text of the Patent Act's eligible subject matter provision, and the ambit of these exceptions has widened recently. Abstract ideas, laws of nature, and natural phenomena cannot be patented.[32] The Supreme Court has taken up each of these exceptions recently, using its decisions to exclude more inventions from patentability.[33] For example, the Court invalidated claims in a patent held by the biotech firm, Myriad Genetics, that covered isolated DNA codings with a specified sequence of amino acids.[34] The claimed sequences corresponded to mutations that significantly increase a woman's lifetime risk of developing breast or ovarian cancers. The Court held that the claimed sequences were ineligible because they were naturally occurring, even though the patent claimed only the isolated sections of the genes. Even before the case was decided, though, Myriad had changed tactics: it built a confidential database of genetic mutations and the maladies associated with them.[35] Frustrated by patent, Myriad turned to secrecy. Only it could offer a test detecting the risks from these mutations, because only Myriad knew about them.[36]

Second, the AIA increased the amount of prior art that can be cited against an application during prosecution or introduced to invalidate a patent during litigation. Under the previous version of the Patent Act, knowledge or use of the claimed invention counted as prior art only if it

---

28. Leahy-Smith America Invents Act, Pub. L. No. 112-29, § 14, 125 Stat. 284, 327–28 (2011) (codified at 35 U.S.C. §§ 102, 103 (2012)) ("[A]ny strategy for reducing, avoiding, or deferring tax liability . . . shall be deemed insufficient to differentiate a claimed invention from the prior art.").

29. 35 U.S.C. § 273(a) (2012).

30. 35 U.S.C. § 287(c) (2012).

31. 35 U.S.C. § 122(d).

32. Diamond v. Chakrabarty, 447 U.S. 303, 309 (1980).

33. Alice Corp. v. CLS Bank Int'l, 134 S. Ct. 2347, 2358 (2014); Mayo Collaborative Servs. v. Prometheus Labs., Inc., 132 S. Ct. 1289, 1294 (2012); Bilski v. Kappos, 561 U.S. 593, 609 (2010).

34. Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 133 S. Ct. 2107, 2120 (2013).

35. *See* Monya Baker, *Policy Paper: Myriad Turns Cancer Genetic Data into Trade Secrets*, NATURE (Oct. 31, 2012, 23:14 BST), http://blogs.nature.com/news/2012/10/policy-paper-myriad-turns-cancer-genetic-data-into-trade-secrets.html.

36. *Id.* The pattern is the same for methods of reducing tax liability: firms hold these techniques or transactions as secrets. *Id.*

occurred within the United States.[37] The AIA removes that geographic limitation—knowledge or use anywhere that antedates the filing of the patent application will prevent issuance.[38] The AIA also increases the temporal scope of the prior art. Before its enactment, references such as patent applications were available only as of their U.S. filing date or publication date, not their foreign filing date.[39] The AIA alters this rule by treating such applications as prior art based on their filing date, even if the applications were not published or otherwise available to the public on that date.[40] This expands the storehouse of "secret" prior art that can be used to deny or invalidate a patent. The AIA eliminates the possibility of "swearing behind" invalidating prior art that existed under the prior version of the Patent Act—the relevant date is when the application was filed, not when the applicant invented the claimed advance.[41] And, the reform expands the ability of third parties to submit prior art during examination, increasing the likelihood that relevant references will be considered.[42] Finally, the inclusion of a prior user defense under the AIA moves the patent regime towards trade secret in that independent invention, if the defendant made commercial use of the claimed invention more than one year prior to the relevant date of filing or public disclosure, prevents liability.[43] In short, the AIA makes more references available in the prior art that can prevent a patent from issuing.

Lastly, the AIA offers new avenues for challenging an issued patent other than litigation in federal district court. Post-grant review enables anyone to attack the validity of a patent within a nine-month period after issuance.[44] The challenge can be based on any of the grounds for invalidating a patent during litigation, such as lack of novelty or obviousness.[45] The party instituting post-grant review bears the burden of persuasion, but that burden is less weighty: it is by a preponderance of the evidence,[46] rather than the clear and convincing standard that applies in litigation in district court.[47] Inter partes review can be invoked after the post-grant review period expires.[48] The basis for the challenge is more limited, covering only lack of novelty or obviousness based upon prior

37. 35 U.S.C. § 102(b) (2012); *see* Lockwood v. Am. Airlines, Inc., 107 F.3d 1565, 1570 (Fed. Cir. 1997) ("If a device was 'known or used by others' in this country before the date of invention . . . it qualifies as prior art.").

38. 35 U.S.C. § 102(a).

39. *In re* Hilmer, 359 F.2d 859, 861 (C.C.P.A. 1966).

40. 35 U.S.C. § 102(a)(2).

41. *See* 37 C.F.R. § 1.131 (2016).

42. Leahy-Smith America Invents Act, Pub. L. No. 112-29, § 8, 125 Stat. 284, 315–16 (codified at 35 U.S.C. § 122(e)).

43. 35 U.S.C. § 273(a) (2012); *see also* 35 U.S.C. § 273(b) (noting that the defendant must establish the requisite commercial use based upon clear and convincing evidence).

44. 35 U.S.C. § 321 (2012).

45. 35 U.S.C. § 321(b) (referencing 35 U.S.C. § 282(b)(2)–(b)(3) (2012)).

46. 35 U.S.C. § 326(e) (2012).

47. 35 U.S.C. § 282.

48. 35 U.S.C. § 311(c) (2012).

art consisting of patents or printed publications.[49] Here, too, the challenger bears the burden of showing unpatentability by a preponderance of the evidence.[50] Inter partes review has been surprisingly popular: as of October 2015, challengers were filing thirty petitions per week, and the Patent Trial and Appeal Board invalidated slightly more than half of challenged claims.[51] Thus, even a successful effort to patent an innovation may be undone after the fact after the implementation of the AIA.

In short, recent changes to patent doctrine reduce the availability of patents to innovators and may increase costs for those who do obtain one.

