ARTICLES

TRADE SECRECY'S INFORMATION PARADOX

Christopher Buccafusco, Jonathan S. Masur** & Deepa Varadarajan****

Trade secret law is meant to encourage socially beneficial behaviors by permitting firms to protect their investments in the creation of valuable information. In theory, the ability to protect valuable information will make firms more likely to create that information in the first instance. But the law can also be used to shield socially harmful behaviors from public oversight. Firms can assert trade secret protection to prevent journalists, watchdogs, and criminal defendants from learning whether they are engaged in dangerous, wrongful, or biased activity. Ideally, trade secret law should sort socially beneficial uses from socially harmful ones, permitting only the former while screening out the latter. However, the problem for trade secret law is that, in a variety of contexts, it is incredibly difficult to know whether the underlying information is beneficial or harmful to society, and thus whether the information should be disclosed, without first disclosing and scrutinizing it. This is trade secrecy's information paradox: it is hard to know whether a trade secret should be protected without first revealing it. This information paradox implicates numerous social interests, including the environment, public health, criminal law, and the success of the regulatory state. It is at the heart of recent concerns about potentially biased bail and sentencing algorithms, environmentally harmful fracking chemicals, and disparate hiring practices. Yet as is the case with many paradoxes, trade secrecy's information paradox cannot easily be solved, at least with any politically feasible set of tools. Unlike other areas of intellectual property, traditional tools (i.e., doctrinal and costly screens) will do little to sort socially

* Duke Law School. We are incredibly indebted to Mikayla Brody and Jessa Goldman for their thoughtful and diligent research assistance. For helpful comments and advice, we thank Stefan Bechtold, Michael Burstein, Charles Tait Graves, Camilla Hrdy, Sonia Katyal, Mark Lemley, Christopher Morten, Arti Rai, Michael Risch, Rebecca Wexler, Felix Wu, and participants at the Intellectual Property Scholars Conference, and the Trade Secret Scholars Workshop.

** University of Chicago Law School. Masur thanks the David & Celia Hilliard Fund and the Wachtell, Lipton, Rosen & Katz Program in Behavioral Law, Finance & Economics for support.

*** Georgia State University College of Law.

harmful trade secrets from socially beneficial ones—leaving piecemeal, contextualized limits on trade secrecy the most viable path forward, at least for the foreseeable future.

INTRODUCTION

Trade secrets are having a moment. As innovation and creativity increasingly arise through algorithms and artificial intelligence, trade secrets have become an essential form of intellectual property. They are no longer "the other IP right"[1]—a mere afterthought to patents, copyrights, and trademarks.[2] Instead, they are a central part of firms' intellectual property strategy.[3] Trade secret law serves an important purpose: encouraging firms to invest in a wide range of innovative activity that society might otherwise go without. But just as trade secrets have finally found a starring role, numerous scholars have begun pointing out trade secrecy's dark side. Firms use trade secrecy to hide a wide array of potentially harmful and discriminatory behaviors from meaningful scrutiny to the detriment of public health, the environment, the criminal legal system, and democratic oversight.[4]

So which argument is correct? Are trade secrets socially beneficial or socially harmful? Both are true. But, we argue, that is precisely the problem with trade secret law. It is simultaneously responsible for incentivizing socially beneficial behaviors while also shielding socially harmful ones. Unfortunately, there is no easy way for the law to figure out which is which at the time a trade secret is asserted. This is trade

---

1 *See* James Pooley, *Trade Secrets: The Other IP Right*, WIPO MAG., June 2013, at 2.

2 *See, e.g.*, Camilla A. Hrdy & Mark A. Lemley, *Abandoning Trade Secrets*, 73 STAN. L. REV. 1 (2021); Camilla A. Hrdy & Christopher B. Seaman, *Beyond Trade Secrecy: Confidentiality Agreements that Act like Noncompetes*, 133 YALE L.J. 669 (2024).

3 *See, e.g.*, JOHN E. JANKOWSKI, NAT'L CTR. FOR SCI. & ENG'G STAT., BUSINESS USE OF INTELLECTUAL PROPERTY PROTECTION DOCUMENTED IN NSF SURVEY 4 (2012) (reporting survey results finding that "a diverse group of industries reported trade secrets as very or somewhat important to their businesses" more so than they did any other form of intellectual property).

4 *See, e.g.*, Jamillah Bowman Williams, *Diversity as a Trade Secret*, 107 GEO. L.J. 1685, 1690–99 (2019); Amy Kapczynski, *The Public History of Trade Secrets*, 55 U.C. DAVIS L. REV. 1367, 1420–28, 1434–36 (2022); Charles Tait Graves & Sonia K. Katyal, *From Trade Secrecy to Seclusion*, 109 GEO. L.J. 1337, 1350–53, 1368–70, 1385–86 (2021); Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265, 1272 (2020); Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV. 1183, 1187–90 (2019); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1395–1402 (2018); Annemarie Bridy, *Trade Secret Prices and High-Tech Devices: How Medical Device Manufacturers Are Seeking to Sustain Profits by Propertizing Prices*, 17 TEX. INTELL. PROP. L.J. 187, 187–89 (2009); Robin Feldman & Charles Tait Graves, *Naked Price and Pharmaceutical Trade Secret Overreach*, 22 YALE J.L. & TECH. 61, 84 (2020); David S. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure*, 59 FLA. L. REV. 135, 177–87 (2007); Christopher J. Morten & Amy Kapczynski, *The Big Data Regulator, Rebooted: Why and How the FDA Can and Should Disclose Confidential Data on Prescription Drugs and Vaccines*, 109 CALIF. L. REV. 493, 522–25 (2021); Christopher J. Morten, *Publicizing Corporate Secrets*, 171 U. PA. L. REV. 1319, 1327 (2023); Joseph P. Fishman & Deepa Varadarajan, *Earning Trade Secrets*, 109 CORNELL L. REV. 1381, 1385–86 (2024).

secrecy's information paradox. In a number of contexts, to know whether the secret information is socially beneficial or harmful, it must be more broadly disclosed and assessed.[5] But once that happens, there is no secret left to keep.

Consider the following scenario: A music streaming service contemplates developing an algorithm to help predict consumers' preferences. The algorithm matches songs with listeners' moods and will enable the firm to do a better job of playing the songs that customers want to hear. Developing such an algorithm may require significant investment to the tune of millions of dollars, from hiring and training programmers to testing and refining the algorithm. If the algorithm is a success, customers will hear more of the music they like, and the firm will benefit financially. Yet if the firm wants to recoup its investment, it must protect its algorithm from being copied—say, by an unscrupulous employee who takes the information to a competing firm.

For a variety of reasons, patent and copyright law are unlikely to protect this algorithm.[6] But if the firm can't protect its innovation, this firm—and others like it—may not have sufficient incentives to develop information of this type in the first place.[7] This is precisely the function trade secret law is meant to fulfill. So long as the music streaming service can keep its valuable algorithm secret, trade secret law provides it some measure of anticopying protection. Trade secrecy thus provides incentives for the development of information that might not otherwise exist. It helps fill a hole left by patent and copyright law that,

---

5 *See infra* Section II.B.

6 *See* Michael Risch, *From Patents to Trade Secrets*, *in* RESEARCH HANDBOOK ON EMPIRICAL STUDIES IN INTELLECTUAL PROPERTY LAW 101, 101–08 (Estelle Derclaye ed., 2023). While copyright law can protect source code, it will not protect the functional aspects of computer software, especially when those aspects are more inventive than expressive. *Id.* at 105. By contrast, software developers have historically been able to use either patents or trade secrets to protect their algorithms. *Id.* at 102. Today, however, patenting software is much more difficult due to the Court's ban on patenting abstract ideas. *Id.* at 106–08. Accordingly, scholars have noted that trade secrets law is the only form of intellectual property that will "reliably protect" algorithms. *Id.* at 102.

7 *See, e.g.*, Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 313–14 (2008); Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 485 (1974) ("Trade 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."); David D. Friedman, William M. Landes & Richard A. Posner, *Some Economics of Trade Secret Law*, J. ECON. PERSPS., Winter 1991, 61, 64 (arguing that trade secrecy is "congruent with the basic economic explanation for patent protection—that it provides a means of internalizing the benefits of innovation").

if left unfilled, would lead to underinvestment in socially productive knowledge.[8]

But now consider this: What if the music-matching algorithm has some unforeseen—or even intended—harmful consequences? Perhaps the firm designed the algorithm to help it pay less in royalties to musicians or to discriminate against independent artists, racial and gender minorities, or competitors.[9] This algorithm could allow the firm to secretly violate a host of state and federal antidiscrimination, trade, and competition laws. In this scenario, the incentive benefits of secrecy are dwarfed by its social costs.[10] But the principal way to discover these harms is through wider disclosure of the algorithm itself—beyond the confidential sharing of information with employees and business collaborators that trade secret law permits. That disclosure could come from a disaffected former employee who wants to share the information with an investigative journalist, or it could arise from an array of advocacy groups clamoring for it in the form of lawsuits and FOIA requests.[11] If the algorithm is protected by trade secret law, however, the public may never learn the truth.[12]

What should judges and agency decisionmakers do when faced with this secrecy-versus-disclosure calculus? If disclosure indeed turns up evidence of bias, then disclosure is important and beneficial to society.[13] It would allow the public to take action against the streaming service, perhaps shaming it into changing its practices or triggering penalties and additional regulatory oversight. But if the information shows no evidence of bias, then disclosing it could ultimately be harmful to society.[14] The streaming service would suffer competitively. But even if one does not care about the profits of any individual firm,

8 *See* Rochelle Cooper Dreyfuss & Orly Lobel, *Economic Espionage as Reality or Rhetoric: Equating Trade Secrecy with National Security*, 20 LEWIS & CLARK L. REV. 419, 424–25 (2016) ("[T]rade secret protection can . . . act as a substitute for patents." *Id.* at 425.).

9 For discussion of concerns that Spotify's algorithms do this, see Christopher Buccafusco & Kristelia García, *Pay-to-Playlist: The Commerce of Music Streaming*, 12 U.C. IRVINE L. REV. 805 (2022).

10 *See infra* Section II.A.

11 Although FOIA doesn't apply to private companies like our hypothetical streaming service, we might imagine that details of the algorithm are held by a regulatory agency and, thus, subject to FOIA. *See* 5 U.S.C. § 552(a) (2018). As we discuss below, we are especially concerned about situations in which the government may "have" the secret information but be unable to devote the resources necessary to evaluating it. *See infra* Section I.B.

12 *See infra* Section I.B. Some of the limits on disclosure that we discuss are not principally matters of trade secret law but instead arise out of a related area of law exempting trade secrets and confidential commercial information from agency disclosure through FOIA requests. We discuss these separately below but lump them together now for ease of discussion.

13 *See infra* Section II.A.

14 *See infra* Section II.A.

society would be harmed if this firm and others like it stopped investing in the creation of such innovations.

Some version of this dilemma arises in a wide variety of contexts. It arises when a judge considers a defendant's request to disclose an algorithm used in criminal sentencing.[15] It arises when an environmental agency considers a journalist's request to disclose chemicals used in hydraulic fracturing.[16] It arises when the Food & Drug Administration (FDA) considers releasing clinical trial data associated with a newly approved drug.[17] And it arises when the Federal Aviation Administration (FAA) considers a watchdog group's demand for flight control system information submitted by Boeing to secure recertification of its grounded 737 MAX passenger jets.[18]

In theory, this is a problem that trade secret law should be able to solve. Ideally, the law would perform a sorting function among potential trade secrets: separating those that will enhance social welfare from those that will diminish it, protecting only the former.[19] Of course, gauging social welfare effects directly is difficult, so other areas of intellectual property law do this sorting through proxies or "doctrinal screens." For instance, an applicant can obtain a patent only on inventions that are novel.[20] Awarding patents to novel inventions will tend to increase social welfare, while awarding patents to inventions that merely mirror existing technologies will likely diminish it.[21]

But what proxy or doctrinal screen will separate the "good" version of the kinds of information described above (e.g., algorithms, fracking fluid composition, clinical trial data, flight control system information) from the "bad"? While trade secret law does not impose a novelty requirement akin to patent law, it has doctrinal screens of its own. Trade secret law requires that the information at issue be

15 *See, e.g.*, Wexler, *supra* note 4, at 1346.

16 *See, e.g.*, Graves & Katyal, *supra* note 4, at 1358.

17 *See, e.g.*, Morten & Kapczynski, *supra* note 4, at 495–96.

18 *See* Flyers Rts. Educ. Fund, Inc. v. FAA, 71 F.4th 1051, 1053 (D.C. Cir. 2023) ("In this Freedom of Information Act suit, Flyers Rights Education Fund . . . seek[s] documents that the FAA relied upon during the recertification process."). Indeed, Boeing has continued to come under scrutiny for malfunctions associated with its 737 MAX passenger jets. *See, e.g.*, Mark Walker, *F.A.A. Chief Pledges 'More Boots on the Ground' to Monitor Boeing*, N.Y. TIMES (Feb. 6, 2024), https://www.nytimes.com/2024/02/06/us/politics/faa-boeing-737-max-9.html [https://perma.cc/Z7Z7-RL9L].

19 *See infra* Section II.A.

20 *See* 35 U.S.C. § 102(a) (2018) ("A person shall be entitled to a patent unless—(1) the claimed invention was patented, described in a printed publication, or in public use, on sale, or otherwise available to the public before the effective filing date of the claimed invention; or (2) the claimed invention was described in a patent . . . or in an application for patent . . . and was effectively filed before the effective filing date of the claimed invention.").

21 *See infra* Section II.A.

sufficiently secret, that it be subject to reasonable secrecy efforts, and that the claimant derive economic value from that secrecy.[22] But unlike patent law's novelty requirement, none of those doctrinal screens are equipped to sort socially valuable trade secrets from socially harmful ones.[23] They tell us only that a firm privately values that information enough to keep it secret.

At bottom, the only thing that distinguishes a good or socially valuable trade secret from a bad or socially harmful one is the fact of the matter. Is the algorithm biased or not? Does the drug data reveal safety concerns, or does it not? Do the chemicals in fracking fluid pose undue risks to public health, or do they not? Yet how can a court or agency answer such questions other than by performing the analysis that the journalist, researcher, or watchdog group seeking discovery of the information itself wants to perform? While limited disclosure of information (e.g., to a judge or regulatory agency) is not incompatible with trade secret protection, wider dissemination of information is. And in many situations, the evaluating judge or agency will not have the resources to perform such a rigorous analysis at the time they are deciding whether to recognize a claimant's assertion of trade secrecy.[24]

Doctrinal screens are not the only way to limit rights to socially valuable contexts. Alternatively, the law sometimes imposes a tax upon socially harmful behavior, seeking to deter it through economic costs.[25] This is known as a "costly screen."[26] The problem is that a costly screen is only effective if it has asymmetric effects on good and bad behavior. Only then will it screen out more bad conduct than good. A firm will engage in the relevant behavior or try to acquire a legal right only if it values that behavior or right more than the cost of the screen. To use patent law as an example again, the high cost of obtaining a patent

22 *See* UNIF. TRADE SECRETS ACT § 1(4) (UNIF. L. COMM'N 1985) (defining "[t]rade secret" to "mean[] information . . . 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").

23 *See infra* Part II.

24 *See infra* Section II.B.

25 *See infra* Part III.

26 *See* Jonathan S. Masur, *Costly Screens and Patent Examination*, 2 J. LEGAL ANALYSIS 687, 687 (2010); *see also* David Fagundes & Jonathan S. Masur, *Costly Intellectual Property*, 65 VAND. L. REV. 677 (2012); Christopher Buccafusco, Mark A. Lemley & Jonathan S. Masur, *Intelligent Design*, 68 DUKE L.J. 75, 87–88 (2018); Christopher Buccafusco, Jonathan S. Masur & Mark P. McKenna, *Competition and Congestion in Trademark Law*, 102 TEX. L. REV. 437, 466–68 (2024).

deters some inventors from seeking patent protection, often in circumstances when doing so would harm social welfare.[27]

Similarly, we could imagine imposing a costly screen on trade secrets: if a firm wished to protect a trade secret, it would be forced to pay some type of tax.[28] But from a firm's perspective, it is just as valuable to keep data secret if it contains evidence of wrongdoing as if it does not—perhaps even more so. A costly screen is thus unlikely to deter firms' efforts to keep malign data secret any more than their salutary efforts to keep benign data secret. Another option is to apply a costly screen only to socially harmful activities. But this just returns to the prior problem: we cannot know whether a firm's data reveals social harm without some party first analyzing it. A court or agency regulator often will not have adequate resources to do this effectively. And thus, broader disclosure—to the groups seeking it or the public—would be necessary for this assessment. That is, we could not know whether to apply the costly screen to a trade secret without first revealing the trade secret.

This is trade secret law's "information paradox." We use this phrase to invoke Kenneth Arrow's famous Information Paradox.[29] In Arrow's paradox, Firm A has a piece of information it wishes to sell to Firm B. But Firm B cannot know how much it should pay for the information until it learns of the information—at which point, it has no need to pay. It already knows the information. Intellectual property rights—including patents, copyrights, and even trade secrets—are a well-known solution to Arrow's Information Paradox.[30] But trade secret law contains its own nested information paradox. In many cases, determining whether a piece of information should be protected by trade secret law—that is, whether protecting it will be socially valuable as opposed to socially harmful—first requires exposing that piece of information to scrutiny. As we explain below, given the vast amount of information claimed under laws that protect trade secrets and confidential information, we highly doubt that courts and government regulators have the resources to engage in the extremely costly screening necessary to sort good secrets from bad. When they don't, those secrets must be exposed to others—journalists, watchdogs, and scholars. But such exposure threatens a firm's ability to protect the information

27 *See* Masur, *supra* note 26, at 687.

28 *See infra* Section III.B.

29 *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, 615 (1962); Michael J. Burstein, *Exchanging Information Without Intellectual Property*, 91 TEX. L. REV. 227, 229 n.4 (2012).

30 *See* Burstein, *supra* note 29, at 258.

as a trade secret. This is a fundamental problem with trade secret law, and it is one that cannot be easily overcome.