C. Absolute and Relative Secrets

It is increasingly difficult to keep secrets. Sharing information is nearly costless as Internet connectivity becomes ubiquitous, and pervasive indexing and capable search make it easy to discover that data.[52] Some information spills inadvertently, as when a personal lubricant company released over 250,000 customer names and addresses onto the Internet by mistake.[53] And some is forced into the open, as when attackers broke into the Office of Personnel Management's database to extract sensitive information about federal employees.[54] Even governments, who have the greatest capacity to impose secrecy, have struggled. Daniel Ellsberg had to photocopy the Pentagon Papers slowly over time to reveal one government report.[55] WikiLeaks,[56] Bradley Manning,[57] and Edward Snowden[58] disclosed more information, by orders of magnitude, with far greater speed and ease. Corporations struggle even more to

---

49. 35 U.S.C. § 311(b).

50. 35 U.S.C. § 316(e) (2012).

51. Matt Cutler, *3 Years of IPR: A Look at the Stats*, LAW360 (Oct. 9, 2015, 3:59 PM), http://www.law360.com/articles/699867/3-years-of-ipr-a-look-at-the-stats; *Harnessing Patent Office Litigation*, HARNESS DICKEY (2015), http://ipr-pgr.com/wp-content/uploads/2015/11/IPR-PGR-Report-Vol.-11.pdf.

52. *See* Bambauer, *supra* note 24, at 64.

53. Ryan Singel, *Security Researcher Wants Lube Maker Fined for Privacy Slip*, WIRED (July 10, 2007, 5:35 PM), http://www.wired.com/2007/07/security-resear/.

54. *See* Dustin Volz, *More Than a Million OPM Hack Victims Still Not Notified*, REUTERS (Dec. 11, 2015, 3:48 PM), http://www.reuters.com/article/us-usa-cybersecurity-opm-idUSKBN0TU2NI20151211.

55. Michael Cooper & Sam Roberts, *After 40 Years, the Complete Pentagon Papers*, N.Y. TIMES (June 7, 2011), http://www.nytimes.com/2011/06/08/us/08pentagon.html?_r=0.

56. *See* Yochai Benkler, *A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate*, 46 HARV. CIV. RTS.-CIV. LIBERTIES L. REV. 311, 315–17 (2011).

57. Adam Gabbatt, *"I Am Chelsea Manning," Says Jailed Soldier Formerly Known as Bradley*, GUARDIAN (Aug. 22, 2013, 12:35 PM), http://www.theguardian.com/world/2013/aug/22/bradley-manning-woman-chelsea-gender-reassignment (stating also that Manning's first name is now Chelsea).

58. *See* Jason M. Breslow, *How Edward Snowden Leaked "Thousands" of NSA Documents*, PBS: FRONTLINE (May 13, 2014), http://www.pbs.org/wgbh/frontline/article/how-edward-snowden-leaked-thousands-of-nsa-documents/.

maintain control over data.[59] Hackers break into a defense contractor's computers to steal information on the Joint Strike Fighter.[60] Attackers breach corporate networks in movie studios[61] and department stores[62] alike. While rigorous data are difficult if not impossible to find, both the number of breaches and their scope appears to be on the rise.[63] Firms are trying to hold back the tide—information technology is designed to reduce the costs of accessing information, not to augment them.

Secret information faces internal threats as well. Most employees carry smartphones that feature high-resolution cameras, e-mail and file transfer programs, and access to the corporate network.[64] Firms routinely defer to employees' choice regarding what devices to attach to corporate networks and what, if any, security precautions to take with those devices.[65] Personnel with access to secrets stored in digital form can store and share them readily, and information stored in analog form can be readily digitized by means of a scan or photograph. Even innocent employees can spill secrets simply by losing their device or having it compromised.[66] Analog information is similarly at risk, as when hospital employees leave a briefcase with information about patients with HIV on the subway.[67] Intellectual property (IP) attorneys have responded with a

---

59. *See, e.g.*, Kaveh Waddell, *Hospitals Aren't the Only Ones Bleeding Stolen Health Records*, ATLANTIC (Dec. 16, 2015), http://www.theatlantic.com/technology/archive/2015/12/hospitals-arent-the-only-ones-bleeding-stolen-health-records/420636/.

60. *See, e.g.*, Franz-Stefan Gady, *New Snowden Documents Reveal Chinese Behind F-35 Hack*, DIPLOMAT (Jan. 27, 2015), http://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/.

61. *See, e.g.*, Mark Seal, *An Exclusive Look Inside Sony's Hacking Saga*, VANITY FAIR (Feb. 4, 2015, 10:00 AM), http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg.

62. *See, e.g.*, Michael Riley, Benjamin Elgin, Dune Lawrence & Carol Matlack, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG (Mar. 13, 2014, 8:31 AM), http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

63. *See, e.g.*, Janet Brumfield, *Verizon 2015 Data Breach Investigations Report*, VERIZON (Apr. 13, 2015), http://news.verizonenterprise.com/2015/04/2015-data-breach-report-info/#release; Fahmida Y. Rashid, *The Most Innovative and Damaging Hacks of 2015*, INFOWORLD (Dec. 28, 2015), http://www.infoworld.com/article/3017980/security/the-most-innovative-and-damaging-hacks-of-2015.html; *2015 Second Annual Data Breach Industry Forecast*, EXPERIAN 2 (2015), https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf.

64. *See* Bone, *supra* note 26, at 274–75 n.147; Ivan. P.L. Png, Law and Innovation: Evidence from State Trade Secrets Laws 6 (June 15, 2012), http://ssrn.com/abstract=1755284 (showing that 75% of misappropriation cases involve current or former employees).

65. This phenomenon is known as "Bring Your Own Device" in the IT sector. *See* Dean Evans, *What Is BYOD and Why Is It Important?*, TECHRADAR (Oct. 7, 2015), http://www.techradar.com/us/news/computing/what-is-byod-and-why-is-it-important--1175088.