Our Article proceeds in four Parts. In Part I, we describe the manner in which trade secret law operates and the policies it is meant to serve. We draw particular attention to "antisocial" trade secrets: information that is nominally protected by trade secret law, but where trade secret protection can cause substantial social harm. In Part II, we analyze the possibility of using legal doctrine (doctrinal screens) to sort negative social value trade secrets from positive social value trade secrets. We demonstrate the fundamental difficulties of doing so, given the legal tools available. Unlike in other areas of law, current trade secrecy rules are equipped only to gauge the private value of information, not its social value. Part III turns to costly screens. We explain why costly screens, which can be quite useful in other areas of intellectual property law, will be largely ineffectual at screening positive and negative trade secrets. Part IV canvasses potential solutions. Trade secret law's information paradox is not theoretically insuperable, just as Arrow's Information Paradox is not theoretically insuperable. But solving it—across the full range of possible subject matter and in the wide variety of contexts in which antisocial trade secrets can arise—would likely require a far greater investment of resources than is politically feasible.

We realize that law review articles are typically presented as "comedies" rather than "tragedies." That is, the standard practice is to point out a pressing problem and propose a solution that neatly resolves it—or tries to, anyway. Ours does not readily fit this mold. The modern landscape of trade secrecy presents problems that are too fundamental to be solved with traditional legal tools—the kinds of doctrinal and costly screens that have worked reasonably well in other areas of intellectual property. But we hope that by illuminating the problem more fully, we might spur additional attention and political will to improve it. To that end, we conclude by highlighting the works of scholars urging more contextualized, subject matter–specific limits on trade secrecy; for the moment, they likely offer the most promising path forward. Ultimately, while piecemeal solutions can help chip away at some aspects of trade secrecy's information paradox, a comprehensive approach to solving it remains elusive.

I. GOOD AND BAD SECRETS

Courts and scholars have disagreed about the justifications for trade secret law, with one scholar going so far as to suggest it has

none.[31] But there is increasing, widespread support for the view that trade secrecy is best conceived as a form of intellectual property law.[32] That is, like patent and copyright, trade secret law grants certain rights to encourage investment in particular kinds of informational goods that otherwise would be underproduced.[33] Yet, as is true of other intellectual property laws, trade secrecy also comes with costs. Some of those costs are the inherent tradeoffs of incentives—by benefiting one party, the law necessarily harms another. Trade secret law, however, produces another, distinctive set of social costs. An emerging body of scholarship has explored how firms claim trade secrets in ways that harm the public.[34] These costs are not the typical tradeoffs between incentives and access, but rather distinct harms to the environment, public health, criminal justice, regulation, and democratic accountability that arise from secrecy.[35] Here, we elaborate on trade secrecy's benefits, and then we review its potential to cause harm.

A. The Case for Trade Secrets

Consider, now, a different algorithm—one that a ridesharing firm plans to develop to help riders better connect with drivers. Researching and developing this algorithm will be costly, with millions of dollars and thousands of hours spent to create and refine it. If the algorithm is successful, its benefits can redound to both the firm and its customers. Riders will be more quickly matched with drivers, and they will be willing to pay the ridesharing firm more money to use its service. The trouble for the firm is that the algorithm is just information, and information can cheaply and easily be copied. An employee could simply download the algorithm onto a personal account and depart for a competitor firm.

This example illustrates the public goods problem of information—it's expensive to create, but cheap to copy.[36] When creators face this sort of public goods problem, they will tend to underinvest in innovation, because they anticipate that competitors will copy their

31 *See, e.g.*, Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241, 245–46 (1998) [hereinafter Bone, *A New Look*]; Robert G. Bone, *The (Still) Shaky Foundations of Trade Secret Law*, 92 TEX. L. REV. 1803, 1804 (2014) [hereinafter Bone, *The (Still) Shaky*].

32 *See supra* note 7 and accompanying text.

33 *See supra* note 7 and accompanying text.

34 *See supra* note 4.

35 *See, e.g.*, Williams, *supra* note 4, at 1690; Kapczynski, *supra* note 4, at 1424–26; Graves & Katyal, *supra* note 4, at 1351–52.

36 *See* Lemley, *supra* note 7, at 329–30.

efforts and eliminate their opportunities to recoup their investments.[37] This is where IP law steps in. If the information in this case had been a movie instead of an algorithm, the firm would have been able to obtain a copyright that would prevent others from copying it.[38] Or if the information had been a new pharmaceutical drug, the firm would have been able to patent its invention—again, preventing others from copying it.[39] The copyright or the patent would give the firm an exclusive right to the information, thereby allowing it to charge higher prices for access to the information and enabling it to recoup its investment in research and development.[40]

The algorithm, however, is not eligible for either a copyright or a patent. Copyright doesn't cover ideas, methods, or processes.[41] And patent law protects only "inventions," which typically must have tangible effects—not algorithms or pure information alone.[42] This is where trade secret law has an important role to play. If the firm complies with trade secret law's doctrinal requirements, it can prevent some people—like its employees—from copying the information (or disclosing it to others).[43] This anticopying protection provides the firm with some measure of confidence to make the investment in R & D that it wouldn't otherwise make.[44]

Trade secret law, then, can be understood as filling a hole left by patent and copyright law that, if unfilled, would lead to underinvestment in socially productive knowledge.[45] Algorithms are just one example of the kinds of knowledge that don't have homes in other IP regimes. But others abound.[46] A great deal of scientific and technical knowledge can be enormously valuable whether or not it becomes eligible for a patent.[47] The early steps in drug discovery or learning that certain approaches to a problem won't work are such examples of

37 *See id.*; Deepa Varadarajan, *Trade Secret Fair Use*, 83 FORDHAM L. REV. 1401, 1405 (2014).

38 *See* 17 U.S.C. § 102(a)(6) (2018).

39 *See* 35 U.S.C. § 101 (2018).

40 *See* 17 U.S.C. § 106; 35 U.S.C. § 154 (2018); Lemley, *supra* note 7, at 329.

41 17 U.S.C. § 102(b).

42 *See* 35 U.S.C. § 101; *see also* Alice Corp. v. CLS Bank Int'l, 573 U.S. 208, 217–18 (2014).

43 *See* Williams, *supra* note 4, at 1700–01.

44 *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 485 (1974) ("Trade 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.").

45 *See id.*; *see also* Lemley, *supra* note 7, at 329–31.

46 *See* Lemley, *supra* note 7, at 335.

47 *See* Feldman & Graves, *supra* note 4, at 64–65; Morten & Kapczynski, *supra* note 4, at 509–10.

valuable information that are otherwise unprotected by patent law.[48] In addition, much business-related data is also not copyrightable or patentable, including data that a firm generates about its customers and employees.[49] As Mark Lemley has observed, granting trade secret protection to these categories of otherwise unprotectable knowledge prevents firms from taking costly self-help measures to keep information secret, and it enables firms to share information with others (e.g., employees and business partners) in ways that can be socially beneficial.[50]

While trade secret law helps promote these goals, preventing the free diffusion of knowledge also imposes social costs. Like other IP rights, trade secret law enacts a tradeoff between the incentives it creates for information's developers and the costs it imposes on others.[51] The increased prices of patented or copyrighted creations amount to a shadow tax that purchasers pay on innovation.[52] This means some efficient uses of those creations won't take place.[53] Similarly, the competitors of firms with patented or copyrighted goods will be limited in their ability to offer related products during the lifetime of the IP rights, as they will have to design around those rights or negotiate permission to use them.[54] Trade secret law creates a similar tradeoff. Trade secrecy prevents competitors from accessing information that would be useful to them and would allow them to offer better products and services to consumers.[55] The higher cost of access to trade secret information is the price society pays for the law's contribution to innovation.[56] These are inherent costs of using exclusive rights to incentivize innovation.

---

48 *See* Benjamin N. Roin, *Unpatentable Drugs and the Standards of Patentability*, 87 TEX. L. REV. 503, 504–05 (2009); Lemley, *supra* note 7, at 335.

49 *See* Lemley, *supra* note 7, at 331.

50 *See id.* at 333–35; *see also Kewanee Oil Co.*, 416 U.S. at 485–86. In addition to these utilitarian rationales for trade secret law, some courts and commentators have emphasized a "commercial morality" and the deterrence of wrongful acts as rationales behind trade secrecy protection. *See id.*; *see also* E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1015 (5th Cir. 1970) (emphasizing trade secrecy's aim "to recognize and enforce higher standards of commercial morality in the business world" (quoting Hyde Corp. v. Huffines, 314 S.W.2d 763, 773 (Tex. 1958))).

51 *Cf.* Glynn S. Lunney, Jr., *Reexamining Copyright's Incentives-Access Paradigm*, 49 VAND. L. REV. 483, 487–88 (1996) (discussing the incentive-cost tradeoff in copyright law).

52 *See* Daniel J. Hemel & Lisa Larrimore Ouellette, *Beyond the Patents-Prizes Debate*, 92 TEX. L. REV. 303, 312 (2013).

53 *See id.* at 314.

54 *See* Christopher Buccafusco, Stefan Bechtold & Christopher Jon Sprigman, *The Nature of Sequential Innovation*, 59 WM. & MARY L. REV. 1 (2017) (discussing designing around IP rights).

55 Lemley, *supra* note 7, at 329–30.

56 *See id.*; Levine, *supra* note 4, at 151–52, 157.

Trade secrecy has another inherent cost that patent and copyright don't share. All patents are published, as are most, but not all, valuable copyrights.[57] From an early stage, others can learn from and build upon patented and copyrighted information, as long as they don't violate exclusive rights. For example, once a patent reveals one means of accomplishing a task, other inventors may learn from it and be better able to develop other ways of doing so that don't infringe the patent.[58] Once one author reveals the massive consumer demand for wizard stories or vaguely medieval sagas, other creators can offer similar content that doesn't infringe the copyright.[59] But when information is held secretly rather than shared publicly, fewer people can learn from and build upon it.[60]

And so—as is true of other areas of intellectual property—trade secret law establishes certain limits on the kind of information that can be protected and the kind of acts it will punish in order to help balance the benefits of protection against its potential costs.[61] For most of its history, trade secret law has been a creature of state law; only recently has federal protection for trade secrets been added to the mix.[62] To

57 The Copyright Act of 1976 removed publication as a component of federal copyright protection. *See* Katyal, *supra* note 4, at 1209; Copyright Act of 1976, Pub. L. No. 94-553, §§ 102, 104, 90 Stat. 2541, 2544–45 (codified at 17 U.S.C. §§ 102, 104 (2018)). Now, copyright begins the moment a work is fixed in a tangible medium of expression. *See* Katyal, *supra* note 4, at 1209; Copyright Act of 1976 § 102. Nonetheless, the majority, if not the vast majority, of commercially valuable copyrighted works are made public. *See* Katyal, *supra* note 4, at 1257. The exception is computer software. *Id.* Typically, patent applications are published after 18 months. *See* 37 C.F.R. § 1.211 (2023).

58 *See* Jeanne C. Fromer, *Patent Disclosure*, 94 IOWA L. REV. 539, 560 (2009).

59 *See* Nichols v. Universal Pictures Corp., 45 F.2d 119, 122 (2d Cir. 1930) ("Though the plaintiff discovered the vein, she could not keep it to herself; so defined, the theme was too generalized an abstraction from what she wrote. It was only a part of her 'ideas.'").

60 *See* Levine, *supra* note 4, at 157.

61 *See id.* at 151–52, 157; Lemley, *supra* note 7, at 329–30.

62 The protection of trade secrets grew out of the nineteenth-century common law of unfair competition, and by the mid-twentieth century, trade secret law's core principles were summarized in the *Restatement (First) of Torts*. RESTATEMENT (FIRST) OF TORTS § 757 (AM. L. INST. 1939). By the end of the twentieth century, the purely common law approach had given way to a statutory regime. *See* UNIF. TRADE SECRETS ACT (UNIF. L. COMM'N 1985). In 1979, the National Conference of Commissioners on Uniform State Laws promulgated the Uniform Trade Secrets Act (UTSA). *Trade Secrets Act*, UNIF. L. COMM'N, https://www.uniformlaws.org/committees/community-home?CommunityKey=3a2538fb-e030-4e2d-a9e2-90373dc05792 [https://perma.cc/U4Q2-LHFE]. Every state except New York has enacted a version of this statute. *See id.* In 2016, Congress enacted the Defend Trade Secrets Act (DTSA), introducing a new federal civil claim for trade secret misappropriation, which parties can assert alongside state law claims; its requirements largely mirror the UTSA. *See* Defend Trade Secrets Act of 2016, 18 U.S.C. §§ 1832–1839 (2018). For a discussion of trade secrecy's evolution from common law to statutory law, see Fishman & Varadarajan, *supra* note 4.

qualify for trade secret protection under state or federal law, information must first and foremost be secret—or at least, secret enough. That is, information cannot be "generally known to" or "readily ascertainable by" others in the relevant industry.[63] If information is common knowledge within an industry or easily deduced by competitors, it is not secret enough to qualify for protection.[64] This limitation serves the law's underlying goal of encouraging investment in informational goods that will otherwise be underproduced. There is no benefit—indeed, there are costs—to awarding exclusive rights in information that everybody already knows or can easily find out.[65]

Not only must information be sufficiently secret, a claimant must also make "reasonable efforts" to keep it so—a requirement that is related to (but conceptually distinct from) the requirement of secrecy.[66] A claimant must engage in at least some affirmative acts to guard against the information's disclosure, such as imposing password protections and confidentiality agreements on employees and business partners with whom the information is shared.[67] While some have questioned the reasonable secrecy efforts requirement,[68] others tout its

63 *See* UNIF. TRADE SECRETS ACT § 1(4) (defining "[t]rade secret" to "mean[] information, 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"); § 1839(3) ("[T]he term 'trade secret' means all forms and types of . . . information . . . if—(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information . . . .").

64 This limitation has existed from the earliest common law cases—long before being enshrined in state and federal statutes. *See, e.g.*, Nat'l Tube Co. v. E. Tube Co., 13 Ohio Cir. Dec. 468, 470 (1902) ("[I]f the idea of these patterns is known generally to the world, or at least to the people interested in that kind and character of business, then it cannot be a trade secret . . . ."), *aff'd*, 70 N.E. 1127 (Ohio 1903).

65 *See* Lemley, *supra* note 7, at 313.

66 UNIF. TRADE SECRETS ACT § 1(4); § 1839(3).

67 *See generally* Deepa Varadarajan, *Trade Secret Precautions, Possession, and Notice*, 68 HASTINGS L.J. 357 (2017) (discussing the reasonable secrecy efforts requirement). Though no single type of precautionary measure is dispositive, the existence of confidentiality agreements has become increasingly important to this assessment. *See* David S. Almeling, Darin W. Snyder, Michael Sapoznikow, Whitney E. McCollum & Jill Weader, *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZ. L. REV. 57, 82–83 (2010/2011) (describing empirical studies suggesting that "confidentiality agreements with employees and business partners are the most important factors in the courts' analysis of reasonable measures").

68 Lemley, *supra* note 7, at 349; Robert G. Bone, *Trade Secrecy, Innovation and the Requirement of Reasonable Secrecy Precautions*, *in* THE LAW AND THEORY OF TRADE SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH 46, 65 (Rochelle C. Dreyfuss & Katherine J. Strandburg eds., 2011) (suggesting this requirement "dampens incentives to create by

ability to help establish the information's secrecy. After all, why would a firm expend resources to protect information that is generally known or easily observed?[69] Perhaps more importantly, in the absence of an ex ante claiming requirement for trade secrets (or any formal application process akin to patent), reasonable secrecy efforts offer some form of notice to employees and others; they announce that certain information is viewed as a trade secret by the putative owner.[70]

Finally, to qualify for protection, information must "derive[] independent economic value, actual or potential," from its secrecy.[71] While courts differ in their understanding of the "independent economic value" element, it is intended to impose a minimal quantitative threshold for the information's value and require this value to stem (at least, in part) from the information's secrecy.[72] Meeting the quantitative threshold for value is not particularly onerous; information need only "provide[] an advantage that is more than trivial."[73] This requirement nonetheless reserves the law's machinery, which "is far from costless," for information with some minimal value.[74] As for the requirement of a "causal connection between value and secrecy," Camilla Hrdy has explained that this aspect of independent economic value "raises the bar on what is needed for protection" and echoes "the policy reasoning behind the secrecy requirement itself."[75]

While satisfaction of these three elements—secrecy, reasonable secrecy efforts, and independent economic value—establishes the

making innovation more costly" and encourages firms to "invest more rather than less in self-help").

69 1 PETER S. MENELL, MARK A. LEMLEY, ROBERT P. MERGES & SHYAMKRISHNA BALGANESH, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE: 2023, at 73 (2023) ("There is an intuitive relationship between the existence of a secret and reasonable efforts to protect a secret. After all, if something is not a secret, there would not seem to be any point to protecting it.").

70 *See* Varadarajan, *supra* note 67, at 377–78; *see also* BondPro Corp. v. Siemens Power Generation, Inc., 463 F.3d 702, 708 (7th Cir. 2006).

71 UNIF. TRADE SECRETS ACT § 1(4); § 1839(3).

72 *See* Camilla A. Hrdy, *The Value in Secrecy*, 91 FORDHAM L. REV. 557, 559–60, 593 (2022); Sharon K. Sandeen, *The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act*, 33 HAMLINE L. REV. 493, 524–26 (2010).

73 RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. e (AM. L. INST. 1995).

74 Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 179–80 (7th Cir. 1991); *see also* Hrdy, *supra* note 72, at 593.

75 *See, e.g.*, Hrdy, *supra* note 72, at 596 ("[T]he alleged trade secret is the information making up the chemical composition for a drug that treats cancer . . . . If most of the composition of the drug is already well known in the industry, and the only thing that is secret about the drug is an alteration or addition, it must be the case that the specific secret alteration or addition gives the holder an economic advantage over others due to being kept secret from others." *Id.* at 595–96.).

existence of a trade secret,[76] not all uses of a trade secret trigger liability. Only the "misappropriation" of a trade secret is prohibited, meaning that the defendant acquired, used, or disclosed it in breach of a confidentiality duty or through "improper means."[77] The paradigmatic case involves an employee, former employee, or business partner who uses a trade secret in violation of a confidentiality duty for their own competing commercial ends.[78] But those who use proper means to acquire trade secret information, such as by independently creating or reverse engineering it, are insulated from liability.[79] The freedom to reverse engineer—"starting with the known product and working backward to divine the process which aided in its development or manufacture"—is an important limitation on a trade secret owner's rights.[80] The Supreme Court has described it as "an essential part of innovation" that "may lead to significant advances in the field."[81]

B. Socially Harmful Trade Secrets

No legal doctrine is perfect—and that is certainly true of IP. There are plenty of bad patents[82] and copyrights.[83] Every doctrine contains tradeoffs that are inherent features of its use. But, as a wave of new scholarship has demonstrated, trade secrecy is increasingly being

76 While these are the only requirements established by state and federal trade secrecy statutes, common law definitions of trade secrecy directed courts to consider additional factors, including "the amount of effort or money expended by [the claimant] in developing the information" at issue. *See* RESTATEMENT (FIRST) OF TORTS, *supra* note 62, § 757 cmt. b; *see also* Fishman & Varadarajan, *supra* note 4, at 1402 (arguing that the assessment of development costs should be a trade secret eligibility requirement). Common law trade secrecy also required the information at issue to be "continuous[ly] use[d] in the operation of the business"; this continuous use requirement was omitted from the UTSA and trade secrecy statutes. RESTATEMENT (FIRST) OF TORTS, *supra* note 62, § 757 cmt. b; *see also* Hrdy & Lemley, *supra* note 2, at 5; Eric R. Claeys, *The Use Requirement at Common Law and Under the Uniform Trade Secrets Act*, 33 HAMLINE L. REV. 583, 583–84 (2010).