66. *See, e.g.*, Defiance Button Mach. Co. v. C & C Metal Prods. Corp., 759 F.2d 1053, 1057–58 (2d Cir. 1985).

67. Carey Goldberg, *MGH Settles for $1M After HIV Patient Records Lost on Subway*, WBUR'S COMMON HEALTH REFORM & REALITY (Feb. 24, 2011), http://commonhealth.wbur.org/2011/02/mass-general-privacy/.

panoply of warnings and advice, but they fight a rearguard action against technology and human error.[68]

The plummeting costs of information have put intellectual property regimes under significant stress. For example, copyright law operates against an implicit assumption of costly reproduction and dissemination. With the shift to digital media and high-speed networks, those activities became increasingly cheap, if not effectively costless, as exemplified by the rise of Napster and its progeny. Copyright owners turned to law as a means of artificially driving up the cost of copying and sharing. Both Congress and the courts reacted by making copyright more potent.[69] Congress passed the No Electronic Theft Act, augmenting the penalties for infringement and making criminal prosecution easier.[70] It enacted Title I of the Digital Millennium Copyright Act, threatening liability for users sophisticated enough to bypass technological protection measures employed by copyright owners.[71] The courts expanded vicarious and contributory liability to hold intermediaries responsible for infringement[72]; when firms circumvented those schemes through clever software design, the Supreme Court invented the new theory of inducement to ensnare them.[73] As technological changes caused information costs to fall, copyright law responded to take up some of the slack.

Patent law faces similar pressures. The advent of low-cost, computer-aided design drawings, and software to produce them, means that consumers increasingly have the information necessary to duplicate patented products, such as dentures[74] and aircraft parts.[75] And, the rise of relatively cheap 3-D printers provides consumers with the means to use those blueprints.[76] Patent owners have responded by attempting to have the

---

68. *See* Michael H. Bunis & Anna Dray-Siegel, *You Need to Work Harder to Fight Trade Secret Theft*, LAW360 (Aug. 7, 2013, 12:38 PM), https://www.choate.com/uploads/1178/doc/Bunis,_Dray-Siegel_-_Law360_-_You_Need_To_Work_Harder_To_Fight_Trade_Secret_Theft.pdf; Trent Livingston, *Today's Connected Employee: A License to Steal*, TRADING SECRETS (Sept. 25, 2014), http://www.tradesecretslaw.com/2014/09/articles/trade-secrets/todays-connected-employee-a-license-to-steal/.

69. JESSICA LITMAN, DIGITAL COPYRIGHT 153–54, 160–61 (2d ed. 2006).

70. No Electronic Theft (NET) Act, Pub. L. No. 105-147, § 2(b), (d), 111 Stat. 2678, 2678–79 (1997) (codified at 17 U.S.C. § 506(a)(1)(A)–(C) (2012), and 18 U.S.C. § 2319(a)–(d) (2012), respectively).

71. Digital Millennium Copyright Act, Pub. L. No. 105-304, § 103(a), 112 Stat. 2860, 2863–65 (1998) (codified at 17 U.S.C. § 1201(a) (2012)).

72. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1019–24 (9th Cir. 2001).

73. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 936–37 (2005).

74. *See* Susan Decker, *Silicon Valley Beats Hollywood in Teeth-Straightening Case*, BLOOMBERG TECH. (Nov. 10, 2015, 8:33 AM), http://www.bloomberg.com/news/articles/2015-11-10/align-loses-patent-appeal-over-copycat-dental-aligners.

75. *See* Frank Catalano, *Boeing Files Patent for 3D-Printed Aircraft Parts—and Yes, It's Already Using Them*, GEEKWIRE (Mar. 6, 2015, 11:23 AM), http://www.geekwire.com/2015/boeing-files-patent-for-3d-printing-of-aircraft-parts-and-yes-its-already-using-them/.

76. Deven R. Desai & Gerard N. Magliocca, *Patents, Meet Napster: 3D Printing and the Digitization of Things*, 102 GEO. L.J. 1691, 1691, 1693 (2014); Timothy R. Holbrook & Lucas S.

International Trade Commission and federal courts block sharing of Computer-Aided Design (CAD) plans via the Internet.[77] Similarly, the ease of moving information technology functions outside U.S. borders has given firms new possibilities for evading infringement liability, particularly for method patents. The response from courts has been mixed. The Court of Appeals for the Federal Circuit adopted a flexible test for systems claims that assesses whether the patented system has been used in the U.S., thereby triggering infringement liability.[78] The Federal Circuit's test evaluates "where control of the system is exercised and beneficial use of the system obtained."[79] This approach meant that the company Research In Motion (RIM), maker of the then-famous Blackberry messaging devices, infringed patents on electronic mail systems that incorporated wireless components.[80] Even though one part of the RIM service was located in Canada, the Federal Circuit reasoned that control and beneficial use were enjoyed in the U.S., where Blackberry users fanatically checked their messages.[81] Similarly, the Federal Circuit interpreted liability for direct infringement of method patents to find that an Internet company was an infringer, even though the company had arranged activity such that its customers performed one step of the patented method for delivering Internet content.[82] A single entity must perform all of the steps of the patented method to infringe, but the Federal Circuit broadened the scope of joint patent infringement to reduce the risk of strategic behavior, particularly in the on-line context.[83]

By contrast, the Supreme Court limited the extraterritorial reach of some aspects of patent law by holding that software code installed on computers outside U.S. borders did not count as a "component," since it was a copy of the code residing on the PCs, rather than the original compact disc itself.[84] This distinction allowed Microsoft to evade liability for infringing a patent on an apparatus for compressing and encoding speech.[85] Thus, while patent law has been attentive to the implications of reduced costs for sharing (and creating) patented inventions, it has only partially reacted to mitigate those effects.

Osborn, *Digital Patent Infringement in an Era of 3D Printing*, 48 U.C. DAVIS L. REV. 1319, 1321–22 (2015); Sapna Kumar, *Regulating Digital Trade*, 67 FLA. L. REV. 1909, 1922–23 (2015).