77 UNIF. TRADE SECRETS ACT § 1(2) (UNIF. L. COMM'N 1985) (defining "[m]isappropriation" as "acquisition of a trade secret . . . by improper means" or "disclosure or use of a trade secret of another without express or implied consent by a person who . . . acquired [it] under circumstances giving rise to a duty to maintain its secrecy or limit its use"); *see also* 18 U.S.C. § 1839(5) (2018) (similarly defining misappropriation under federal law).

78 *See* Deepa Varadarajan, *Business Secrecy Expansion and FOIA*, 68 UCLA L. REV. 462, 480 (2021).

79 *See* § 1839(6); Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974); UNIF. TRADE SECRETS ACT § 1 cmt..

80 *Kewanee Oil Co.*, 416 U.S. at 476.

81 Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 160 (1989).

82 *See, e.g.*, U.S. Patent No. 6,004,596 (issued Dec. 21, 1999) (granting a patent for a sealed, crustless PB&J sandwich).

83 *See, e.g.*, REBECCA BLACK, FRIDAY (ARK Music Factory 2011); HOWARD THE DUCK (Lucasfilm 1986).

manipulated for antisocial purposes that have nothing to do with its mission of encouraging investment in knowledge.[84] Firms are asserting trade secret rights to block disclosure of a vast range of information that adversely affects journalism, the environment, public health, criminal justice, regulation and democracy.[85] These efforts are not simply the inevitable push and pull of IP's incentives-versus-access paradigm. Rather, they represent an entirely separate category of socially harmful trade secret use.[86] Our goal here is not to exhaustively catalogue the antisocial uses of trade secrecy, nor to evaluate whether trade secrecy protection produces a net social benefit. Rather, we wish to give some sense of the scale and scope of socially harmful trade secrets in order to later determine whether and how the law can screen good uses from bad.

Avoiding public oversight is one of the most significant antisocial uses of trade secrecy in the modern era.[87] Society relies on journalists, watchdogs, and other nongovernmental organizations (NGOs) to discover and report antisocial behavior, but firms have increasingly relied on assertions of trade secrecy and confidentiality to block disclosure of information to these groups (and by extension, the general public). Examples abound, from potentially toxic chemicals (used in hydraulic fracturing and elsewhere) and harmful pharmaceuticals to attempts to discover and disclose firms' data on workplace injuries, sexual harassment claims, and employee diversity.[88] Consider the following examples.

The Environmental Protection Agency (EPA) regulates new chemicals under the Toxic Substances Control Act, which requires companies to notify the agency of new chemicals they plan to release and to provide information about a chemical if they have reason to believe that it "presents a substantial risk of injury to health or the environment."[89] This data, once collected by the agency, can be obtained by the public via the Freedom of Information Act (FOIA).[90] FOIA provides the public with an enforceable right of access to federal agency records, requiring agencies to disclose requested records unless the

84 *See, e.g.*, *supra* note 4 and accompanying text.

85 *See supra* note 4 and accompanying text.

86 Graves & Katyal, *supra* note 4, at 1352 (explaining that this "category of concerns goes beyond the prevention of disclosure and implicates what we see as a wider host of dignitary concerns regarding personal attributes of employees and harms suffered in the workplace, including diversity data, prior complaints of harassment involving race or gender, or forced arbitration or salary information").

87 *See id.* at 1352–53.

88 *See generally id.* (discussing these and many other examples).

89 Toxic Substances Control Act, Pub. L. No. 94-469, § 8(e), 90 Stat. 2003, 2029–30 (1976) (codified at 15 U.S.C. § 2607(e) (2018)).

90 5 U.S.C. § 552 (2018).

information is subject to one of nine enumerated exemptions.[91] There are good reasons to allow members of the public to obtain EPA data on chemical usage. For instance, independent journalists or scientists might discover an environmental hazard that the agency itself has not found. However, Exemption 4 of FOIA authorizes agencies to withhold two categories of information from requesters: trade secrets and confidential commercial information.[92] Firms often rely on Exemption 4 to resist public disclosure of information submitted to agencies.[93] The result is that attempts by journalists, NGOs, and other watchdogs to uncover data about risks via FOIA requests to agencies are frequently stymied by assertions of secrecy.[94]

Similar limitations in the Federal Insecticide, Fungicide, and Rodenticide Act, the Federal Water Pollution Control Act, and the Clean Air Act also hinder the disclosure of vital information, if it is claimed as confidential or a trade secret.[95] Several striking examples concern firms engaged in hydraulic fracturing, or fracking, which uses high-pressure injection of chemical fluids into rocks to extract oil and gas.[96] Fracking firms have prevented the disclosure of the bare names of chemicals they use because they claim that doing so would allow competitors to reverse engineer their processes.[97] Their refusal extends even to medical professionals who are treating victims of fracking accidents.[98]

These assertions of secrecy would not present a significant social problem if the EPA and similar agencies were infallible and could be trusted to safeguard public health and welfare in every instance. A perfect government regulator would be a full solution to the problem of firms emitting potentially toxic chemicals.[99] Indeed, Congress has

91 *See* § 552(b).

92 *See* § 552(b)(4) (authorizing agencies to withhold "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential"). When an agency examiner denies a request for information, FOIA not only provides an administrative appeals process but also affords the requester a remedy in federal court, which reviews the agency withholding decisions de novo, and where the agency bears the burden of proof in defending nondisclosure. § 552(a)(4)–(6).

93 *See* Varadarajan, *supra* note 78, at 468.

94 *See* § 552(b)(4); Toxic Substances Control Act § 14(a) (prohibiting the EPA from disclosing any material that would fall within FOIA's Exemption 4 protections for trade secrecy to the public). *See generally* Varadarajan, *supra* note 78.

95 *See* Federal Insecticide, Fungicide, and Rodenticide Act, 7 U.S.C. § 136 (2018); Federal Water Pollution Control Act, 33 U.S.C. §§ 1251–1376 (2018); Clean Air Act, 42 U.S.C. §§ 7401–7671 (2018).

96 *See* Graves & Katyal, *supra* note 4, at 1359.

97 *Id.* at 1360.

98 *Id.*

99 There is an analogy to the movement for corporate social responsibility. If public regulators—EPA, OSHA, etc.—were perfect, there would be no need to worry about

recently added whistleblower immunity provisions to federal trade secret law. These provisions exempt from trade secret liability a whistleblower who discloses information to a government official or attorney "solely for the purpose of reporting or investigating a suspected violation of law."[100] In theory, then, regulators should have an even easier time obtaining access to information that is not disclosed to the general public.

But of course, regulators are not perfect, and examples abound of hazards that agencies have missed and the public has caught.[101] One of FOIA's fundamental justifications is that agencies are, in fact, fallible, and that public disclosure is the best way to "hold the governors accountable to the governed."[102] Outside experts, researchers, journalists, and watchdog groups serve as an important check on the limitations and resource constraints of agencies.[103]

Would chemical manufacturers and fracking firms suffer if data about their activities were made public? Almost certainly. One problem, from the perspective of the firm asserting its trade secret rights, is

---

whether corporations would act in a socially responsible fashion of their own accord. Regulators would simply ensure that corporations behaved optimally, backed by threat of sanction. But of course regulators are not perfect, and thus it is important to explore the possibility that corporations might be incentivized to act prosocially by means other than government regulation. *See* Hajin Kim, *Expecting Corporate Prosociality*, 53 J. LEGAL STUD. 267, 268 (2024); Hajin Kim, Joshua Macey & Kristen Underhill, *Does ESG Crowd In or Out Support for Regulation?*, AM. L. & ECON. REV. (July 28, 2025), https://academic.oup.com/aler/advance-article/doi/10.1093/aler/ahaf009/8215653 [https://perma.cc/F8LB-QNFB]. *See generally* Virginia Harper Ho, *"Enlightened Shareholder Value": Corporate Governance Beyond the Shareholder-Stakeholder Divide*, 36 J. CORP. L. 59 (2010).

100 18 U.S.C. § 1833(b)(1)(A)(ii) (2018) ("An individual shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that—(A) is made—(i) in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of law . . . ." § 1833(b)(1).). Congress included this whistleblower provision as part of the Defend Trade Secrets Act of 2016, which enacted a new federal civil remedy for trade secret misappropriation. *See* Defend Trade Secrets Act of 2016, 18 U.S.C. §§ 1832–1839 (2018); *supra* note 62; *see also* Peter S. Menell, *Tailoring a Public Policy Exception to Trade Secret Protection*, 105 CALIF. L. REV. 1, 61–62 (2017).

101 *See, e.g.*, Mary L. Lyndon, *Trade Secrets and Information Access in Environmental Law*, *in* THE LAW AND THEORY OF TRADE SECRECY, *supra* note 68, at 442, 444–45; Varadarajan, *supra* note 37, at 1442–43.

102 NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 (1978); *see also* U.S. Dep't of State v. Ray, 502 U.S. 164, 173 (1991) (describing FOIA's purpose "to pierce the veil of administrative secrecy and to open agency action to the light of public scrutiny" (quoting Dep't of the Air Force v. Rose, 425 U.S. 352, 361 (1976))).

103 *Cf.* Margaret B. Kwoka, *FOIA, Inc.*, 65 DUKE L.J. 1361, 1371, 1361 (2016) (explaining that FOIA was "designed largely by journalists, for journalists, and with the particular goal in mind that journalists would use access to government information to provide knowledge to the public" but also describing how journalists' efforts are being "crowded out" by profit-seeking FOIA requesters).

that competitors could free ride on their discoveries, in the way that trade secret law attempts to deter.[104] But, more importantly, firms might suffer by virtue of being subject to greater journalistic, political, and regulatory oversight.[105] That oversight would increase their costs and decrease their profits. In extreme cases, disclosure could even put a firm out of business—for example, if the public learned that its chemicals cause serious health risks. The same trade secret thus presents the possibility of doing a substantial amount of good or a substantial amount of harm. On the one hand, recognizing trade secrets can help prevent the sort of free riding that animates trade secrecy law.[106] But, on the other hand, if the information reveals socially harmful activity, then recognizing trade secrets in these situations undermines social welfare by limiting society's ability to gauge and regulate risks.

Similarly, in the context of drug safety, pharmaceutical firms have asserted trade secrecy and confidentiality to prevent the FDA from disclosing critical health information to the public.[107] Christopher Morten and Amy Kapczynski describe this widespread practice of data secrecy, highlighting the notable example of Vioxx—Merck's blockbuster, multibillion-dollar drug that was quickly pulled from the market after causing heart attacks, strokes, and heart failure.[108] Evidence of this linkage was uncovered only through litigation, despite the fact that Merck had submitted data signaling these risks to the FDA several years before.[109] Although the FDA had the relevant data in its possession, trade secrecy prevented independent researchers and the public from accessing it—at the possible cost of tens of thousands of lives.[110]

Firms also assert secrecy over labor and employment data that is of significant interest to the public. The Department of Labor collects vast quantities of data relating to employees, including about employee demographics and workplace injuries.[111] But in recent cases, the Department withheld records requested by the Center for Investigative Reporting on the grounds that such information was confidential.[112] The companies asserted that workplace injury information was critical

104 *See supra* Section I.A.

105 *See supra* note 4 and accompanying text.

106 *See supra* Section I.A.

107 *See* Morten & Kapczynski, *supra* note 4, at 496.

108 *See id.*

109 *See id.*

110 *See id.*

111 *See Injuries, Illnesses, and Fatalities*, U.S. BUREAU OF LAB. STAT., https://www.bls.gov/iif/ [https://perma.cc/C62Q-DP43].

112 *See* Ctr. for Investigative Reporting v. U.S. Dep't of Lab., 424 F. Supp. 3d 771, 775 (N.D. Cal. 2019); Ctr. for Investigative Reporting v. U.S. Dep't of Lab., 470 F. Supp. 3d 1096, 1103–04 (N.D. Cal. 2020); Ctr. for Investigative Reporting v. Dep't of Lab., No. 18-cv-02414, 2020 WL 2995209, at *2 (N.D. Cal. June 4, 2020).

to their "operational mission and commercial success."[113] Swayed by these assertions, the Department determined that the requested records comprised "information in which the establishments have a commercial interest, information that deals with commerce, and information that is related to business or trade."[114]

Of course, if firms do indeed have horrendous records on diversity or workplace injuries, they probably aren't wrong that disclosing those records would be detrimental to them. Google, for instance, might have an even harder time attracting women engineers if its diversity data revealed that it currently employs very few women engineers. Amazon might have to pay warehouse staff higher wages if it were revealed that large numbers of people are injured while working in its facilities. But that's the whole point, isn't it? We want this information to be made public because publicity is a vital mechanism for changing bad behavior. It is also a vital mechanism for checking that regulators are properly performing their oversight function.

A firm's ability to resist disclosure of potentially damaging information has only increased in recent years. When an agency receives information from a private firm, and then someone files a FOIA request for that information, the agency is not required to withhold it.[115] This is true even if the information falls within one of FOIA's exemptions, as they are permissive rather than mandatory.[116] But if requested information is claimed to be a trade secret or confidential commercial information under Exemption 4, an agency's withholding calculus is complicated by the Trade Secrets Act, a criminal statute.[117] Some

113 Defendant's Motion for Summary Judgment at 12, *Ctr. for Investigative Reporting*, 470 F. Supp. 3d 1096 (No. 19-cv-05603), *quoted in* Graves & Katyal, *supra* note 4, at 1364.

114 Defendant's Motion for Summary Judgment: Memorandum of Points and Authorities in Support Thereof at 13, *Ctr. for Investigative Reporting*, 2020 WL 2995209 (No. 18-cv-02414).

115 *See* 5 U.S.C. § 552(a)(3)(A) (2018).

116 *See* Chrysler Corp. v. Brown, 441 U.S. 281, 293–94 (1979) (explaining that FOIA's "exemptions were only meant to permit the agency to withhold certain information, and were not meant to mandate nondisclosure").

117 *See* 18 U.S.C. § 1905 (2018) ("Whoever, being an officer or employee of the United States or of any department or agency thereof, . . . publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties . . . , which information concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association . . . shall be fined under this title, or imprisoned not more than one year, or both; and shall be removed from office or employment.").

courts have held that this statute prohibits agencies from releasing information covered by FOIA Exemption 4.[118]

More recently, the Supreme Court significantly expanded the scope of information that falls within Exemption 4 in its 2019 decision, *Food Marketing Institute v. Argus Leader Media*.[119] Prior to this decision, agencies were unlikely to withhold requested information as "confidential" unless its disclosure would cause "substantial harm to the competitive position of the person from whom the information was obtained."[120] But *Argus Leader* eliminated any assessment of harm, holding instead that commercial information is "confidential" and can be withheld under Exemption 4 so long as the submitter (and, possibly, the government) "treat[s] [it] as private."[121] And while the *Argus Leader* decision makes no mention of the "trade secret" category,[122] by expanding the category of "confidential" commercial information to align more closely with firms' own privacy preferences, the decision's practical effect is to collapse the two categories into one that is far

118 *See, e.g.*, McDonnell Douglas Corp. v. Widnall, 57 F.3d 1162, 1164 (D.C. Cir. 1995) (stating that "the scope of the Trade Secrets Act 'is at least co-extensive with that of Exemption 4 of FOIA'" and "[c]onsequently, whenever a party succeeds in demonstrating that its materials fall within Exemption 4, the government is precluded from releasing the information by virtue of the Trade Secrets Act" (quoting CNA Fin. Corp. v. Donovan, 830 F.2d 1132, 1151 (D.C. Cir. 1987))). But others have questioned this interpretation of the Trade Secrets Act as being coextensive with Exemption 4. *See, e.g.*, Gen. Elec. Co. v. U.S. Nuclear Regul. Comm'n, 750 F.2d 1394, 1402 (7th Cir. 1984) ("Exemption 4 is broadly worded, and it is hard to believe that Congress wanted seekers after information to stub their toes on a rather obscure criminal statute almost certainly designed to protect that narrower category of trade secrets—secret formulas and the like—whose disclosure could be devastating to the owners and not just harmful.").

119 Food Mktg. Inst. v. Argus Leader Media, 139 S. Ct. 2356 (2019).

120 Nat'l Parks & Conservation Ass'n v. Morton, 498 F.2d 765, 770 (D.C. Cir. 1974), *abrogated by Argus Leader*, 139 S. Ct. 2356. Although the D.C. Circuit later qualified this holding in *Critical Mass Energy Project v. Nuclear Regulatory Commission*, 975 F.2d 871, 878 (D.C. Cir. 1992) (en banc), applying it to required rather than voluntary agency submissions, the substantial competitive harm test of *National Parks* was widely adopted by other circuits. *Id.* at 876.

121 *Argus Leader*, 139 S. Ct. at 2366. The Court held that information is "confidential" for Exemption 4 purposes "[a]t least" where it is "[(1)] both customarily and actually treated as private by its owner and [(2)] provided to the government under an assurance of privacy." *Id.* In this phrasing, the Court left the precise boundaries of the test undefined, observing, "At least the first of these conditions must be met; it is hard to see how information could be deemed confidential if its owner shares it freely. But the Court need not resolve whether both conditions are necessary because both conditions are clearly met here." *Id.* at 2359.