77. ClearCorrect Operating, LLC v. Int'l Trade Comm'n, 810 F.3d 1283, 1286–87, 1289 (Fed. Cir. 2015) (reversing International Trade Commission order that the ITC had jurisdiction to ban "electronically imported data" under 19 U.S.C. § 1337 (2012)).

78. NTP, Inc. v. Research in Motion, Ltd., 418 F.3d 1282, 1316–17 (Fed. Cir. 2005), *abrogated on other grounds by* Zoltek Corp. v. U.S., 672 F.3d 1309 (Fed. Cir. 2012), *as recognized in* IRIS Corp. v. Japan Airlines Corp., 769 F.3d 1359 (Fed. Cir. 2014).

79. *Id.* at 1317.

80. *Id.* at 1317, 1325.

81. *Id.* at 1317.

82. Akamai Techs., Inc. v. Limelight Networks, Inc., 692 F.3d 1301, 1306, 1313, 1318 (Fed. Cir. 2012) (per curiam), *rev'd* Limelight Networks, Inc. v. Akamai Techs., Inc., 134 S. Ct. 2111 (2014).

83. *See id.* at 1317–18.

84. Microsoft Corp. v. AT&T Corp., 550 U.S. 437, 449–51, 454 (2007).

85. *Id.* at 458–59.

Lastly, trademark law has had to respond to falling information costs. The rise of the commercial Internet, especially the Web, led to a wave of cybersquatting, where infringers used well-known marks in domain names, meta tags, e-mail messages, or page content to draw users to their sites.[86] Trademark holders responded with the usual array of claims sounding in the Lanham Act or state equivalents, unfair competition, or tort.[87] However, some behavior, such as registering but then warehousing infringing domain names, fell outside the boundaries of these doctrines, and some foreign defendants evaded enforcement.[88] Congress responded by passing the Anticybersquatting Consumer Protection Act (ACPA), which penalized registering and trafficking in infringing domain names, enabled plaintiffs to proceed *in rem* against domain names in the absence of *in personam* jurisdiction, and offered heavy statutory damages to drive up the cost of infringement.[89]

There are at least two additional shifts on the horizon that are likely to make it more difficult to maintain secrets. The first is technological. The much-lauded "Internet of Things" is beginning to become reality. The standard example is the refrigerator.[90] The functionality of the fridge is largely unchanged from the era of the icebox—multiple temperature zones and built-in ice and water dispensers count as major feature changes. But, many refrigerators have chips—CPUs—that determine when to run the compressor, when to defrost, and other cooling-related decisions. The humble fridge is thus catching up to other appliances, such as coffee makers, which use chips that allow users to program automatic brewing of coffee; washing machines, which use CPUs to determine wash cycle time and water temperature; and heating/air conditioning units, which employ chips to implement schedules for warming or cooling the household.[91] Increasingly, however, the refrigerator—and by extension other household appliances—will have an Internet connection as well. It will be able to schedule maintenance, report on inventory, and display your daily calendar by connecting to the Net. The networked refrigerator has two important ramifications for secrecy. First, these devices will generate new data.[92] For example, a smart fridge used in a lab might generate a

86. *See* Nicholas Foss Barbantonis, *Should Contributory Cybersquatting Be Actionable?*, 17 N.C. J.L. & TECH. 79, 83, 96 (2015).

87. *See, e.g.*, CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1020 (S.D. Ohio 1997).

88. *See* Sporty's Farm L.L.C. v. Sportsman's Mkt., Inc., 202 F.3d 489, 495–96 (2d Cir. 2000).

89. 15 U.S.C. § 1125(d) (2012).

90. And that is not the most ridiculous one. *See* Andrew Liszewski, *This Smart Rubber Duckie Makes Bathtime Even More Fun (and Safer)*, TOYLAND (Jan. 7, 2015, 2:07 PM), http://toyland.gizmodo.com/this-smart-rubber-duckie-makes-bathtime-lots-of-fun-an-1678038671.

91. *See* Richard Baguley & Colin McDonald, *Appliance Science: The Internet of Toasters (and Other Things)*, CNET (Mar. 2, 2015, 11:26 AM), http://www.cnet.com/news/appliance-science-the-internet-of-toasters-and-other-things/.

92. *See* Klint Finley, *Hacked Fridges Aren't the Internet of Things' Biggest Worry*, WIRED (Mar. 12, 2015, 8:00 AM), http://www.wired.com/2015/03/hacked-fridges-arent-internet-things-biggest-worry/.

report notifying scientists that a particular chemical stored inside it is in short supply. Previously, the scientists would have learned this information via visual inspection. Now, though, the appliance itself produces the information. Data that is more widely shared is more vulnerable to disclosure. This brings up the second point: connecting additional devices to the Internet makes them vulnerable to hacking and data breaches.[93] For example, Samsung smart refrigerators implement the Secure Sockets Layer (SSL) encryption protocol, but fail to authenticate the digital certificates used in SSL, leaving the fridges vulnerable to hackers, who successfully impersonate the certificates via a "man-in-the-middle" attack.[94] Thus, the advent of the Internet of Things means that devices generate more data, and also increase the attack surface for hackers.[95] The trend will be similar to the introduction of the Internet-connected cell phone in the workplace, which presented new cybersecurity challenges for firms.[96]

The second change is legal. Recent federal cybersecurity legislation immunizes firms, such as Internet service providers, that share information on IT threats with the federal government.[97] In theory, this new legal regime is intended to protect trade secrets (among other things) by helping private companies and the government collaborate to prevent hacking, intrusions, and other forms of threats. However, it also increases risks to secrecy. As more information is monitored, shared, and stored, some information pertinent to trade secrets will be collected and is thus at risk of disclosure.[98] The new statute imposes few requirements upon the firms that share information and immunizes them from any legal liability for doing so.[99] The federal cybersecurity program increases information dissemination, in part by protecting firms from liability when they engage in sharing.[100] As data related to trade secrets flows across the network, some is likely to be collected, deliberately or inadvertently, and then shared. The sharing entity has sub-optimal incentives to sort or

93. *See* Julie Bort, *For the First Time, Hackers Have Used a Refrigerator to Attack Businesses*, BUS. INSIDER (Jan. 16, 2014, 1:36 PM), http://www.businessinsider.com/hackers-use-a-refridgerator-to-attack-businesses-2014-1.