122 A trade secret for FOIA purposes is more narrowly defined as a "secret, commercially valuable plan, formula, process, or device that is used for the making, preparing, compounding, or processing of trade commodities and that can be said to be the end product of either innovation or substantial effort." Pub. Citizen Health Rsch. Grp. v. FDA, 704 F.2d 1280, 1288 (D.C. Cir. 1983).

easier to satisfy. In the wake of *Argus Leader*, journalists and watchdog groups are likely to have a harder time uncovering the kind of bad behavior discussed above.[123]

Nor is the oversight task of journalists and watchdog groups made easier by trade secret law's whistleblower immunity provisions, discussed above. Notably, these provisions insulate from trade secret liability only those who disclose information in the course of reporting suspected violations of law to a "government official" or "attorney."[124] These whistleblower provisions are thus quite limited in application and do not apply to any disclosures that are made to journalists, researchers, or nongovernmental officials interested in assessing the information. [125]

Finally—and this is certainly not the last or least significant example—consider the increasing role of trade secrecy in our criminal legal system. Algorithms are being used in a wide variety of criminal investigation, adjudication, detention, and sentencing contexts, and their use will only grow with advances in machine learning and artificial intelligence.[126] Perhaps algorithms, with their rote objectivity, will be free from many of the biases that impair human judgment in these contexts.[127] Or perhaps they won't.[128] In fact, there is reason to suspect that risk assessment algorithms used to determine future conduct for bail, sentencing, and parole purposes are biased against racial minorities—perhaps just as much as human decisionmakers.[129]

If courts—or court-appointed special masters—were capable of assessing the performance of these algorithms and determining whether they are biased, that would be a full solution. Here too, as with the regulatory agencies described above, a perfect governmental actor would make public disclosure of the information unnecessary. Yet we know from experience that judges are rarely capable of performing this task and too rarely hire or appoint others to do it for them. In order to know whether criminal justice algorithms are, in fact, biased

123 *See* Varadarajan, *supra* note 78, at 468.

124 *See* 18 U.S.C. § 1833(b)(1).

125 Commentators have identified several limitations and problems with the application of these provisions. *See, e.g.*, Graves & Katyal, *supra* note 4, at 1366–68.

126 *See generally* Wexler, *supra* note 4; Elizabeth A. Rowe & Nyja Prior, *Procuring Algorithmic Transparency*, 74 ALA. L. REV. 303 (2022); Hannah Bloch-Wehba, *Visible Policing: Technology, Transparency, and Democratic Control*, 109 CALIF. L. REV. 917 (2021).

127 *See, e.g.*, Rowe & Prior, *supra* note 126, at 313 (describing how "[a]n increasing number of jurisdictions continue to adopt statistical algorithmic software in various criminal justice contexts in an attempt to maximize resources, reduce bias, and promote justice").

128 *See* Ngozi Okidegbe, *The Democratizing Potential of Algorithms?*, 53 CONN. L. REV. 739, 757–66 (2022).

129 *See* Rowe & Prior, *supra* note 126, at 327–30.

against certain groups, it is thus essential that people outside of the firms that develop them—including defendants, their attorneys, and their experts—be able to study these algorithms.[130]

Unfortunately, trade secrecy claims have stifled disclosure in this area as well. Both software development firms and the law enforcement agencies that use their products have fought to prevent access to confidential algorithms.[131] In one oft-cited example, the California Court of Appeals denied a death penalty–eligible defendant access to algorithmic source code that was used to calculate the likely presence of his DNA at the crime scene.[132] While the trial court had ordered disclosure of the source code (subject to a protective order), the software developer objected, arguing that its code was covered by California's trade secret privilege.[133] The appeals court ruled for the developer, "likely becoming the first appellate court in the nation's history to extend a trade secret evidentiary privilege to a criminal case."[134] Other courts have followed suit.[135] Similarly, in the post-trial context, firms that develop risk assessment algorithms to assist trial courts in sentencing decisions have invoked trade secrecy, preventing criminal defendants from understanding how their risk scores for recidivism are determined and whether these tools generate biased or discriminatory predictions.[136]

Disclosure of harmful secrets is likely even more important in the criminal context than in the other regulatory contexts we have discussed because adversarial adjudication is the principal means by which we test the quality of evidence.[137] While environmental and labor law have regulatory bodies that are primarily responsible for

130 *See id.*

131 Wexler, *supra* note 4, at 1365.

132 *See* People v. Superior Ct. (*Chubbs*), No. B258569, 2015 WL 139069, at *1–2 (Cal. Ct. App. Jan. 9, 2015); Wexler, *supra* note 4, at 1358.

133 *Chubbs*, 2015 WL 139069, at *4.

134 Wexler, *supra* note 4, at 1359.

135 *Id.* at 1360–61 (noting that "*Chubbs* is now being cited in criminal proceedings across the country to justify withholding trade secret evidence from the accused" and that "[o]ther courts have adopted similar reasoning, whether via an explicit evidentiary privilege or by more loosely incorporating the trade secret status of evidence into their evaluations of defendant's discovery and subpoena motions") (citing examples); *see also* Rowe & Prior, *supra* note 126, at 325–26 (describing the impact of *Chubbs*).

136 *See, e.g.*, State v. Loomis, 881 N.W.2d 749, 761 (Wis. 2016); *see also* Wexler, *supra* note 4, at 1369 (discussing the "trade secret obstacles" defendants face in "challenging their risk assessment scores"); Rowe & Prior, *supra* note 126, at 327–30; Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/BR23-KV2K].

137 *See* Rebecca Wexler, *Privacy Asymmetries: Access to Data in Criminal Defense Investigations*, 68 UCLA L. REV. 212, 215–17, 222–24 (2021).

policing bad behavior by firms, criminal law has less oversight from federal or state regulators. We rely on defendants, their lawyers, and their experts to challenge the quality of the data that is used to arrest, detain, convict, and punish them.[138] But they cannot perform this role effectively when their access to secret information is curtailed.[139]

The social welfare tradeoff in these examples remains tricky. In the absence of trade secret protection, firms might be unwilling to produce algorithms and other valuable information in the first place, because they could be easily copied by competitors.[140] Thus, if the algorithms are socially valuable, so is trade secrecy. But trade secrecy also prevents us from learning whether they are, in fact, socially valuable. Trade secrecy law seems caught in a version of Arrow's Information Paradox: policymakers cannot determine whether the information should be disclosed without first disclosing it.[141] But disclosing it more broadly risks the possibility of eliminating trade secret protection. In the Parts that follow, we explore whether law can find a solution—either through doctrinal screens or costly screens, which are both mechanisms that have been effective in other areas of intellectual property.

II. WHY DOCTRINAL SCREENS FAIL

Granting intellectual property rights can be good for society. IP rights encourage creativity and innovation, and they promote fair and valuable competition. But granting IP rights can also be costly for society. When IP rights are unnecessary, they raise costs for consumers and competitors without corresponding benefits.[142] The goal of any IP regime is to grant rights when doing so is socially valuable, but to prevent claimants from obtaining rights when doing so would be socially costly.[143]

Of course, Congress can't simply pass a law that says "grant copyrights or patents when doing so would increase social welfare, and deny them when it wouldn't." Or maybe it theoretically could, but such a

138 *See id.*

139 *See id.* at 215–17.

140 *See supra* Section I.A.

141 *See infra* Section II.B.

142 IP rights allow their owners to charge higher prices to consumers and impose additional costs on those seeking to develop their own works or improve on existing ones—e.g., paying licensing fees or engaging in expensive efforts to design around existing rights. *See* Christopher Buccafusco & Jonathan S. Masur, *Innovation and Incarceration: An Economic Analysis of Criminal Intellectual Property Law*, 87 S. CAL. L. REV. 275, 282–83 (2014); Mark A. Lemley, *Ex Ante Versus Ex Post Justifications for Intellectual Property*, 71 U. CHI. L. REV. 129, 129 (2004).

143 *See* Buccafusco, Lemley & Masur, *supra* note 26, at 87.

law would be completely unworkable in practice.[144] For how is a court or the United States Patent and Trademark Office (PTO) supposed to know whether a given patent or copyright will increase social welfare?[145] Instead, legal doctrines (doctrinal screens) act as proxies for social welfare; they help decisionmakers screen welfare-enhancing assertions of rights and entitlements from welfare-diminishing ones.[146] That is, doctrinal screens operate as wholesale-level proxies for social welfare, eliminating IP rights that the law predicts will be welfare diminishing. These screens helpfully avoid much retail-level analysis of whether each individually asserted right would be welfare improving or welfare diminishing.

One might imagine that trade secret law should do the same. Like other areas of IP, it, too, could incorporate such doctrinal screens, proxies for separating trade secrets that increase social welfare from those that don't, and make the grant of legal rights contingent upon the existence of those proxies. Yet this is not what trade secret law actually does.[147] In this Part, we show how the law's current doctrinal screens—secrecy, reasonable secrecy efforts, and economic value—aren't up to this sorting task. More importantly, we explain that even superior versions of these screens are likely to fail in similar ways. Fundamental aspects of trade secrets render doctrinal screens ineffectual in identifying welfare-enhancing assertions of rights. This problem is endemic to the nature of trade secrets, and thus, it cannot be overcome by even the best-intentioned policymaker.[148]

---

144 Imagine, for example, that the United States Patent and Trademark Office (PTO) was tasked with determining, at the time of patent filing, whether a new pharmaceutical would improve patient outcomes or not. There is no way it could have sufficient information at that moment to do so accurately. Instead, the law relies on doctrinal screens to exclude predictably harmful patent rights. *See* Christopher Buccafusco & Jonathan S. Masur, *Drugs, Patents, and Well-Being*, 98 WASH. U. L. REV. 1403, 1409–11 (2021).

145 *See* Bleistein v. Donaldson Lithographing Co., 188 U.S. 239, 251 (1903) ("It would be a dangerous undertaking for persons trained only to the law to constitute themselves final judges of the worth of pictorial illustrations, outside of the narrowest and most obvious limits."). While a judicially created doctrine of "moral utility" once allowed courts and the PTO to deny patents on morally problematic inventions (e.g., gambling devices) on grounds that they were not "useful," it has been more or less excised from U.S. patent law. *See, e.g.*, Juicy Whip, Inc. v. Orange Bang, Inc., 185 F.3d 1364, 1366–67 (Fed. Cir. 1999).

146 *See* Buccafusco, Lemley & Masur, *supra* note 26, at 91. Some examples of proxies include the novelty screen for patents and the distinctiveness screen for trademarks. *See infra* Section II.A.

147 *See infra* Section II.B.

148 This is not to say that any doctrinal adjustment to trade secrecy is unwarranted or futile. Some can better align trade secrecy doctrine with its underlying incentive justification, *see* Fishman & Varadarajan, *supra* note 4, at 1424–44, or help ensure that employees have better notice of purported trade secret boundaries in the absence of any ex ante claiming requirement, *see* Varadarajan, *supra* note 67, at 388–94, or help address concerns of worker mobility and cumulative innovation by departing employees, *see, e.g.*, Camilla A.

The result of trade secrecy law's failure to screen out socially harmful rights through doctrinal proxies is that virtually all of the necessary screening has to happen by agencies and judges. That is, because trade secrecy law does little to screen out socially harmful secrets at the wholesale level, almost all of the screening has to occur at the retail level. This is exactly the sort of right-by-right screening that the law tried hard to avoid because of how resource intensive it is.

Below, Section II.A describes the shortcomings of existing doctrine. We then turn in Section II.B to the theoretical limits that likely prevent *any* potential trade secret doctrine from performing the kind of sorting function that a well-intentioned policymaker would like it to do.

A. Screening for Social vs. Private Value

The goal of a doctrinal screen is to sort socially valuable claims from socially costly ones, granting rights only to the former.[149] While no doctrinal screen is perfect,[150] some are better proxies for social value than others. Consider patent law's novelty screen.[151] We can be pretty confident that granting a patent to a claimed invention that already exists won't be good for society.[152] Society already has access to the invention, so the patent didn't incentivize its creation, and granting a new patent will simply increase costs for consumers and

---

Hrdy, *The General Knowledge, Skill, and Experience Paradox*, 60 B.C. L. REV. 2409 (2019); Joseph P. Fishman & Deepa Varadarajan, *Similar Secrets*, 167 U. PA. L. REV. 1051 (2019), to name a few examples. But doctrinal adjustments are unlikely to perform a useful screening function for many of the antisocial secrets we highlight here, which are largely technical in nature and require significant investments to develop—e.g., algorithms, fracking chemicals, airplane design information, etc.

149 *See* Dan L. Burk & Mark A. Lemley, *Policy Levers in Patent Law*, 89 VA. L. REV. 1575, 1580, 1638–58 (2003) (explaining various ways that IP laws are calibrated to generate net social benefits).

150 Buccafusco, Lemley & Masur, *supra* note 26, at 91.

151 To receive patent protection, the claimed invention must be novel. *See* 35 U.S.C. § 102(a) (2018) ("A person shall be entitled to a patent unless—(1) the claimed invention was patented, described in a printed publication, or in public use, on sale, or otherwise available to the public before the effective filing date of the claimed invention; or (2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention."); Bilski v. Kappos, 561 U.S. 593, 601–02 (2010). The novelty requirement seeks to balance "the tension, ever present in patent law, between stimulating innovation by protecting inventors and impeding progress by granting patents when not justified by the statutory design." *Id.* at 609.

152 *See* Stephen Yelderman, *The Value of Accuracy in the Patent System*, 84 U. CHI. L. REV. 1217, 1244 (2017).

competitors.[153] The same is true of patent law's nonobviousness screen, which requires a patentable invention to offer more than just a trivial advance over what already exists.[154] Or consider trademark law's doctrinal screen against generic marks.[155] It would be bad for society if just one seller of coffee, for example, had the exclusive right to call its product "coffee."[156] Thus, trademark doctrine prevents firms from claiming generic marks.[157] This is not to say that there won't be false positives—for instance, patents that pass the required doctrinal screens but are nonetheless socially harmful, such as a new type of poison gas. But these doctrinal screens generally do a good job of eliminating what would be harmful IP rights without inhibiting socially beneficial ones.

Trade secrecy law imposes three doctrinal screens to determine the validity of a claim—secrecy, reasonable secrecy efforts, and independent economic value—all of which we discussed in the previous Part.[158] As we argue in this Part, however, none is up to the task of sorting socially beneficial secrets from socially harmful ones. This is because the law's doctrinal screens map on to the wrong sort of value.

Any given legal right or behavior has both "social value" and "private value."[159] The social value is the value of that thing to society at large.[160] The private value is the value of that thing to the party that owns it.[161] For instance, a useful patented pharmaceutical drug has

153 *See* Buccafusco, Lemley & Masur, *supra* note 26, at 90–91.

154 *See* 35 U.S.C. § 103 (2018) ("A patent . . . may not be obtained . . . if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains.").

155 To receive trademark protection, the claimed mark must not be generic. Two Pesos, Inc. v. Taco Cabana, Inc., 505 U.S. 763, 768 (1992). Generic marks are those which "refe[r] to the genus of which the particular product is a species." *Id.* (alteration in original) (quoting Park 'N Fly, Inc. v. Dollar Park & Fly, Inc., 469 U.S. 189, 194 (1985)).

156 If generic marks received trademark protection, this could confuse and mislead consumers about the nature of certain products, resulting in higher consumer search costs. *See* Buccafusco, Masur & McKenna, *supra* note 26, at 452–53; Stacey L. Dogan & Mark A. Lemley, *Trademarks and Consumer Search Costs on the Internet*, 41 HOUS. L. REV. 777, 786 (2004) ("[T]rademarks contribute to economic efficiency by reducing consumer search costs.").

157 15 U.S.C. § 1052(e) (2018) (prohibiting registration of generic trademarks).

158 *See supra* Section I.A.

159 *See* Buccafusco, Lemley & Masur, *supra* note 26, at 89–90. This categorization was originally laid out in Fagundes & Masur, *supra* note 26, at 692–705, and Masur, *supra* note 26, at 701–15.

160 *See* Buccafusco, Lemley & Masur, *supra* note 26, at 89.

161 *See id.* Whether an IP right has high or low private value depends on the putative owner's ability to generate significant income from the ownership of that right. *See id.* The more income the owner can generate, the higher the private value of the IP right. Such income may come from production, licensing, or litigation. *See id.*

high social value and high private value. The drug is socially valuable, in that it can be used to cure disease and thus help people, and the drug would not have been created but for the patent. But the patented drug is also privately valuable, because the firm or individual who owns the patent can use it to earn substantial revenue from selling the drug or licensing the patent. On the other hand, a patent on horse-and-buggy technology likely has low private value and negative social value. The patent is worthless (or close to it) to its owner, because there is no way to monetize an invention that nobody wants. But the patent might also create negative social value if it forces new innovators to engineer around it, increases their search costs as they comb through existing patents to determine which they might infringe, or otherwise throws sand into the gears of innovation.[162]

Policymakers are supposed to care about social value, not private value.[163] Their concern is how legal rights affect overall social welfare, not how they affect the wealth or power of a given individual actor. Private value is only important insofar as it is an input to social value or insofar as effects on private value cause firms to take actions that increase or decrease social value.

As we explained above, trade secret protection is most likely to be socially valuable when it applies to information requiring costly investment that a firm would not otherwise make absent a trade secret—like the algorithm example discussed at the outset.[164] By contrast, granting trade secret protection will generally be bad for society when the social benefits of disclosure exceed the private benefits of secrecy. As we discuss in the subsections that follow, none of trade secrecy law's doctrinal screens—secrecy, reasonable secrecy efforts, or independent economic value—are likely to differentiate these sorts of claims especially well. The problem is that these doctrinal screens are, at best, proxies for private value rather than social value.

1. Secrecy and Reasonable Secrecy Efforts

First, consider the secrecy requirement. In order to form the basis for a valid trade secret right, the claimed information must be sufficiently secret. It cannot be "generally known to" or "readily ascertainable by" others in the relevant industry.[165] Relatedly, a trade secret

162 *See* Masur, *supra* note 26, at 704 (noting that patents have negative social value when they "provide no corresponding social benefit to offset the transaction costs and hindrances to competition they create").

163 Or at least they do ideally, which is to say that they should.

164 *See supra* Section I.A.