94. John Leyden, *Samsung Smart Fridge Leaves Gmail Logins Open to Attack*, REGISTER (Aug. 24, 2015, 9:03), http://www.theregister.co.uk/2015/08/24/smart_fridge_security_fubar/.

95. *See generally* Lorenzo Franceschi-Bicchierai, *Smart Fridge Only Capable of Displaying Buggy Future of the Internet of Things*, MOTHERBOARD (Dec. 11, 2015, 11:33 AM), http://motherboard.vice.com/read/smart-fridge-only-capable-of-displaying-buggy-future-of-the-internet-of-things ("This is the future, where your fridge has apps, and can probably be hacked.").

96. *See, e.g.*, Rebekah Mintzer, *From Smartphones with Love: Devices Aid Corporate Espionage*, CORP. COUNSEL (Apr. 29, 2014), http://www.corpcounsel.com/id=1202652989359/From-Smartphones-With-Love-Devices-Aid-Corporate-Espionage?slreturn=20160215171934.

97. The Cybersecurity Information Sharing Act of 2015 (CISA), S. 754, 114th Cong., was passed by Congress and signed into law by President Barack Obama in December 2015. Everett Rosenfeld, *The Controversial 'Surveillance' Act Obama Just Signed*, CNBC (Dec. 22, 2015, 12:34 PM), http://www.cnbc.com/2015/12/22/the-controversial-surveillance-act-obama-just-signed.html.

98. *See* Jennifer Granick, *OmniCISA Pits DHS Against the FCC and FTC on User Privacy*, JUST SECURITY (Dec. 16, 2015, 6:09 PM), https://www.justsecurity.org/28386/omnicisa-pits-government-against-self-privacy/.

99. *See* Derek E. Bambauer, *Sharing Shortcomings*, 47 LOY. U. CHI. L.J. 465, 482–84 (2015).

100. *See id.*

safeguard the information because it is relieved of liability when it discloses it.[101]

Technology has shifted to make it harder than ever to control who can access and use information. Firms face low-skilled attackers, who employ automated tools to look for vulnerabilities and misconfigurations; high-skilled ones, who can write custom exploits; and insiders, who can misuse their access to systems and information.[102] It is not possible to reverse or even meaningfully modify this change with technology alone. Rather, innovators will have to supplement code with law, turning inevitably to trade secret as their only alternative.[103]

III. IMPLICATIONS

The expanded use of trade secret that this Article predicts will cause growing pains. Trade secret prioritizes protecting an owner's legitimate expectations of confidentiality, to encourage innovation, to discourage unethical behavior, or both.[104] Enforcing rights in a trade secret, however, will at times implicate, if not override, other important values. To date, trade secret doctrine has not had to grapple much with when and how to accommodate those countervailing values. Courts tend to invoke the property label or condemn unfair business practices without any real analysis—the conclusion is treated as self-supporting.[105] But a failure to do so risks override, either by judicial decision or legislative fiat. Courts and legislators will have to grapple with whether to maximize protection for covered secrets or to accommodate countervailing interests;[106] whether to prefer experimentation or uniformity;[107] and whether to continue the expansion in criminal enforcement or to curtail it to mirror patent law.[108] This Part explores each of these challenges.

Perhaps the greatest risk to trade secret is when it clashes with free speech. Unlike trademark or copyright, trade secret contains no built-in

---

101. *See id.*

102. *See* Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1016, 1022–23 (2014); *see also* David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287 (2014).

103. *See generally* Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661 *passim* (1998) (discussing how law regulates behavior both directly and indirectly).

104. Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 481–82 (1974).

105. The cases often remind one of a line from Ring Lardner's novel *The Young Immigrunts*: "Shut up he explained." RING W. LARDNER, JR., THE YOUNG IMMIGRUNTS 778 (1920). Thanks to Toni Massaro for this reference.

106. *See* David S. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure*, 59 FLA. L. REV. 135 *passim* (2007).

107. *See* Michael Risch, *An Empirical Look at Trade Secret Law's Shift from Common to Statutory Law*, *in* INTELLECTUAL PROPERTY AND THE COMMON LAW 151, 156 (Shyamkrishna Balganesh ed., 2013).

108. *See* Robert M. Isackson & Sonia Valdez, *New Year, New Progress: The Defend Trade Secrets Act Reports Out from the Senate Judiciary Committee*, ORRICK: TRADE SECRETS WATCH (Jan. 29, 2016), http://blogs.orrick.com/trade-secrets-watch/2016/01/29/new-year-new-progress-the-defend-trade-secrets-act-reports-out-from-the-senate-judiciary-committee/#more-1749.

accommodation for First Amendment interests.[109] Scholars have criticized this myopia, but courts have rarely faced cases that present significant free speech issues.[110] An increase in trade secret protection, and hence litigation, makes such a clash inevitable, though. For example, energy companies have begun to extract natural gas through a process known as fracking.[111] Fracking requires injection of chemicals into the ground to enable withdrawal of the gas; the firms treat the components and make-up of the inoculants as trade secrets.[112] Critics have charged that the chemicals pose significant health risks. Energy companies have refused to divulge their formulas, even to legislators, by citing trade secrecy.[113] A whistleblower, who made the formula public—or a newspaper that published it—might be held liable for misappropriation, perhaps even facing an injunction against further distribution.[114] Such a remedy would immediately implicate the First Amendment, especially if the health risks proved to be real.[115] Courts have refused to block dissemination of other content obtained in violation of various laws, and it is likely that free speech interests would eventually trump here, too.[116]

The second tension is with federalism. Trade secret is a creature of state law, developing initially as a tort that policed unfair business practices.[117] The advent of the Uniform Trade Secrets Act (UTSA) in 1979 was an important shift towards greater uniformity among the states, nearly all of which have adopted it.[118] However, three states (New York, Massachusetts, and Texas) with important innovation sectors do not use the UTSA.[119] States differ from one another on which UTSA provisions they have adopted and the statutory language used to implement them.[120]

---

109. *See* Deepa Varadarajan, *Trade Secret Fair Use*, 83 FORDHAM L. REV. 1401, 1404–06, 1412 (2014).

110. *See* Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777, 777–78 (2007).

111. John M. Golden & Hannah J. Wiseman, *The Fracking Revolution: Shale Gas as a Case Study in Innovation Policy*, 64 EMORY L.J. 955, 955, 962 (2015).

112. Mary Winter, *Drilling Down on Shale Gas*, ST. LEGISLATURES, July–Aug. 2013, at 8, http://www.ncsl.org/Portals/1/Documents/magazine/articles/2013/SL_0713-Trends.pdf.

113. Hannah Wiseman, *Trade Secrets, Disclosure, and Dissent in a Fracturing Energy Revolution*, 111 COLUM. L. REV. SIDEBAR 1, 1–2 (2010).

114. *Cf.* Peter S. Menell, *Tailoring a Public Policy Exception to Trade Secret Protection*, 105 CALIF. L. REV. (forthcoming) (manuscript at 16–17) (Univ. Cal. Berkeley Pub. Law Research Paper No. 2686565, Nov. 2015), http://ssrn.com/abstract=2686565 (discussing that injunctions are routinely used to suppress the disclosure of trade secrets).

115. *See* Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147, 229–32 (1998).

116. *See* N.Y. Times Co. v. United States, 403 U.S. 713, 726–27 (1971) (Brennan, J., concurring) (per curiam) (explaining that a prior restraint suppressing the distribution of a classified study violates the First Amendment); *see also* Bartnicki v. Vopper, 532 U.S. 514, 535 (2001) (holding that disclosure of an illegally recorded conversation was protected by the First Amendment because it was about a matter of public concern).

117. *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 478–93 (1974) (discussing the evolution and policy of trade secret law).

118. *See generally* Risch, *supra* note 107.

119. Png, *supra* note 64, at 2.

120. *See generally* Risch, *supra* note 107.

Common law precedent continues to play a role in cases brought under UTSA-based statutes, and some states, such as California, have not entirely pre-empted common law trade secret.[121] All of these features generate variation among state trade secret regimes. This accords well with the concept of state regimes as useful policy experiments.[122] The federal role in trade secret law is currently limited to enforcement via criminal prosecution under certain circumstances, such as where misappropriation benefits a foreign power.[123]

That is likely to change as trade secret usage expands. The past several congressional sessions have seen the introduction of legislation to federalize trade secret.[124] Supporters tout the benefits of uniformity and predictability, particularly for firms that operate in multiple states.[125] A federal trade secret system would have drawbacks, however.[126] It would sacrifice the distributed development and evolution of doctrine that state variation produces.[127] It would increase the workload of the federal court system, particularly if jurisdiction were to be exclusively federal.[128] And, a federal statute would need to decide between pre-empting similar state claims, as with patent and copyright, or whether to operate in parallel, as with trademark.

Shifting to a federal trade secret system also heightens the clash with other legal regimes. California, for example, denies enforcement to any contractual term that limits labor mobility.[129] While it may be nominally possible to craft an agreement that protects a firm's trade secrets after an employee leaves the company, success at that task has been scarce to date.[130] A federal trade secret regime would thus have spillover effects into other areas of state-based regulation.

---

121. *Id.*

122. *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("[A] single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

123. *See* 18 U.S.C. § 1831(a) (2012).

124. *See, e.g.*, Defend Trade Secrets Act of 2015, H.R. 3326, 114th Cong., https://www.congress.gov/114/bills/hr3326/BILLS-114hr3326ih.pdf.

125. *See, e.g.*, Orrin Hatch & Chris Coons, *Pass the Defend Trade Secrets Act*, HILL (Jan. 27, 2016, 7:00 PM), http://thehill.com/opinion/op-ed/267205-pass-the-defend-trade-secrets-act.

126. *See* Christopher B. Seaman, *The Case Against Federalizing Trade Secrecy*, 101 VA. L. REV. 317, 321–22 (2015).

127. *See* Letter from Eric Goldman, Professor of Law, Santa Clara Univ. Sch. of Law et al. to Honorable Charles E. Grassley, Chairman, U.S. Senate Comm. on the Judiciary et al. 1, 7 (Nov. 17, 2015), http://cyberlaw.stanford.edu/files/blogs/2015%20Professors%20Letter%20in%20Opposition%20to%20DTSA%20FINAL.pdf.

128. *Id.* at 1, 5–6.

129. CAL. BUS. & PROF. CODE § 16600 (West 2016) ("[E]very contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void.").

130. *See* Edwards v. Arthur Andersen LLP, 189 P.3d 285, 292 (Cal. 2008) (holding that an employee's non-competition and non-solicitation agreement was invalid because it restricted the employee from practicing his profession). *But see* Richmond Techs., Inc. v. Aumtech Bus. Sols., No.