165 *See* UNIF. TRADE SECRETS ACT § 1(4)(i) (UNIF. L. COMM'N 1985); *supra* notes 63–65 and accompanying text.

claimant must exercise reasonable efforts to maintain the information's secrecy,[166] for example by imposing nondisclosure contracts on parties with whom it shares the secret and other types of access restrictions.[167]

But what do we learn about the value of information merely from the fact of its secrecy or a claimant's efforts to keep it secret? We learn that keeping the information secret is *privately* valuable to the firm. Maintaining secrecy isn't costless to the firm.[168] It may have to write and enforce contracts[169] or construct physical or software-based anti-disclosure barriers.[170] Thus, it will only attempt to maintain secrecy when it believes that doing so is more valuable to it than allowing the information to be disclosed would be.[171]

But notice that the firm is only contemplating whether secrecy is valuable to its own interests, not whether secrecy is valuable to society's interests. That a firm is willing to maintain the secrecy of its diversity data,[172] algorithmic source code,[173] fracking chemical composition,[174] airplane design information,[175] drug clinical trial data,[176] or workplace

166 UNIF. TRADE SECRETS ACT § 1(4)(ii); *see also supra* text accompanying notes 66–70.

167 *See, e.g.*, W. Short Home, LLC v. Graeser, 661 F. Supp. 3d 356, 374–75 (M.D. Pa. 2023) (holding that plaintiff company took reasonable steps to protect its trade secrets by, among other things, utilizing and enforcing nonsolicitation and nondisclosure provisions in employment agreements); Allstate Ins. Co. v. Fougere, 79 F.4th 172, 192–93 (1st Cir. 2023); Bison Advisors LLC v. Kessler, No. 14-cv-3121, 2016 WL 4361517, at *4 (D. Minn. Aug. 12, 2016); API Ams. Inc. v. Miller, 380 F. Supp. 3d 1141, 1148–49 (D. Kan. 2019).

168 *See, e.g.*, Elizabeth A. Rowe, *Contributory Negligence, Technology, and Trade Secrets*, 17 GEO. MASON L. REV. 1, 9 (2009); Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 180 (7th Cir. 1991) ("[R]econfigurations of patterns of work and production are far from costless . . . .").

169 *See* AvidAir Helicopter Supply, Inc. v. Rolls-Royce Corp., 663 F.3d 966, 974 (8th Cir. 2011) (noting that the existence of confidentiality agreements is frequently considered as a factor in establishing a trade secret claim).

170 *See* Heska Corp. v. Qorvo US, Inc., No. 19-cv-1108, 2020 WL 5821078, at *6 (M.D.N.C. Sept. 30, 2020) (citing Trans-Radial Sols., LLC v. Burlington Med., LLC, No. 18-cv-656, 2019 WL 3557879, at *16 (E.D. Va. Aug. 5, 2019)) (noting that physical barriers to accessing information constitutes a reasonable effort to maintain a trade secret).

171 *See Rockwell*, 925 F.2d at 179–80 ("[T]he more the owner of the trade secret spends on preventing the secret from leaking out, the more he demonstrates that the secret has real value deserving of legal protection . . . .").

172 *See, e.g.*, Moussouris v. Microsoft Corp., No. 15-cv-1483, 2018 WL 1159251, at *12 (W.D. Wash. Feb. 16, 2018) (finding defendant's argument that its diversity initiatives and strategies constituted trade secrets to be "very persuasive" while finding defendant's argument that its raw diversity data constituted trade secrets to be "less persuasive"), *report and recommendation adopted by* No. 15-cv-1483, 2018 WL 1157997 (W.D. Wash. Mar. 1, 2018).

173 *See, e.g.*, Vt. Microsystems, Inc. v. Autodesk, Inc., 88 F.3d 142, 149 (2d Cir. 1996) (affirming that defendant's triangle-shading algorithm constituted a trade secret).

174 *See supra* text accompanying notes 97–98.

175 *See* Flyers Rts. Educ. Fund, Inc. v. FAA, 71 F.4th 1051, 1056 (D.C. Cir. 2023).

176 *See supra* text accompanying notes 107–110.

injury statistics[177] only tells us that the firm thinks public disclosure of that information would be bad for the firm. Maybe it thinks that disclosure would be bad because it would undermine investment in that information.[178] But the firm might have any number of other private justifications for maintaining the secrecy of that information.[179] Thus, the secrecy and reasonable secrecy efforts requirements are doing virtually nothing to screen out the sorts of socially costly trade secrets we described in Part I.[180]

2. Independent Economic Value

The same problem exists for trade secret law's other doctrinal screen—the independent economic value requirement. The requirement that information "derive[] independent economic value, actual or potential" from its secrecy[181] has been quite valueless in application. As Camilla Hrdy has explained, many courts and commentators view the economic value requirement as virtually nonexistent.[182] After all, if maintaining secrecy is at least somewhat costly to the claimant, then a rational claimant wouldn't invest in secrecy unless the information's secrecy had some value.[183] Independent economic value thus becomes tautological with secrecy—if the firm is expending resources on secrecy, it must be doing so because the information is valuable.[184]

---

177 *See, e.g.*, Ctr. for Investigative Reporting v. U.S. Dep't of Lab., 470 F. Supp. 3d 1096, 1104, 1108 (N.D. Cal. 2020) (finding that the FOIA exemption for trade secrets and commercial and financial information did not apply to work-related injuries and illnesses where the retailer did not customarily or actually treat the data as private).

178 *See* Winston Rsch. Corp. v. Minn. Mining & Mfg. Co., 350 F.2d 134, 138 (9th Cir. 1965) (observing that "the results of research and development must be accorded reasonable protection from disclosure or private investment in such activities will be inhibited").

179 For example, firms have used NDAs to silence victims of sexual assault in order to avoid prosecution and to advance their reputational interests. *See, e.g.*, Ronan Farrow, *Harvey Weinstein's Secret Settlements*, THE NEW YORKER (Nov. 21, 2017), https://www.newyorker.com/news/news-desk/harvey-weinsteins-secret-settlements [https://perma.cc/55GJ-TQS7].

180 *See supra* Section I.B.

181 *See supra* notes 71–75 and accompanying text.

182 *See* Hrdy, *supra* note 72, at 560 ("Courts and commentators assume, not irrationally, that any information that ends up in court as the plausible subject of trade secret litigation has at least *potential* economic value sufficient to satisfy the statute. Why else would the plaintiff have bothered to take secrecy precautions?").

183 *Id.*; *see also* Varadarajan, *supra* note 67, at 375 (explaining the view of some courts and commentators that a "plaintiff's secrecy precautions are circumstantial evidence of . . . the information's independent economic value").

184 *But see* Hrdy, *supra* note 72, at 561 ("Independent economic value cannot be presumed from the mere fact that the plaintiff kept information secret . . . ."); Eric E. Johnson, *Trade Secret Subject Matter*, 33 HAMLINE L. REV. 545, 556–57, 567–73 (2010) (suggesting that economic value is a particularly important component of trade secret subject matter);

Consider again the fracking example.[185] A mining firm, through substantial research and development, creates a mix of substances that it believes offers the most efficient extraction of natural gas. This information provides a competitive advantage to the firm, and public disclosure would undermine that advantage. Thus, the firm is willing to invest in costly secrecy barriers, and the information's secrecy creates independent economic value to the firm. Any court or FOIA decisionmaker would correctly assess that trade secret law's doctrinal screens are met.

But it should now be obvious that, just like the secrecy screen, the independent value screen only conditions a right's validity on the *private value* to the claimant. Once again, that a claimant expends money or effort on secrecy shows only that the claimant prefers secrecy to the corresponding expense. Since private value and social value in secrecy might diverge for a wide variety of reasons, the private value in secrecy isn't a good proxy for its social value. Just as likely, the opposite could be true. As we explained above, the chemical mixture could cause massive harm to human and environmental well-being. The independent economic value screen does nothing to tell us whether that's the case.

Making the "economic" component of the value requirement do more useful screening is also unlikely to work. A general definition of "economic" value—that is, the definition that economists might employ—would encompass anything that has business value to a firm,[186] including keeping embarrassing (or even fraudulent) information from reaching the public.[187] It would thus cover trade secrets with both positive and negative social value. Of course, one could imagine narrower definitions.

Graves & Katyal, *supra* note 4, at 1406 (suggesting that economic value may allow courts to address overreliance on trade secrecy law in nontraditional contexts).

185 *See supra* Section I.B.

186 *See* Hrdy, *supra* note 72, at 570–71 (noting that "economic" is an "extremely broad term," *id.* at 570, and that economic value may be generated in a variety of ways, including from "early-stage research and 'negative know-how' (knowledge of what not to do), from licensing information to others for use, and even from intentionally hiding the information to avoid competing with a business's other product lines," *id.* at 571 (footnotes omitted)).

187 An example of this is Microsoft's attempt to claim employee diversity data as trade secrets. Moussouris v. Microsoft Corp., No. 15-cv-1483, 2018 WL 1159251, at *10 (W.D. Wash. Feb. 16, 2018), *report and recommendation adopted by* No. 15-cv-1483, 2018 WL 1157997 (W.D. Wash. Mar. 1, 2018). While Microsoft argued otherwise, many speculated that its real reason for seeking trade secret protection was to prevent its embarrassingly low diversity numbers from becoming public. *See, e.g.*, Jamillah Bowman Williams, *Why Companies Shouldn't Be Allowed to Treat Their Diversity Numbers as Trade Secrets*, HARV. BUS. REV. (Feb. 15, 2019), https://hbr.org/2019/02/why-companies-shouldnt-be-allowed-to-treat-their-diversity-numbers-as-trade-secrets [https://perma.cc/9UN4-TK3C].

Hrdy, for example, suggests that only competitive market value, and not reputational value, should count as economic value for trade secrecy purposes.[188] In a similar vein, recent cases assessing whether agencies properly withheld confidential commercial information under FOIA Exemption 4 suggest a more exacting view of the term "commercial."[189] These narrower definitions might make it likelier that trade secrecy protection would primarily apply to information with some positive social value. Information about increasing manufacturing efficiency, for instance, is perhaps more likely to have positive social value than information about employee diversity. But it would be difficult to cabin the rule in a way that would make it an effective screen—particularly for technical subject matter.

Take the algorithm example. Any reasonable definition of "economic" would include (potentially) discriminatory algorithms because the algorithm itself has potential business value. And, of course, it is impossible to know at the time the right is asserted whether the algorithm is biased or not. Similarly, it is hard to argue that the composition of fracking fluids has no potential commercial value—even if it has environmental consequences. Even for nontechnical business information, drawing a line between reputational versus commercial harm would be hard to do and easy to manipulate. Firms could persuasively claim—and they do[190]—that hiring, salary, or pricing data are important to the firm's competitive opportunities to hire workers or price goods. Ultimately, the problem is that the same information could be (a) competitively important to the firm, or (b) reputationally damaging to the firm, or (c) both, depending upon the precise content of the information. And it is very difficult to know the truth of the matter until the information is revealed. On this analysis, trade secrecy law's doctrinal screens turn out to be good proxies for private value,

188 Hrdy, *supra* note 72, at 599–602.

189 *See, e.g.*, Citizens for Resp. & Ethics in Wash. v. U.S. Dep't of Just., 58 F.4th 1255, 1264 (D.C. Cir. 2023) (holding that agency withholding of the names of pentobarbital suppliers for federal executions was not "commercial" information just because it could subject the contractors to "public scrutiny following disclosure"); N.Y. Times Co. v. U.S. FDA, 529 F. Supp. 3d 260, 276–79 (S.D.N.Y. 2021) (rejecting defendant's claim that "customer complaints about the physical characteristics or effects of Juul's products" are "commercial" information just because they "pertain to or are related to commerce," *id.* at 279). *See generally* Deepa Varadarajan, *Narrowing FOIA's Exemption for Business Secrets*, 123 MICH. L. REV. ONLINE 1 (2024).

190 *See, e.g.*, Defendant Department of Labor's Bellwether Motion for Summary Judgment at 15–16, Ctr. for Investigative Reporting v. U.S. Dep't of Lab., 2023 WL 8879244 (N.D. Cal. Dec. 22, 2023) (No. 22-cv-07182) (asserting that the companies do not wish to disclose their EEO-1 diversity data to protect "staffing strategies" and "personnel activities," among other reasons, *id.* at 16).

which policymakers shouldn't care much about, and poor proxies for social value, which policymakers do care about.

B. The Information Paradox

Existing doctrinal screens are not effective at separating positive and negative social value trade secrets.[191] But perhaps that is merely because the law is not appropriately designed. Would better-calibrated doctrinal screens, keyed to different trade secret characteristics, perform this sorting role more effectively?

Unfortunately, we think the answer is likely to be no. There is a fundamental problem with attempting to use doctrinal screens to separate positive and negative social value trade secrets. The problem lies with the unavailability of suitable doctrinal proxies. As we explained above, several legal disciplines use doctrinal proxies to perform this screening function.[192] IP law itself offers multiple examples. Copyrights can be claimed only for "original works of authorship,"[193] and inventions must be novel and nonobvious to be patentable.[194] "Original," "new," and "nonobvious" are sensible (if imperfect) proxies for whether a work of authorship or an invention will actually produce positive social value.[195] This way, authors and inventors are encouraged to pursue new and varied ideas, and they won't be able to claim exclusive rights to stuff that we already have.[196] Trademark law has its own set of doctrinal screens related to distinctiveness that are meant to sort socially valuable marks from socially costly ones.[197] Trademark law encourages firms to choose marks that will help consumers find the goods they want while discouraging firms from choosing marks that will excessively burden competition.[198] We don't expect these regimes to generate the correct answers all the time, but we do think that they operate as reasonably good proxies for socially valuable and socially costly rights.

---

191 *See supra* Section II.A.

192 *See supra* Section II.A.

193 17 U.S.C. § 102(a) (2018) ("Copyright protection subsists, in accordance with this title, in original works of authorship fixed in any tangible medium of expression . . . .").

194 *See* 35 U.S.C. §§ 102–103 (2018).

195 *See supra* Section I.A.

196 *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 429 (1984) ("[Copyright] is intended to motivate the creative activity of authors and inventors by the provision of a special reward, and to allow the public access to the products of their genius after the limited period of exclusive control has expired."); Bilski v. Kappos, 561 U.S. 593, 609 (2010) (noting that patent law seeks to balance "stimulating innovation by protecting inventors and impeding progress by granting patents when not justified by the statutory design").

197 *See supra* text accompanying notes 155–57.

198 *See supra* text accompanying notes 155–57.

But these sorts of reasonable proxies are simply unavailable for trade secrets. If a trade secret right protects socially beneficial information that wouldn't have been created absent the right, then society benefits from secrecy.[199] But if the right protects socially harmful information, then society benefits from disclosure, because it can do something about the wrongful behavior. Unfortunately, the law offers no good proxies for gauging social welfare effects because it is often very hard to know, at the time trade secret rights are asserted, whether the underlying information is beneficial or harmful. We're left with little more than "allow trade secrets when they're good for social welfare, and don't when they are bad for it."

To see why, return to our initial example of a music-matching algorithm developed by a streaming service—one that allows customers to hear the songs they most want to hear.[200] As we explained, the algorithm cannot be copyrighted or patented, leading the firm to treat the algorithm as a trade secret to prevent copying that would undermine the service's incentives to develop it.[201] But if the service designed the algorithm to help it pay lower royalties to musicians or in ways that discriminate against independent artists, minorities, or competitors, then the algorithm could allow the firm to secretly violate state and federal antidiscrimination, trade, and competition laws. In this scenario, the incentive benefits of secrecy may be dwarfed by its social costs.[202]

The problem is that at the time the trade secret or confidential information claim is asserted, we are unlikely to know which of these sorts of algorithms we're dealing with. Is it the socially beneficial one or the socially harmful one? In a number of contexts, we can't know, and, more importantly, we can't predict. In virtually all of the examples of troublesome trade secrets described in Part I, we can easily imagine a situation in which the right is protecting socially valuable information that might not exist but for the secret. We want search engine algorithms to be a protectable trade secret, *unless* they violate antitrust law, and we want bail algorithms to be secret (maybe), *unless* they're discriminatory.[203] Without the trade secrecy, we're less likely to get the

199 *See supra* Section I.A.

200 *See supra* text accompanying notes 6–10.

201 *See supra* text accompanying notes 7–8.

202 *See supra* text accompanying notes 9–10.

203 It might be the case that we don't want bail algorithms (or any algorithms used in the criminal justice context) to be secret, because we think that the stakes are so high that everyone should have access to them. If that's true, though, then we need to commit to other incentive mechanisms to ensure that they exist. Of course, it might also be the case that we don't want any such algorithms to exist in the first place. We take no position on these claims. For fuller discussion of these issues, see Rowe & Prior, *supra* note 126, and Ngozi Okidegbe, *To Democratize Algorithms*, 69 UCLA L. REV. 1688 (2023).

algorithms in the first place, but without broader disclosure, we're less likely to know if they're socially harmful (or perhaps even illegal). Similarly, we want fracking compounds to be secret, *unless* they're destroying the environment. We want clinical trial data for pharmaceuticals to be secret, *unless* they disclose dangers to public health. Unfortunately, we have no way of predicting at the time the rights are asserted which ones we're dealing with. This is trade secrecy's information paradox.

Our argument is a version of Kenneth Arrow's famous "Information Paradox."[204] Imagine, for example, an author has an idea for a movie that she wants to pitch to a studio. It is just an idea, so it cannot be copyrighted. The author wants to be paid for her idea, but the studio only wants to pay for good ideas. This is the paradox. Before the author discloses the idea, the studio doesn't know whether it is good so the studio is unwilling to invest in it. Once the author discloses the idea, however, the studio has what it wants (it knows the idea), and there is no reason to pay the author. The situation in trade secret law is analogous.[205] The law should allow firms to keep good information secret and out of competitors' hands, but bad information should not be protected from disclosure. The problem is that it's hard to know whether the information is good or bad until it is disclosed more broadly for meaningful assessment and scrutiny. Once the information is disclosed, however, the firm asserting the right has nothing left to protect.

It is possible to overcome Arrow's Information Paradox,[206] and it might be possible to overcome trade secret's information paradox, but we are skeptical. As we discuss further in Part IV, one solution might seem to be some type of *in camera* trade secret review.[207] If a criminal defendant files a motion to disclose the details of a sentencing algorithm, the court should review the algorithm (in secret!) to determine whether it is, in fact, biased. If it is, the algorithm is disclosed to the

204 *See* Arrow, *supra* note 29, at 615.

205 And in the run-of-the-mill trade secrecy case, trade secret law—like other areas of IP—is often regarded as a solution to Arrow's Information Paradox. *See supra* text accompanying note 30.

206 *See* Burstein, *supra* note 29, at 247–74 (noting that, while the conventional legal solution to the information paradox is a grant of IP rights, information holders can also use the characteristics of the information, contractual and norms-based mechanisms, and other legal and business strategies to exchange information while also protecting it).

207 *See, e.g.*, Loop AI Labs Inc. v. Gatti, 195 F. Supp. 3d 1107, 1112 (N.D. Cal. 2016) (noting that California law requires courts to "'preserve the secrecy of an alleged trade secret by reasonable means,' including . . . holding in camera hearings" (quoting CAL. CIV. CODE § 3426.5 (West 2016))); Hayden v. Int'l Bus. Machs. Corp., No. 21-cv-2485, 2023 WL 4622914, at *13 (S.D.N.Y. July 14, 2023) (conducting an *in camera* review of contested material and determining that it was probative on the issue of trade secret misappropriation).

defense (and presumably the public); if it is not, the algorithm remains secret. Perhaps the defense could even be consulted in a more limited fashion, under obligations of secrecy.[208] Or, analogously, when a fracking company discloses the chemicals it uses to the EPA, the agency determines whether those chemicals are harmful to human health. If so, it releases detailed information regarding the chemicals to the public (perhaps even proactively, in absence of a specific FOIA request).[209] If not, the information stays within the agency.

This might seem like an attractive state of affairs—careful, confidential review of the underlying information, followed by a determination as to whether the public would be better served by the information being kept secret or becoming public. But as the description above should indicate, it is hard to imagine this arrangement being implemented, at least for many of the examples we have described. Notice that we have returned to the problem of retail analysis that the law tries to avoid. The fundamental problem is epistemic. How will a court be able to determine, on its own, whether an algorithm is biased? That can be an enormously challenging and technical question, with an answer only discernable by experts after lengthy study.[210] An agency like the EPA might seem better positioned to determine whether the fracking chemicals are harmful, and indeed the agency makes that type of decision frequently.[211] Similarly, the FAA may be able to evaluate the safety of Boeing's flight control system redesign, and OSHA may be able to evaluate the severity of worker injury information it receives

208 *See infra* Section IV.D (discussing such proposals in the criminal justice context).

209 *See* Morten, *supra* note 4 (discussing the benefits of proactive disclosure by agencies over ad hoc disclosure pursuant to individual FOIA requests).

210 This is especially true for machine-learning programs which operate through deep neural networks. Mariano-Florentino Cuéllar & Aziz Z. Huq, *Privacy's Political Economy and the State of Machine Learning: An Essay in Honor of Stephen J. Schulhofer*, 76 N.Y.U. ANN. SURV. AM. L. 317, 331 (2021) (noting that machine-learning algorithms "can be opaque" because they are "not explainable in human language" or because they are shielded by trade secrecy law (quoting Tal Z. Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503, 1519)). However, it is possible to design more understandable algorithms, such as decision trees which allow data to be shown in an intelligible way. *See* Deven R. Desai & Joshua A. Kroll, *Trust but Verify: A Guide to Algorithms and the Law*, 31 HARV. J.L. & TECH. 1, 53 (2017); STUART J. RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH 657 (4th ed. 2021).

211 *See, e.g.*, EPA, HYDRAULIC FRACTURING FOR OIL AND GAS: IMPACTS FROM THE HYDRAULIC FRACTURING WATER CYCLE ON DRINKING WATER RESOURCES IN THE UNITED STATES, EXECUTIVE SUMMARY 38–39 (2016) (summarizing EPA's findings on potential hazards from chemicals used in fracking); Hiroko Tabuchi, *E.P.A Approved Toxic Chemicals for Fracking a Decade Ago, New Files Show*, N.Y. TIMES (Oct. 20, 2021), https://www.nytimes.com/2021/07/12/climate/epa-pfas-fracking-forever-chemicals.html [https://perma.cc/NF2S-P4AE] (noting that, in 2011, EPA identified serious health risks associated with the chemicals used in fracking).

from various employers, and the FDA may be able to assess the efficacy of a new drug based on submitted clinical trial data.

But as the examples provided in Part I (and numerous others) illustrate, agencies are hardly infallible.[212] Indeed, that is the whole point of public disclosure: independent scientists and journalists might (and often do)[213] catch things that an agency misses. Even if we believed regulators could be able to make the correct determinations with sufficient time and resources, the scope of federal and state regulatory oversight would have to increase significantly to be able to accurately assess the social value of every asserted trade secret. Regulatory scrutiny is only a full solution if we believe that regulators are perfect and infallible. FOIA and other public disclosure mechanisms are living proof that we do not hold such a belief.

Contrast trade secrecy's approach with how other areas of IP law decide these types of doctrinal screening questions. When an inventor applies for a patent, for instance, the PTO examiner who decides whether or not to grant the patent has a lot of information at her disposal.[214] The patent indicates precisely what is being claimed,[215] and the application must necessarily include substantial information about what, if anything, makes the invention new, nonobvious, useful, and so forth.[216] The examiner is a specialist in the patent's particular scientific or technological field, and she is well positioned to evaluate the nature of the contribution that it makes.[217] While she may not know whether a particular drug, for example, will be especially successful at curing a disease, she will be able to apply, more or less successfully, the law's

212 *See supra* Section I.B.

213 *See* Morten, *supra* note 4, at 1340–43 (discussing several examples).

214 Patent applications must include a specification, a drawing, and an inventor's oath. 35 U.S.C. § 111(a)(2) (2018). Patent applications must demonstrate satisfaction of several patentability requirements. *See, e.g.*, 35 U.S.C. §§ 101–103, 112 (2018) (establishing requirements of patentable subject matter, utility, novelty, nonobviousness, enablement, and written description).

215 *See* 37 C.F.R. § 1.75(a) (2023) ("The [patent] specification must conclude with a claim particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention or discovery.").

216 *See* 37 C.F.R. § 1.71(a)–(b) (2023) ("The specification must include a written description of the invention or discovery and of the manner and process of making and using the same, and is required to be in such full, clear, concise, and exact terms as to enable any person skilled in the art or science to which the invention or discovery appertains, or with which it is most nearly connected, to make and use the same . . . . The specification must set forth the precise invention for which a patent is solicited, in such a manner as to distinguish it from other inventions and from what is old. It must describe completely a specific embodiment of the process, machine, manufacture, composition of matter or improvement invented, and must explain the mode of operation or principle whenever applicable.").

217 *See* MENELL ET AL., *supra* note 69, at 179.

proxies for positive social value patents—novelty, nonobviousness, and the like.

Moreover, when an examiner evaluates whether a patent or trademark application should be granted, most of the relevant information is available on the face of the application. The examiner need not look further than the four corners of the application to determine whether the invention is enabled,[218] or whether the trademark is descriptive or arbitrary.[219] Determining whether an invention is novel can certainly require additional research, but the patent often provides a starting point by listing some relevant prior inventions.[220] And the remaining relevant information is typically found in other patents.[221] In the hands of an expert decisionmaker, screening these types of IP rights is a manageable task.

For many types of trade secrets, however, the relevant information is not available on the face of any document. Rather, it is buried deep within the data, the chemical formula, or the computer code that comprises the trade secret.[222] Only careful, skillful analysis of that data or code can reveal whether the trade secret has positive social value (and thus should be protected) or negative social value (and thus should be revealed).[223] This type of analysis could take months or years; indeed, experts might easily disagree about the right answer, and even more time and effort might be required to resolve the question. This is precisely why it can be important for negative-value trade secrets to be disclosed to the public: only careful scrutiny by a wide-ranging community of experts can expose the insidious nature of the information.[224]

Yet this also means that it is impossible to predict whether a particular trade secret is harmful (and thus must be made available to the

218 *See* 35 U.S.C. § 112.

219 *See* 37 C.F.R. § 2.32(a)(6), (c) (2023) ("The application [for a trademark] must . . . include . . . [a] list of the particular goods or services on or in connection with which the applicant uses or intends to use the mark . . . [and] must include a drawing that [constitutes a substantially exact representation of the mark].").

220 *See* Mark A. Lemley & Bhaven Sampat, *Examiner Characteristics and Patent Office Outcomes*, 94 REV. ECON. & STAT. 817, 818 (2012).

221 *See id.*

222 *See, e.g.*, Melissa Hamilton, *The Biased Algorithm: Evidence of Disparate Impact on Hispanics*, 56 AM. CRIM. L. REV. 1553, 1558 (2019) (explaining how trade secrets can be proprietary algorithmic instruments which are not transparent about what is input into the software or how the outputs are generated or quantified).

223 *See* Desai & Kroll, *supra* note 210, at 46 ("The use of software by the private sector in regulated industries raises a tension between trade secrets and the need to know whether a system adheres to agreed-upon or required standards.").

224 *See* Hamilton, *supra* note 222, at 1558–59 (noting that many observers are calling for third-party auditing of algorithms and arguing that "cross-disciplinary sharing is necessary because of difficulties in translation where data scientists are often not trained in law and policy," *id.* at 1559).

public) or helpful (and thus should be protected to incentivize its creation) without first revealing it more broadly.[225] This is trade secret law's information paradox. And in practical terms it is surprisingly difficult to overcome.

III. COSTLY SCREENS AS SOLUTION?

Doctrinal screens are not the only available mechanism for policymakers trying to limit rights to socially valuable contexts. Another mechanism the law uses to separate the wheat from the chaff is to impose costs—financial or otherwise—that will fall disproportionately on the chaff. By making the chaff more costly, private actors will be dissuaded from engaging in the behavior that leads to the chaff in the first place. This mechanism is known as a "costly screen."[226] The cost is meant to screen out some undesirable behavior or undesirable legal right.[227]

In this Part, we show that trade secret law contains features that plausibly function as costly screens.[228] The reasonable secrecy efforts requirement, for example, imposes costs on claimants that might prevent them from obtaining (and maintaining) rights when the private value of doing so is low. We argue, however, that neither the law's existing costly screens nor any set of new ones could meaningfully eliminate socially harmful trade secrets. The problem is that the social harm that would be averted from disclosure is exactly what makes the right privately valuable to the claimant.

A. How Costly Screens Work

Despite their technical-sounding definition, costly screens are quite common in law and legal theory.[229] A pollution tax, which

225 *See* Desai & Kroll, *supra* note 210, at 56 ("Because software and data can be treated as trade secrets, trade secret law clashes with the ability to know whether software is operating as it should and by extension trade secret law can interfere with legal-political accountability . . . .").

226 *See generally* Fagundes & Masur, *supra* note 26; Masur, *supra* note 26.

227 *See* Fagundes & Masur, *supra* note 26, at 683–85; Masur, *supra* note 26, at 690; *see also* Deepa Varadarajan, *Forfeiting IP*, 59 AM. BUS. L.J. 175, 209 (2022) ("Costly screens can eliminate these IP rights that needlessly create hurdles for other innovators. Namely, the goal of a costly screen is to reduce the number of IP rights with low private and social value—'bad' IP rights—without deterring those that are likely to have high social value—'good' IP rights. The key question, then, is whether a particular costly screen is likely to deter the bad without deterring the good." (footnote omitted)).

228 *See infra* Section III.B.

229 *See* Masur, *supra* note 26, at 717 (explaining how costly screens may operate across a variety of administrative contexts, including "due process protections for employees subject only to 'for-cause' termination and summary-process evictions; the obtaining of

requires a polluter to pay some fee per ton of pollution that it emits, is a type of costly screen.[230] The desire to avoid the tax should cause the polluter to reduce the amount of pollution it emits or to avoid it entirely, thereby curbing the undesirable behavior.[231] Even more conventional types of pollution control, like requiring polluters to install pollution-abating technologies on their smokestacks, function as costly screens.[232] Technologies, like scrubbers, come with some cost,[233] and a desire to avoid paying that cost should cause some marginal polluters to reduce or eliminate their pollution.[234]

For a costly screen to work, the cost must either be applied directly—to the undesirable thing or behavior or legal right—or indirectly, to something correlated with it. In the examples above, for instance, the cost is applied directly to pollution—the undesirable thing. One could also imagine a tax applied to the burning of coal.[235] While burning coal is not necessarily undesirable in and of itself, the pollution it generates certainly is. In this way, the behavior being taxed—burning coal—is highly correlated with the undesirable thing to be deterred: pollution.

Sometimes, though, it is impossible to isolate the undesirable thing or behavior with a costly screen because some versions of the behavior are socially valuable. In that situation, a costly screen can be leveled against an entire class of things. Patent law provides a good example. A patent applicant must pay tens of thousands of dollars in fees and costs to obtain a valid patent from the PTO.[236] These costs are

---

pollution permits; and numerous types of immigration visas, as well as citizenship status and even residence within the United States").

230 *See, e.g.*, 26 U.S.C. § 4681 (2018) (providing that Congress may tax chlorinated fluorocarbons (CFCs) in order to reduce the usage of these stratospheric ozone depleting chemicals).

231 *See* Fagundes & Masur, *supra* note 26, at 683 (explaining that a regulator may address the social costs of pollution by imposing a permit fee).

232 *See* Masur, *supra* note 26, at 721–24 (explaining how pollution-controlling devices function as costly screens).

233 *See id.* at 722 ("The pollution-controlling devices that firms must install are certainly expensive . . . .").

234 *See id.* ("[T]he high cost of compliance with environmental laws can . . . weed[] out those polluting activities that may not be cost-benefit justified, or at least may stray close to the borderline.").

235 *See, e.g.*, Mapco, Inc. v. Grunder, 470 F. Supp. 401, 408–09 (N.D. Ohio 1979) (finding that an Ohio taxing scheme had the practical effect of inverting the natural coal market by artificially making low-sulfur coal less desirable than high-sulfur coal by taxing coal on a sliding scale inversely related to the coal's sulfur content).

236 *See* Fagundes & Masur, *supra* note 26, at 685 ("For patent applicants, the process of patent examination is costly. The average patent applicant will pay more than $20,000 to obtain a patent, and that figure can be much higher for patents in complex technological fields.").

applied to all patents, since there is no obvious way for the PTO to apply higher costs to bad patents only.[237] These costs are not directly connected with any undesirable behavior or legal right that one wishes to deter. But these costs might still be correlated with those undesirables in a way that allows them to be screened out. To see how, note that a costly screen operates according to private value, not social value.[238] The firm or individual faced with the screen must decide whether to engage in the relevant behavior or acquire the relevant legal right, and they will do so only if the private value of the right exceeds the cost of the screen.[239] The typical corporate actor will not care if their actions benefit society—just that the firm benefits.[240] Thus, costly screens will have little to no effect on actions or rights with high private value.[241] They will only affect actions whose private value is lower than the cost of the screen.[242]

With respect to patent fees, then, if obtaining a patent cost about $30,000 in various fees, an inventor who believed that the value of the right was only $20,000 wouldn't bother getting the patent. However, if the fees were only $10,000, she would.[243] Or imagine a situation in which trademark law made it much more expensive to get a descriptive trademark than a fanciful one.[244] If the claimant was basically indifferent between the descriptive mark and the fanciful one, they would choose the fanciful one to avoid the fee. This would be socially beneficial because fanciful marks impose fewer competition costs than do descriptive marks.[245] In both of these examples, a costly screen that is leveled against a class of things would push the claimant into the socially valuable decision—not because the claimant necessarily cared about social value, but because it cared about private value.

In this way, costly screens eliminate low private value rights. And the costly screen's effectiveness will be determined by whether the low

237 *See id.* at 685–86.

238 *See id.* at 692 (explaining that private value indicates what the IP right is worth to the IP holder and that social value indicates what the IP right is worth to social welfare at large).

239 *Id.* at 680.

240 *See* Masur, *supra* note 26, at 699.

241 *See* Buccafusco, Lemley & Masur, *supra* note 26, at 92 ("For high private value rights, costly screens are irrelevant. If the rights are highly valuable to their potential owner, the owner will invest the money to obtain them regardless of the cost.").

242 *See id.* ("[I]f the rights have low value to their owners, the costly screen will deter the putative owner from obtaining the right in the first place.").

243 *See* Fagundes & Masur, *supra* note 26, at 680 (explaining that the patent examination process "deters applicants from seeking patents when the value of the exclusive right is less than the price of overcoming the screen").

244 Buccafusco, Masur & McKenna, *supra* note 26, at 442.

245 *Id.* at 464–66.

private value rights tend to have positive or negative social value.[246] If they have negative social value, then eliminating them will benefit society. If they have positive social value, then eliminating them will be harmful to society. And if they are mixed, the results will be mixed. Accordingly, some of us (with various co-authors) have argued in past work that (1) almost all low private value patents have negative social value, and thus costly screens should be applied to both utility[247] and design[248] patents; (2) many low private value copyrights have positive social value, and thus costly screens would be unwise for copyrights;[249] and (3) certain types of low private value trademarks have negative social value, and thus these trademarks should be subjected to a costly screen.[250]

B. Costly Trade Secret Screens

What, then, of costly screens and trade secrets? As an initial matter, relatively few—or perhaps even zero—of the bad trade secrets described above in Part I are low private value.[251] Firms that have developed proprietary algorithms and have developed a substantial market share in those algorithms have a strong incentive not to disclose the algorithms and risk their business.[252] The same is true for firms that develop fracking fluids or firms that engage in clinical trials to test the safety and efficacy of new drugs. The demographic employment data that Google and similarly situated firms hold is also highly valuable to them, or else they would have released it on their own already. That information might be valuable because Google has figured out a key to hiring efficiently, or it might be valuable because the demographic data would be highly embarrassing to a firm supposedly committed to diversity.[253] Or both could be true. None of these trade secrets are

246 *See* Buccafusco, Lemley & Masur, *supra* note 26, at 94 ("Accordingly, costly screens are appropriate when the number of potential low private value/negative social value rights . . . is high and the number of potential low private value/positive social value rights . . . is low, and they are counterproductive when the reverse is true.").

247 *See* Masur, *supra* note 26, at 712.

248 Buccafusco, Lemley & Masur, *supra* note 26, at 109.

249 *See* Fagundes & Masur, *supra* note 26, at 705–06.

250 *See* Buccafusco, Masur & McKenna, *supra* note 26, at 486.

251 *See supra* Section I.B.

252 *See* Masur, *supra* note 26, at 689 (explaining that high private value inventions can include inventions that "lead to blocking [other uses] and allow their owners to extract significant rents"); Bloch-Wehba, *supra* note 4, at 1289 (noting that vendors of proprietary algorithms may be reluctant to disclose them).