The third tension relates to enforcement. While patent law provides stronger property-like rights over an invention, trade secret's enforcement regime does have one significant advantage: criminal penalties at both the state[131] and federal[132] level. Patent law is unusual in this regard: the federal Copyright Act[133] and Lanham Act[134] (trademark) both create criminal liability in some circumstances, and some neighboring rights, such as the federal anti-bootlegging statute,[135] also impose criminal penalties. Scholars largely conclude that the lack of criminal penalties for patent infringement is not a deliberate policy decision, but rather derives from public choice issues.[136] Criminal enforcement of IP rights is attractive to at least some innovators, since it can augment deterrence through greater sanctions, and because it transfers some of the cost of vindicating intellectual property rights from the owner to the public fisc. If innovators shift to relying more on trade secret, they are likely to push prosecutors to pursue charges against infringers. And while the number of federal criminal cases involving intellectual property is quite small, state prosecutors may be more amenable to such pressures, especially where the rightsholder is a state resident and the alleged infringer is not.[137]

To date, trade secret doctrine has largely evaded clashes with other legal regimes. The increasing use of legal protections for confidential information will mean that legislators and courts must confront and resolve clashes with free speech protections, federalism concerns, and choice of enforcement models.

IV. CONCLUSION

It is difficult to prophesy, especially about the future.[138]

11-CV-02460-LHK, 2011 WL 2607158, at *15–21 (N.D. Cal. July 1, 2011) (holding (in a trial for a preliminary injunction) that a non-compete clause may be enforceable and employees may have engaged in unfair competition and breached a non-disclosure agreement).

131. *See, e.g.*, CAL. PENAL CODE § 499c (West 2016); MASS. GEN. LAWS ch. 266, § 30(4) (2016); NEV. REV. STAT. § 600A.035 (2015); TEX. PENAL CODE ANN. § 31.05 (West 2015).

132. 18 U.S.C. §§ 1831–1832 (2012).

133. 17 U.S.C. § 506 (2012).

134. 18 U.S.C. § 2320 (2012).

135. 18 U.S.C. § 2319A(a)(3) (2012).

136. Irina D. Manta, *The Puzzle of Criminal Sanctions for Intellectual Property Infringement*, 24 HARV. J.L. & TECH. 469, 505–12 (2011).

137. *See* Derek E. Bambauer, *Exposed*, 98 MINN. L. REV. 2025, 2053 n.157 (2014) (first citing U.S. DEP'T OF JUSTICE, PRO IP ACT ANN. REP. FY2012, at 31 (2012), https://www.justice.gov/sites/default/files/dag/legacy/2013/01/29/doj-pro-ip-rpt2012.pdf; and then citing U.S. DEP'T OF JUSTICE, FED. JUST. STAT., 2009, at 13 (2011), http://bjs.gov/content/pub/pdf/fjs09.pdf).

138. This quote has been variously attributed, most prominently to Niels Bohr and Yogi Berra (an unlikely pairing). It is likely a variant of a Dutch aphorism. *It's Difficult to Make Predictions, Especially About the Future*, QUOTE INVESTIGATOR (Oct. 20, 2013), http://quoteinvestigator.com/2013/10/20/no-predict/; *see also* Letters to the Editor, *The Perils of Prediction, June 2nd*, ECONOMIST (July 15, 2007, 17:59 PM), http://www.economist.com/blogs/theinbox/2007/07/the_perils_of_prediction_june.

To summarize, I argue that innovators must inevitably turn to trade secret, as patents are increasingly costly or unavailable, and other measures of maintaining more absolute secrecy are less reliable. This framework usefully generates some predictions that can be tested empirically. First, it suggests that trade secret litigation should not only increase, but that the rate of increase should go up over time.[139] Second, the ratio of trade secret suits to patent suits should increase as well, if innovators are shifting from the latter to the former as their preferred method of protection. Third, criminal prosecution of trade secret cases should increase at both the state and federal levels, both in absolute terms and relative to IP cases as a whole.[140] Fourth, firms are likely to attempt to develop new ways of measuring the value of trade secrets to address the valuation problem.[141] Finally—and perhaps most difficult to quantify—the frequency with which defendants interpose defenses unrelated to trade secret will increase. California may be an especially useful testing ground for this prediction since the state has several other legal regimes that can conflict with trade secret protection.

One challenge to evaluating claims empirically is that trade secrets are hard to detect. There is no registration process for a trade secret; it is defined only retrospectively in litigation to determine whether misappropriation has occurred.[142] Secrets are hard to value on a firm's books and difficult to measure in quantity or quality.[143] An increase in utilization of trade secrets might be detected by proxy, such as the volume of litigation, perhaps after a lag time. But, by definition, these advances are secrets and not amenable to measurement. The existence and scale of any shift will be challenging to determine, and will likely need to use secondary or partial measures, such as proxies or surveys, rather than direct observation.

Litigation is one such secondary measure, and this Article predicts that trade secret litigation will increase; that the rate of increase will also go up; and that it will increase relative to patent litigation.[144] An increase in litigation assumes that actual or threatened misappropriation is either independent of the volume of trade secrets or varies directly with it. Thus, more trade secrets generates more misappropriation, particularly given that self-help becomes less effective with technological shifts that

139. *See* David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 301 (2010); *see also* David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZ. L. REV. 57, 61 (2011); Png, *supra* note 64, at 3.

140. This is concededly difficult to measure. *See* Josh Lerner, Using Litigation to Understand Trade Secrets: A Preliminary Exploration 8 (Aug. 2006), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=922520.

141. *See* Bambauer & Sepe, *supra* note 3, at 29–30.

142. *See* Chagai Vinizky, *Trade Secrets Registry*, 35 PACE L. REV. 455, 457 (2014) (proposing registration for trade secrets).

143. *See* Bambauer & Sepe, *supra* note 3, at 5.

144. *See* Lerner, *supra* note 140, at 11–12.

drive the cost of distributing information down. Those shifts also explain the change in the rate of increase—firms will need to employ litigation to protect secrets more often than in the past because their own precautions become less effective.