253 *See* Williams, *supra* note 4, at 1691–92 (highlighting the pressure Google received in the past for a lack of diversity); Ellen McGirt, *An Inside Look at How Google Is Embracing Diversity*, FORTUNE (Jan. 20, 2017, 6:30 AM EST), https://fortune.com/longform/google-diversity/ [https://perma.cc/RMJ9-SYRA] (emphasizing Google's commitment to

being asserted for no particular reason, or for modest nuisance value, or any such rationale.[254] All of them have meaningful business worth to the firm.[255]

Further, they have all, in some sense, passed a type of costly screen already. First, trade secret law imposes a costly screen through its reasonable secrecy efforts requirement. A firm must undertake reasonable efforts to protect the secrecy of information it wants to claim as a trade secret.[256] For example, we could imagine a firm erecting expensive walls to prevent competitors from learning its manufacturing process. Presumably, the firm would only do so when the value of its secrets exceeds the cost of building walls.[257] However, most secrecy efforts are not that costly, and over time they are getting cheaper—particularly as courts focus their assessment on contractual secrecy efforts like nondisclosure agreements, rather than physical restrictions like walls or vaults.[258] In many cases, having reasonable computer security and password protections on sensitive files and imposing nondisclosure agreements on employees and business collaborators are sufficient to comply with the rule.[259] But even these efforts are not free, particularly for larger firms storing substantial quantities of sensitive data and engaging with large numbers of employees and other business collaborators (e.g., vendors, subcontractors, etc.).[260] In addition, the firms involved have been willing to expend resources to assert their trade secrecy claims in court, a process that ranges from moderately to extremely expensive.[261] Or to the extent that these claims arise in the FOIA context, firms have been willing to expend resources in resisting

diversity); Johan Moreno, *Google Slashes Diversity Programs After Big Promises*, FORBES (Jan. 2, 2024, 7:21 PM EST), https://www.forbes.com/sites/johanmoreno/2023/12/31/google-slashes-diversity-programs-after-big-promises [https://perma.cc/BGW7-KUFJ] (outlining Google's cuts to its diversity programs).

254 *See* Masur, *supra* note 26, at 699 (explaining that firms seek IP rights for high private value inventions); Buccafusco, Lemley & Masur, *supra* note 26, at 89–94.

255 *See* Masur, *supra* note 26, at 688–90.

256 UNIF. TRADE SECRETS ACT § 1(4) (UNIF. L. COMM'N 1985) (requiring reasonable efforts as an element of a trade secret); *see also supra* Section I.A.

257 *See* Lemley, *supra* note 7, at 334–35 (explaining that without trade secret protections, a firm might construct even extremely costly defenses to protect valuable trade secrets).

258 *See* Varadarajan, *supra* note 67, at 390–91.

259 *See id.* at 373.

260 *See* Lemley, *supra* note 7, at 333–34; *cf.* Bone, *A New Look*, *supra* note 31, at 273–81 (noting that enforcement and licensing costs of trade secrets can be especially high).

261 On average, trade secret litigation costs can range from $425,000 to $2,950,000. Bone, *The (Still) Shaky*, *supra* note 31, at 1809 n.33 (citing AM. INTELL. PROP. L. ASS'N, REPORT OF THE ECONOMIC SURVEY: 2013, at 36 (2013)).

agency disclosure—perhaps even culminating in a "reverse FOIA" lawsuit to stop the agency's release of information.[262]

It might be the case that these costly screens are just too cheap, and if the law boosted the price of trade secrecy, socially harmful behavior would abate. We are doubtful, though. If the law were to impose additional costly screens, they would be unlikely to work at separating wheat from chaff because the good trade secrets are not obviously more privately valuable than the bad ones.[263] For example, if a sentencing algorithm is unbiased, the firm that created it stands to lose money if the algorithm is revealed because it can be copied by competitors.[264] If the algorithm is biased, the firm stands to lose perhaps *even more money* if the bias is revealed and customers no longer wish to use it.[265] In this situation, the "bad" trade secret may be even more privately valuable than the "good" one. The fracking firm faces a similar calculus. Disclosure of the firm's chemical compounds might enable its competitors to eat into its profits, but the firm stands to lose even more if disclosure subjects it to massive fines and civil damages awards from polluting.[266]

All of the above reasons are explanation enough for why costly screens make an awkward fit for trade secrets. But there is a more fundamental reason as well. Legal rights, particularly intellectual property rights, are structurally bundled with the things that they protect.[267] Thus, for instance, a patent on a valuable invention is privately valuable because of the patent—the legal right.[268] It is the patent that allows its

---

262 *See* Varadarajan, *supra* note 78, at 487–88 ("Before releasing information that may be covered by Exemption 4, agencies typically notify submitters and provide them an opportunity to object. [If] an agency disagrees with a submitter's objection and plans to release the information, the submitter can seek to enjoin the agency from releasing that information by filing a 'reverse FOIA' suit." (footnote omitted)); *see, e.g.*, Canadian Com. Corp. v. Dep't of the Air Force, 514 F.3d 37, 39 (D.C. Cir. 2008).

263 *See supra* Section II.B; Buccafusco, Masur & McKenna, *supra* note 26, at 474 (explaining that useful costly screens can rely in part on private judgments about the value of the information or behavior by firms).

264 *See supra* Section I.A.

265 *See supra* Section I.A. Google, for example, suffered a large reputational hit in 2015 when consumers discovered its photo-recognition tool was perpetuating racial stereotypes. Similarly, Google's Translate tool produced results that reflected gender stereotypes. Li Zhou, *Is Your Software Racist?*, POLITICO (Feb. 8, 2018, 6:42 PM EST), https://www.politico.com/agenda/story/2018/02/07/algorithmic-bias-software-recommendations-000631/ [https://perma.cc/4PXJ-SYXJ].

266 *See supra* subsection II.A.2.

267 *See* Lisa Larrimore Ouellette, *Patentable Subject Matter and Nonpatent Innovation Incentives*, 5 U.C. IRVINE L. REV. 1115, 1131 (2015) (stating that "separating the value of patents from the value of the underlying [invention] is difficult, and separating the value of patent-like incentives from patents themselves is even more challenging").

268 *See id.* at 1131.

owner to collect significant profits by selling the invention.[269] And the social value of the patent derives from the fact that it generates incentives for someone to create the underlying invention—the thing that is protected by the legal right.[270] The patent does not exist without the invention.[271] And in many cases where there would not be adequate incentives to develop the invention without the reward of a patent, the invention does not exist without the patent either.[272] As a result, imposing a costly screen that eliminates the patent will, in many cases, eliminate the underlying invention as well.[273] This is why it is important that no highly socially valuable inventions are protected by low private value patent rights; in that situation, a costly screen could be very harmful to society.[274]

Now consider the structure of trade secrets. For the bad trade secrets described above, there is an underlying piece of information—e.g., an algorithm, employment data, chemical composition data, or drug safety and efficacy data.[275] This information has positive private value to the firm that controls it if and only if the firm can keep the information secret.[276] If the information must be publicly disclosed, its private value becomes zero or negative (or very small).[277] For instance, if the bail algorithm is publicly disclosed, it can be copied, and its value to the firm largely disappears or even becomes negative if the algorithm turns out to be biased. Similarly, Google presumably receives some informational benefit from keeping track of the demographics of its workforce.[278] But if it must disclose that information, the result could be a severe reputational penalty.[279]

On the other hand, the sort of information protected by bad trade secrets likely has positive social value if and only if it is publicly

269 *See* Masur, *supra* note 26, at 702–03; Buccafusco, Lemley & Masur, *supra* note 26, at 105.

270 *See* Fagundes & Masur, *supra* note 26, at 701 ("With very few exceptions, any truly novel, commercially relevant invention—that is, any socially productive invention—will give rise to a privately valuable patent on that invention. This is precisely the point of the patent system: patents allow inventors to capture a substantial portion of the wealth created by their inventions." (footnote omitted)); Masur, *supra* note 26, at 690.

271 *See* Fagundes & Masur, *supra* note 26, at 701.

272 *Cf.* Ouellette, *supra* note 267, at 1116, 1125–26, 1141 (explaining that patents incentivize innovation because they offer profit incentives and rewards like supracompetitive prices).

273 *See* Buccafusco, Lemley & Masur, *supra* note 26, at 92.

274 *See id.* at 94.

275 *See supra* Part I.

276 *See* Hrdy, *supra* note 72, at 559.

277 *Id.*

278 *See supra* notes 252–55 and accompanying text.

279 *See supra* notes 252–55 and accompanying text.

disclosed.[280] If the sentencing algorithm remains secret but turns out to be biased, it could do a great deal of social harm by leading to unjust and unnecessary incarceration, and there are few mechanisms by which to correct this injustice.[281] Similarly, if Google is engaging in problematic hiring practices, society only benefits from Google's record-keeping if it can learn who Google is actually hiring and hold the company to account when its actions fall short. And, of course, for the information to be disclosed it must exist in the first place.

Once again, if and only if the information is socially valuable do we want it to exist in the first place and, thus, be covered by a trade secret. If the information is socially harmful, we don't want the secrecy. If a costly screen prevents a firm from obtaining a trade secret on some information, and consequently the firm *does not create or collect the information in the first place*, the result is problematic as a matter of social welfare.[282] If Google recognizes that it can no longer maintain a trade secret in its employment records and thus decides not to collect detailed demographic data regarding its employees, then that data can never see the light of day. If firms do not create sentencing algorithms because they know they will not be able to protect those algorithms, society will never be able to capture the potential benefits from such an invention. Trade secrets unbundle the legal right and the thing that the legal right protects. This is notably different from patent law, where the premise of the analysis was that society would suffer no disadvantage if the underlying low social value invention never came into existence, along with the patent covering it.[283]

This means that costly screens for trade secrets must thread a narrow needle. They will only function properly when the underlying information has meaningful private value to the firm developing it, even if that firm knows it will eventually have to disclose such information. In other words, the firm must be willing to create the underlying information even if it cannot protect it with a trade secret. At the same time, there must not be such great private value if the information were kept secret that the firm will maintain it as a trade secret in the face of a

280 *See supra* Section I.B.

281 *See* Hamilton, *supra* note 222, at 1557, 1559 (stating that a ProPublica study of popular risk analysis tool COMPAS was discriminatory against Black arrestees but "no formal mechanism in the law or in the sciences exists to consistently enforce any form of algorithmic accountability"); *see, e.g.*, Rebecca Wexler, *Code of Silence: How Private Companies Hide Flaws in the Software that Governments Use to Decide Who Goes to Prison and Who Gets Out*, WASH. MONTHLY (June 11, 2017), https://washingtonmonthly.com/2017/06/11/code-of-silence/ [https://perma.cc/K42N-R8PU].

282 *See* Fagundes & Masur, *supra* note 26, at 728 ("The costlier the screen, the more likely it is that [firms] will decline to create [underlying information] where they are skeptical of clearing the value of the screen.").

283 *See* Masur, *supra* note 26, at 689.

costly screen.[284] That is, the information has to be valuable enough to create but not valuable enough to pay to protect. Only under these circumstances will the firm have the necessary incentive to create the information, which will then see the light of day when the costly screen dissuades the firm from claiming a trade secret.[285] Yet in many of the troublesome examples described in Part I,[286] these conditions do not hold. Either the firm would not likely have created the information in the first place if it couldn't have kept it secret or the firm would be willing to pay substantial amounts of money to maintain its secrecy. Thus, a costly screen would inevitably set the rate too high, such that investment in information would be discouraged, or it would set the rate too low, such that socially harmful secrets would still be kept secret.

284 *See* Buccafusco, Lemley & Masur, *supra* note 26, at 94 (explaining that in general, costly screens are meant to reduce the number of low private value IP rights, but are counterproductive when they screen out rights with positive social value); Fagundes & Masur, *supra* note 26, at 728.

285 There may be some situations in which these circumstances are present—for example, in the context of nontechnical business information that would be created or collected by firms anyway. It is possible, for instance, that the mass of confidentiality clauses that firms compel even low-level employees to sign covers information that does not actually have much value to the firms. The firms would have created that information anyway, and they're simply using the confidentiality clause as a cudgel in employment contexts. If that's right, firms might be unwilling to pay costly screens to maintain the asserted confidentiality. To some degree, information that firms collect and assemble regarding employees might get collected and assembled anyway, in response to various government regulations and reporting requirements. Companies are obligated to track and report to the government, for example, workplace injury information and employee demographic data involving job category, ethnicity, race, gender, or veteran status. 29 C.F.R. pt. 1904 (2023); 29 C.F.R. § 1602.7 (2023); 41 C.F.R. § 61-300.11 (2023). Customer complaints might also be created or collected regardless of trade secret protection incentives. Complaints might be valuable for other reasons like improving products and detecting defects or other risks. *See* Janelle Barlow, *Believe It: Complaints Are Gifts*, GLOB. SUPPLY CHAIN REV., Oct. 2009, at 8, 9; 15 U.S.C. § 2064(b) (2018) (requiring companies to report product safety issues like substantially risky defects). Companies might also initially track user data online so they can monetize it, but reach a point where they are collecting data with a purpose that "consists of nothing more than the ability to continue amassing potentially useful data"—in other words, collecting (potentially worthless) data just for the sake of collecting. Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 628 (2014); *see also* Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 426 (2018).

286 *See supra* Section I.B.

IV. INCOMPLETE SOLUTIONS TO TRADE SECRECY'S INFORMATION PARADOX

We have argued that trade secret law reflects a fundamental paradox about the value of disclosing information.[287] When Kenneth Arrow proposed his Information Paradox, it seemed like it would cause large, insoluble challenges. But over time, scholars have learned how parties are able to exchange valuable information with each other even in the absence of IP rights.[288] Perhaps trade secrecy's information paradox will also prove soluble.

We hope so, but we have doubts—at least outside of limited subject matter contexts. Here, we evaluate several potential solutions and explore both their promise and their limitations. One significant challenge to evaluating these options is that doing so requires preexisting normative beliefs about the relative costs and benefits of trade secret law itself. If we make secrets harder to protect, we may undermine investment in information or increase wasteful expenditures on self-help. But if secrets are too easy to protect, we will limit opportunities for oversight and regulation. Which of those is the bigger concern is virtually impossible to know, especially in light of the almost total lack of empirical research on trade secrets.[289] But note, again, that part of the empirical problem arises from the paradox of secrecy itself: How could we ever know whether secrets are doing more harm than good when the relevant information is kept secret?[290]

A. The Inapplicability of Solutions to Arrow's Information Paradox

Consider a paradigmatic example of Arrow's Information Paradox.[291] A biotechnology startup firm has developed a new compound that it believes has important therapeutic effects. But the startup isn't in a position to commercialize the compound. For that, it needs a large pharmaceutical company that specializes in commercialization.

287 *See supra* Part II.

288 *See, e.g.*, Burstein, *supra* note 29.

289 Several recent papers have begun the empirical study of trade secret law, but the field remains nascent. *See, e.g.*, David S. Levine & Christopher B. Seaman, *The DTSA at One: An Empirical Study of the First Year of Litigation Under the Defend Trade Secrets Act*, 53 WAKE FOREST L. REV. 105 (2018); Andrea Contigiani, David H. Hsu & Iwan Barankay, *Trade Secrets and Innovation: Evidence from the "Inevitable Disclosure" Doctrine*, 39 STRATEGIC MGMT. J. 2921 (2018); I.P.L. Png, *Secrecy and Patents: Theory and Evidence from the Uniform Trade Secrets Act*, 2 STRATEGY SCI. 176 (2017); I.P.L. Png, *Law and Innovation: Evidence from State Trade Secrets Laws*, 99 REV. ECON. & STAT. 167 (2017).

290 *See* Orly Lobel, *The DTSA and the New Secrecy Ecology*, 1 BUS. ENTREPRENEURSHIP & TAX L. REV. 369, 376 (2017) ("Because they are secret in nature, empirical research on trade secrets has been inherently difficult to conduct.").

291 This example comes from Burstein, *supra* note 29, at 232–33.

The biotech company can't fully disclose the compound, because if it did, it would give away all of its value. But if the biotech company doesn't disclose the compound at all, the pharma company doesn't know whether it should invest. This is the paradox: disclosure is necessary but impossible.

As scholars have demonstrated, however, firms have a number of solutions to the paradox.[292] They might begin by disclosing general information about the compound based on an initial agreement, and then disclose more information as the two companies decide whether to cooperate.[293] By sequentially revealing information, the biotech firm can give the pharmaceutical company confidence that it has something of value without giving everything away. And the pharmaceutical company can make increasing levels of investment without committing fully. Finally, because many of these interactions arise among repeat players in the market,[294] social norms can discipline firms against bad behavior.[295]

Notably, none of these factors apply to the trade secret contexts we're interested in, such as when a watchdog organization seeks disclosure of a firm's secret algorithm. The organization and the firm aren't looking for ways to cooperate with one another. Rather, their interests are often adverse. The watchdog organization wants to reveal data that reflects poorly on the firm, while the firm would prefer to keep it secret. This also means that social norms are unlikely to inhibit antisocial behavior.

---

292 These solutions include intellectual property rights, contracts, industry norms, and alternative sources of appropriability. Burstein, *supra* note 29, at 258–74 (first citing Robert P. Merges, *A Transactional View of Property Rights*, 20 BERKELEY TECH. L.J. 1477 (2005); then citing Ronald J. Gilson, Charles F. Sabel & Robert E. Scott, *Contracting for Innovation: Vertical Disintegration and Interfirm Collaboration*, 109 COLUM. L. REV. 431 (2009); then citing Wesley M. Cohen & Daniel A. Levinthal, *Innovation and Learning: The Two Faces of R&D*, 99 ECON. J. 569 (1989); then citing Walter W. Powell, Kenneth W. Koput & Laurel Smith-Doerr, *Interorganizational Collaboration and the Locus of Innovation: Networks of Learning in Biotechnology*, 41 ADMIN. SCI. Q. 116 (1996); then citing DAVID J. TEECE, MANAGING INTELLECTUAL CAPITAL: ORGANIZATIONAL, STRATEGIC, AND POLICY DIMENSIONS (2000); then citing Richard C. Levin, Alvin K. Klevorick, Richard R. Nelson & Sidney G. Winter, *Appropriating the Returns from Industrial Research and Development*, 3 BROOKINGS PAPERS ON ECON. ACTIVITY 783 (1987); and then citing Wesley M. Cohen, Richard R. Nelson & John P. Walsh, *Protecting Their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (or Not)* (Nat'l Bureau of Econ. Rsch., Working Paper No. 7552, 2000)).

293 Burstein, *supra* note 29, at 263–66.

294 *See id.* at 270 ("[C]onsolidation in the pharmaceutical industry has left relatively few large firms capable of carrying out the development and marketing necessary to commercialize the products of biotechnological research. These few firms are therefore the primary 'customers' of biotech firms seeking to license their potential targets.").

295 *See id.* ("A firm that divulges private information is not likely to find many entrepreneurs seeking financing from it in the future.").

In addition, partial disclosure of the firm's algorithm won't necessarily help the watchdog organization. It needs complete access to the algorithm to know how it works. Only by understanding how the algorithm treats different inputs can the watchdog organization learn whether the algorithm is generating biased results. So incomplete disclosure doesn't solve the problem.

B. Massively Increasing Regulatory Oversight

Many of the potentially harmful trade secrets we discuss are embodied in information that regulatory agencies like the EPA and Department of Labor already possess.[296] Even if agencies have the inclination to rigorously evaluate the submitted information upon receipt of a FOIA request, they do not have nearly enough resources to do so.

Consider the magnitude of FOIA requests that agencies already receive. The SEC receives more than 12,000 requests per year,[297] while the FDA receives more than 10,000 and the EPA receives slightly fewer than that.[298] While these numbers are much smaller than the number of utility patent applications filed at the PTO annually (approximately 500,000–600,000),[299] so are the agencies' staffs. The PTO employs more than 8,000 examiners to evaluate those patents[300]—a number that some argue is still too small for thorough review.[301] By contrast, the FTC employs five attorneys and five government information specialists to review more than 1,500 annual requests.[302] Massively ramping up regulatory oversight at EPA, FTC, OSHA, FDA, and a host of other agencies would be a truly resource-intensive endeavor.

But it's not just a question of increasing staff. The task that agencies face is, in many respects, monumentally greater than the one faced by the PTO. As we explained above, a PTO examiner must decide whether a submitted application represents a novel and nonobvious invention in a fairly confined field of prior art.[303] These doctrinal

296 *See* Morten, *supra* note 4, at 1340 (noting that federal regulatory agencies hold "oceans of information . . . from the companies they regulate," *id.* at 1333, and "tend to keep corporate secrets secret," *id.* at 1340).

297 *See* Kwoka, *supra* note 103, at 1382.

298 *See id.* at 1388, 1398.

299 *U.S. Patent Statistics Chart Calendar Years 1963–2020*, U.S. PAT. & TRADEMARK OFF. (Sept. 4, 2025, 9:50 PM), https://www.uspto.gov/web/offices/ac/ido/oeip/taf/us_stat.htm [https://perma.cc/228C-TZBS].

300 U.S. PAT. & TRADEMARK OFF., FY 2022 AGENCY FINANCIAL REPORT 20 (2022).

301 Michael D. Frakes & Melissa F. Wasserman, *Does the U.S. Patent and Trademark Office Grant Too Many Bad Patents? Evidence from a Quasi-Experiment*, 67 STAN. L. REV. 613, 673 (2015).

302 FTC, CHIEF FOIA OFFICER REPORT 1 (2023).

303 *See supra* Section II.B.

screens are reasonable proxies for social welfare.[304] But FOIA examiners across a range of agencies have a much harder task, as we noted in Part II.[305] They can't simply apply doctrinal proxies for social value because such proxies do not exist for trade secrets.[306] Instead, they would have to learn and assess whether the underlying information is itself good or bad. Is the claimed algorithm appropriately helping consumers find music, or it is inappropriately discriminating against certain types of artists? This is a serious research question that could require a team of scholars and weeks or months of investigation. Nor is this assessment of the public's interest in learning information something FOIA examiners typically do.[307] To adequately staff administrative agencies and provide adequate training for employees to make these assessments—including at the state agency level—would require public investment on a truly massive scale.[308] We aren't opposed, in principle, to these expenditures, but no one should believe that they are self-evidently politically feasible, especially under current conditions.

C. Disclosure Bonds and Criminal Penalties

In Part III, we evaluated the (in)effectiveness of having trade secret claimants pass additional costly screens to obtain protection. An inverse possibility could involve having parties who request the disclosure of secrets post expensive bonds when information is disclosed. This would condition disclosure on the requesting party's belief that the information will reveal social harm. The requesting party is thus incentivized to request disclosure of the secret only when it thinks that doing so will be worth it.

Thus, for example, a watchdog group desiring release of a firm's fracking data from the EPA might be compelled to post a bond that would be forfeited to the firm if the information turned out not to be socially harmful. The watchdog group would have to make an affirmative showing to the EPA that it had uncovered socially harmful behavior by the fracking firm to avoid losing its money. Such a bond might

304 *See supra* Section II.B.

305 *See supra* Section II.B.

306 *See supra* Section II.B.

307 *See* Morten & Kapczynski, *supra* note 4, at 524 (observing that while these kinds of "balancing tests" that "weigh the public interest in the information being sought against the corporate interest in ongoing secrecy" are "standard in many countries' freedom of information laws," that is not the case in the United States).

308 Indeed, critics of FOIA already note the sizable resources that agencies devote "that could be used to other ends." *Id.* at 527 (noting that "between 2008 and 2017, the FDA spent $305 million on FOIA at $2,653 per request," of which "[u]ser fees recover[ed] only a trivial fraction").

have salutary effects, given that a substantial number of FOIA requests come from market rivals creating nuisances for their competitors.[309] This bond-posting approach might also be easier for agencies to administer than the current FOIA system.[310] Rather than the EPA determining on its own whether the chemicals are harmful, it need only evaluate the watchdog's claim that they are.[311] The challenge, however, is setting the optimal price of the bond. If the price is set too low, requesters will obtain too much information, undermining trade secret law's incentive function.[312] Firms won't be able to trust their secrets with agencies, so they either won't invest in creating that information or they will seek opportunities to avoid providing it.[313] Either outcome is suboptimal. Yet if the price of the bond is set too high, requesters will be discouraged from seeking disclosure. Since the most socially valuable requesters are likely to be nonprofits, any price that would adequately compensate claimants for their losses would likely far exceed the requesters' ability to pay.[314]

Of course, when the law faces the problem of parties without the ability to pay for the harm that they cause, it can resort to criminal sanctions.[315] For example, criminal punishment for copyright infringement could make economic sense when monetary damages won't deter infringers who could never pay for the magnitude of the losses that

309 Kwoka, *supra* note 103, at 1381 (noting that some of the highest-volume FOIA requesters are "information resellers compet[ing] against each other in the private market for public records"). Kwoka and other scholars have expressed various concerns about the limitations and pitfalls of FOIA. *See, e.g.*, Margaret B. Kwoka, *First-Person FOIA*, 127 YALE L.J. 2204 (2018); David E. Pozen, *Freedom of Information Beyond the Freedom of Information Act*, 165 U. PA. L. REV. 1097, 1099 (2017) (observing that FOIA "has proven deficient in significant respects").

310 *See* Kwoka, *supra* note 103, at 1416–20 (highlighting the vast resources that federal agencies must spend to fulfill FOIA requests by businesses); *supra* Section II.B.

311 Of course, we would hope that the EPA would learn of the danger in the first instance, but, as we've shown above, that isn't feasible in many cases. *See supra* Section II.B.

312 Indeed, FOIA already imposes a nominal fee structure, which allows agencies to impose fees for "reasonable standard charges for document search, duplication, and review." 5 U.S.C. § 552(a)(4)(A)(ii)(I) (2018); *see also* Kwoka, *supra* note 103, at 1372–73 (describing FOIA's fee structure).

313 *See supra* Section III.B (explaining that firms may be disincentivized to create information in the first place if it will not be protected and are reluctant to reveal secrets or data that lose value when publicized).

314 FOIA currently imposes a differential fee structure that charges socially valuable requesters less; if a "request is made by an educational or noncommercial scientific institution, whose purpose is scholarly or scientific research; or a representative of the news media," the fees imposed by an agency are limited to duplication charges. § 552(a)(4)(A)(ii)(II). These fees clearly aren't meant to function as bonds, though, because they're far too low to adequately compensate firms for inappropriate disclosure. They are instead better understood as a costly screen on the requesters' side of the equation.

315 *See* Buccafusco & Masur, *supra* note 142, at 309–15.

they cause.[316] Similarly, we could imagine criminal penalties imposed on requesters of trade secrets if it turns out that the disclosed information is not socially harmful but the information is publicized. But this approach seems deeply unpalatable. Criminal penalties for engaging in potentially socially valuable journalism and oversight seem both disproportionate and likely to excessively chill beneficial behavior.[317]

D. Contextualized Limits on Trade Secrecy

As previously discussed in Parts II and III, trade secrecy's information paradox undercuts the ability of one-size-fits-all screens to distinguish beneficial from harmful claims. Alternatively, the law could adopt specific limitations on trade secrets for particular kinds of information or in specific contexts, where the costs of secrecy are especially likely to outweigh its benefits. A number of scholars have advocated for these kinds of context-specific proposals.[318]

In the context of pharmaceuticals, for example, Christopher Morten and Amy Kapczynski argue that the FDA should proactively disclose safety and efficacy data about approved drugs and vaccines.[319] Since drugs and vaccines are protected by patents, firms already have incentives to develop them in the first place. It is far from clear that protecting clinical trial data with trade secrecy provides additional development incentives.[320] Secrecy does, however, prevent meaningful oversight about the potential health risks that approved drugs create.[321] Independent researchers can provide a much-needed check on industry players and regulators.[322] To this end, Morten and Kapczynski argue that proactive disclosure is an optimal path forward—one in which "the FDA should prioritize health researchers over industry actors" and employ "data use agreements to ensure those researchers protect

316 *See id.* at 307.

317 *See id.* at 277 (stating that using criminal sanctions to protect IP can chill important beneficial behavior).

318 *See, e.g.*, Morten & Kapczynski, *supra* note 4; Morten, *supra* note 4; Wexler, *supra* note 4.

319 Morten & Kapczynski, *supra* note 4, at 497–98.

320 *Id.* at 550 (noting the "absence of any study showing conclusively that clinical data secrecy provides significant incentives to innovate").

321 *See id.* at 496 (observing that data secrecy for the drug Vioxx concealed important health risks and resulted in an estimated tens of thousands of deaths because the data was not made available to the scientific community).

322 *Id.* at 497 (describing "an emerging consensus that independent researchers need better access to clinical trial data to keep both the industry and regulators honest and accountable").

legitimate public interests."[323] This approach may not work, however, in other regulatory contexts. As these authors note, the pharmaceutical context specifically offers "fertile conditions . . . that allow clinical trial data publicity to inform the public"—including, for example, "publicly funded scientists with the skills and desire to analyze that data."[324]

Morten has also drawn attention to the ways in which some administrative agencies' enabling statutes allow more flexibility for disclosing confidential information.[325] For example, the National Transportation Safety Board (NTSB) and the National Institutes of Health (NIH) are enabled to disclose some trade secrets when doing so is consistent with their statutory mandates.[326] While this added flexibility means that agencies can release confidential information when they have reason to know that doing so will be socially valuable, it still doesn't solve the problem of when agencies will in fact have such knowledge.

In the criminal justice context, Rebecca Wexler has advocated for similar restrictions on trade secrecy.[327] She argues that trade secrets should not be privileged in criminal proceedings, and judges should permit defendants access to evidence about the algorithms and data used to arrest or prosecute them.[328] This context invites a different set of calculations than pharmaceutical safety and efficacy data. On one hand, many of these algorithms wouldn't otherwise qualify for IP protection, so there is a risk of underproduction in the absence of trade secrecy.[329] On the other hand, the stakes for criminal defendants might be even higher than for people taking pharmaceuticals.[330] And,

323 *Id.* at 500. Data use agreements, which prevent unauthorized dissemination of the data (e.g., outside of peer-reviewed medical journals) or commercial use, have been used by the European Medicines Agency and other entities. *See id.* at 547.

324 *Id.* at 501, 558 (observing that "[i]t is not open data alone, but data publicity in a context where resources and expertise exist to enable intelligible uses of such data, that furthers democratic accountability," *id.* at 501); *see also* Morten, *supra* note 4, at 1352 (suggesting that other agencies, in addition to the FDA, could employ a similar "information publicity" model—"provid[ing] moderated access to corporate secrets subject to both legal and technical limits," like data use agreements, "which dictate which users get access and constrict the uses those users make of that information"—e.g., prohibiting competitive uses).

325 *See* Morten, *supra* note 4, 1382–84.

326 *See* 49 U.S.C. § 1114(b)(3) (2018) (NTSB); 42 U.S.C § 282(i) (2018) (NIH).

327 *See* Wexler, *supra* note 4.

328 *See id.* at 1353.

329 *Id.* at 1364, 1371 (stating that "[t]rade secrecy is a primary intellectual property protection for source code").

330 *See id.* at 1361 (noting that because of the ability of software developers to withhold software information as trade secrets, "[a] death penalty defendant . . . [was] forced to undergo trial without the opportunity to review or challenge the source code of the forensic software used to analyze the evidence against him").

as we've noted above, the adversarial system plays an essential role in uncovering bad behavior in criminal cases, where there is less regulatory oversight.[331] Also, it is likely that even without an explicit trade secret privilege, judges can utilize other safeguards—like "protective orders, sealing, and limited courtroom closures"—to prevent trade secret information from spilling out beyond the view of defendants and their counsel.[332] Ultimately, if algorithms are to play a role in the criminal legal system, perhaps society would be better off if they were developed by governments and paid for with public dollars. Then, secrecy wouldn't be essential for innovation, and the public would be able to scrutinize criminal law's tools.

In the alternative, it might be possible to test certain algorithms for bias without revealing the trade secrets that power them. So-called "black box testing" is a mechanism for examining the behavior of algorithms without "opening" the "black box" of the algorithm itself to examine its inner workings.[333] Instead, the tester feeds the algorithm a series of preselected hypothetical test cases and scrutinizes the algorithm's *output*, rather than its means of arriving at that output.[334] With careful black box testing, an expert can determine whether an algorithm is biased along some dimension of importance.[335] In theory, then, a test would only require the disclosure of the algorithm itself, as an end user might find it, rather than disclosure of the trade secrets that undergird the algorithm.

This is a promising solution for the class of algorithms to which it can be applied. But it is important to note that it is a mechanism for skirting the issue of trade secrets entirely rather than a means of sorting between information that should and should not be protectable as a trade secret. The key feature of black box testing is that it permits the public to learn the relevant information without affecting the incentives of the inventor to develop the trade secret in the first instance. It eliminates the need to determine whether a particular secret should be protectable in the first instance, thereby solving trade secrecy's information paradox. But it does not provide any guidance for those situations in which the discovery of the trade secret is essential to the

331 *See* Wexler, *supra* note 137, at 222–24 (explaining that adversarial adjudication is important for testing the quality of evidence); *see also supra* Section I.B.

332 Wexler, *supra* note 4, at 1395.

333 Srinivas Nidhra & Jagruthi Dondeti, *Black Box and White Box Testing Techniques—A Literature Review*, INT'L J. EMBEDDED SYS. & APPLICATIONS, June 2012, at 29, 29–34.

334 *See* Akanksha Verma, Amita Khatana & Sarika Chaudhary, *A Comparative Study of Black Box Testing and White Box Testing*, INT'L J. COMPUT. SCIS. & ENG'G, Dec. 2017, at 301, 301–02.

335 *See* Nidhra & Dondeti, *supra* note 333, at 33.

evaluation of the trade secret. It is a valuable tactic but only within its limited domain.

Given the challenges of establishing one-size-fits-all screens that can effectively distinguish beneficial versus harmful trade secret claims across the full range of protectable subject matter, perhaps these kinds of context-specific proposals offer the most fruitful path forward. There is a loose analogy to the doctrine of patentable subject matter, in which the Supreme Court has decided that some types of early-stage inventions and discoveries, novel though they may be, should not be entitled to patent protection because it believes the social costs of protecting them will exceed the benefits.[336] Trade secret law could mimic these types of categorical exceptions, though it could do so based on context and type of technology, rather than based on the state of development of the secret. To succeed, however, these proposals would require a marshaling of legislative, judicial, or agency will to change the status quo[337]—no easy feat. Ultimately, while piecemeal solutions may be able to chip away at some aspects of trade secrecy's information paradox, a comprehensive approach to solving this problem remains elusive.

CONCLUSION

By allowing firms to protect valuable secret information that lies beyond the reach of patent and copyright laws, trade secret law encourages innovation that benefits society. Yet firms have also invoked trade secret law to shield socially harmful behavior from public view and regulatory oversight. Firms have invoked the protections of trade secrecy (and its FOIA equivalent) to prevent journalists, watchdog groups, and even criminal defendants from learning about products and services that might be biased, discriminatory, or otherwise harmful to public health and safety.

336 *See* JONATHAN S. MASUR & LISA LARRIMORE OUELLETTE, PATENT LAW: CASES, PROBLEMS, AND MATERIALS 252–53 (3d ed. 2023).

337 *See, e.g.*, Justice in Forensic Algorithms Act of 2021, H.R. 2438, 117th Cong. (2021); Press Release, Mark Takano, Representative, Cong., Reps. Takano and Evans Reintroduce the Justice in Forensic Algorithms Act to Protect Defendants' Due Process Rights in the Criminal Justice System (Apr. 8, 2021), https://takano.house.gov/newsroom/press-releases/reps-takano-and-evans-reintroduce-the-justice-in-forensic-algorithms-act-to-protect-defendants-due-process-rights-in-the-criminal-justice-system [https://perma.cc/3PFX-XJC5]; Morten & Kapczynski, *supra* note 4, at 497–98, 501 (suggesting that more proactive disclosure of clinical trial data by the FDA "can be achieved without legislative reform," *id.* at 498, but "will require revisions to the FDA's current regulations, corrections to its interpretations of certain statutes, and, for the most sensitive data, data use agreements," *id.* at 501).

As we have demonstrated in this Article, underlying this problem is what we call "trade secrecy's information paradox"—trade secrecy's unique, nested version of Kenneth Arrow's more famous Information Paradox. At the time a claimant asserts a trade secret, it is virtually impossible to know whether the underlying information is beneficial or harmful to society. Answering this question first requires exposing the information to broader scrutiny. But that disclosure destroys any chance of protecting it as a trade secret; this can lead to copying by competitors and depressed incentives for creating similar innovations. So what is a decisionmaker to do?

Trade secrecy's information paradox is at the heart of recent disputes over potentially biased bail algorithms, environmentally harmful chemicals, unsafe and ineffective new drugs, and disparate hiring practices. It implicates numerous social interests, from public health to the success of the regulatory state. Unlike other areas of intellectual property, traditional doctrinal tools offer less promise for screening out socially harmful trade secrets. While doctrinal and costly screens can be effective in other IP contexts—sorting socially harmful patents and trademarks from socially beneficial ones—the story is decidedly less rosy for trade secrecy. Trade secrecy's information paradox cannot be easily solved, at least with any politically feasible set of tools.

A problem without a solution is rarely highlighted in legal scholarship. In law (though not necessarily in life), comedies make for much better reading than tragedies. While our Article offers no easy answers, it nonetheless clarifies the problem itself. By illuminating the unique nature and scope of trade secrecy's information paradox and explaining why doctrinal and costly screens are unlikely to be as helpful in this area as they have been elsewhere in IP, we hope to call renewed attention to this problem and motivate the search for innovative answers. Perhaps by illuminating a tragedy, we can help set the stage for an eventual comedy.