Lawsuits are not always successful even when claims are meritorious, leading to suboptimal deterrence. Misappropriators know there is at least some chance that they will escape detection or, if caught, will avoid liability.[145] Trade secret owners are thus likely to lobby both for criminal penalties for misappropriation and for prosecutors to bring charges against alleged infringers. Law enforcement resources are relatively static. If reliance on trade secrecy does increase, prosecutions will likely remain mostly constant in the short run, which means that criminal enforcement would decrease relative to the level of misappropriation. Trade secret owners will respond by pressing for more resources to be devoted to the problem, in an absolute sense and as a share of a prosecutor's time and budget. This prediction mirrors what has happened in other areas of IP, where rightsholders have pressed successfully for more resources to battle infringement. For example, the PRO IP Act of 2008 created dedicated federal positions in the executive branch and in embassies to combat violations of IP rights.[146] Politically, it is likely palatable to go after misappropriation, given the roots of trade secrecy in policing unethical commercial behavior.[147] Prosecutions for trade secrets offenses are likely to rise over time.

As innovators shift to trade secret, they face the risk that outsiders, such as shareholders, will be unable to value correctly their advances.[148] Indeed, underpricing is likely to occur. Because claims of having a secret invention are cheap talk, markets will rationally discount those claims, and innovators will be unable to realize fully the value of their secret advances. Firms are likely to try to overcome Arrow's paradox to realize the full value of their innovation.[149] There are a number of standard valuation models, but all rely on access to information—precisely the problem with a secret.[150] The most likely answer is to use a third-party certifi-

145. *See* A. Mitchell Polinsky & Steven Shavell, *Punitive Damages: An Economic Analysis*, 111 HARV. L. REV. 869, 887–95 (1998).

146. Prioritizing Resources and Organization for Intellectual Property Act of 2008, Pub. L. No. 110-403, § 301, 122 Stat. 4256, 4264–66 (codified as amended at 15 U.S.C. § 8111 (2012)).

147. Changes to patent enforcement are somewhat cabined politically because firms can reasonably predict that they may be an infringer as well as a rightsholder, particularly given the uncertain definition of a patent's claims or boundaries before trial. By contrast, firms are likely to believe (even if inaccurately) that they will not engage in unethical behavior such as espionage or inducing employees to breach agreements. *See generally* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 485–87 (1974) (discussing the steps companies and individuals will take to protect against breaches of confidence and "industrial espionage").

148. Bambauer & Sepe, *supra* note 3, at 29–32.

149. Arrow, *supra* note 21, at 623–25.

150. *See, e.g.*, Gavin C. Reid, Nicola Searle & Saurabh Vishnubhakat, *What's It Worth to Keep a Secret?*, 13 DUKE L. & TECH. REV. 116, 137–40 (2015); Robert P. Schweihs, *The Value of a Trade*

er, where the certifier is under a duty of confidentiality to the trade secret owner, but is sufficiently trustworthy that its estimate of the secret's value will be credible.[151]

Unfortunately, the history of third-party certifiers is mixed at best. Certifiers must constantly balance credibility, which protects their reputation and makes their signals valuable, against appealing to clients, who want the highest possible rating for their secrets. There can be adverse selection, as with services that rate the privacy protections provided by Web sites.[152] Firms can set up their own certifiers, a practice known informally as "greenwashing."[153] Companies may be selective about the information they disclose to certifiers. And, the time lag between the certifier's estimate and the eventual revelation of the secret's value (as embodied in products and services) may make it hard to gauge how accurate those calculations were. One can expect firms to try to gain credit in the marketplace for their secret innovations, but it will be challenging to do so.

* * *

This Article's claim about the coming rise of trade secrecy is a descriptive one, not a normative one. Trade secret is generally viewed with skepticism by legal scholars, who tend to prefer the disclosure-based regime of patents.[154] Ultimately, whether the shift towards trade secret is desirable depends upon a complex and likely unknowable empirical calculus. If trade secrecy enables innovators to capture more of the returns from inventions, since secrets can have indefinite duration, the change is likely to increase incentives to engage in this type of research and development.[155] And, depending upon whether one prefers coordinated versus distributed investigation of an advance's prospects, trade secret could increase or decrease development of an invention.[156] Finally, secrecy prevents others in the field from learning about innovation, which may

---

Secret, INSIGHTS, Autumn 2009, at 48, 51–53, http://www.willamette.com/insights_journal/09/autumn_2009_5.pdf.

151. The use of trusted third parties to overcome information asymmetry problems, and specifically Arrow's paradox, has occurred in a number of situations, including when motion picture and television producers receive unsolicited scripts. *See* Catherine L. Fisk, *The Role of Private Intellectual Property Rights in Markets for Labor and Ideas: Screen Credit and the Writers Guild of America, 1938-2000*, 32 BERKELEY J. EMP. & LAB. L. 215, 249–50, 261–664 (2011). I have proposed such a method for managing markets for software vulnerability disclosures. *See* Derek E. Bambauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1100–03 (2011).

152. *See* Benjamin Edelman, *Adverse Selection in Online "Trust" Certifications and Search Results*, ELECTRONIC COM. RES. & APPLICATIONS *passim* (2010), http://www.benedelman.org/publications/advsel-trust-se.pdf.

153. *See* Derek E. Bambauer, *Cybersieves*, 59 DUKE L.J. 377, 440–41 (2009).

154. *See, e.g.*, Bone, *supra* note 26, at 282–84, 292–93.

155. *See* Andrew A. Schwartz, *The Corporate Preference for Trade Secret*, 74 OHIO ST. L.J. 623, 637–38 (2013); *see also* Png, *supra* note 64, at 1.

156. *See* Edmund W. Kitch, *The Nature and Function of the Patent System*, 20 J.L. & ECON. 265, 288 (1977).

decrease research and development by others.[157] The net effect on innovation is unclear, but the coming rise of trade secrets could provide a valuable, quasi-natural experiment to evaluate the merits of secrecy versus disclosure.

157. This assumes that patents function to disseminate information, an assumption challenged by Mark Lemley and other scholars. Some firms instruct researchers not to read patents, for fear of increased damages if the companies are later found to infringe those patents. Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 333 n.89 (2008). Moreover, patents often do not reveal key information related to commercializing an invention, as opposed to simply practicing it. *See also* Michael J. Burstein, *Exchanging Information Without Intellectual Property*, 91 TEX. L. REV. 227, 247–54 (2012).