From Trade Secrecy to Seclusion

CHARLES TAIT GRAVES* & SONIA K. KATYAL**

By all accounts, trade secret law is now recognized as one of the major categories of intellectual property law. Less recognized, however, is the degree to which private actors are pushing the law past its traditional, market-competitive boundaries and toward an all-purpose seclusion doctrine. We argue that trade secret law today is increasingly functioning not merely as a tool to protect intellectual property against misappropriation, but often as a tool for open-ended concealment. The law is moving from trade secrecy to trade seclusion. This shift raises serious concerns, ultimately distorting the flow of information that should be available to the public.

Confronting these disparate claims of trade secrecy or confidentiality—which can crop up in civil litigation, criminal law, open records disputes, and elsewhere—requires, first of all, a common vocabulary. In this Article, we collect and identify a variety of nontraditional cases to demonstrate the alarming extension of trade secrecy arguments in a host of different areas of law. We classify these scattered claims into three categories: investigatory concerns involving journalists and whistleblowers; delegative concerns where the government relies on private technologies, such as automated decisionmaking and artificial intelligence; and dignitary concerns where employers seek control over employee attributes, such as diversity data and workplace harms, beyond the normal context of employer/employee trade secret lawsuits.

In our final Section, we present a range of solutions. Some suggest ways to recuperate trade secret law's traditional architecture and thus pay heed to its intrinsic boundaries. As we argue, some nontraditional trade secrecy claims involve information that is not a trade secret at all. And, even where information qualifies as secret (or as confidential, in open-records parlance), we draw upon recent scholarly efforts to define doctrinal limits to trade secrecy and similar

* Partner, Wilson Sonsini Goodrich & Rosati; Adjunct Professor, Hastings College of the Law, University of California.

** Haas Distinguished Chair and Co-Associate Dean for Research, University of California, Berkeley, School of Law. We are grateful to Catherine Fisk, Neal Katyal, Rebecca Wexler, Vicki Cundiff, Sharon Sandeen, Camilla Hrdy, Deepa Varadarajan, Rebecca Tushnet, Jeanne Fromer, Margaret Chon, Margaret Kwoka, Michael Risch, David Levine, Mark Lemley, Elizabeth Rowe, Victoria Baranetsky, Simone Ross, Pamela Samuelson, Felix Wu, Robin Feldman, Helen Norton, and Karina Condra for their comments, conversation, and input on drafts of this Article, including at the July 2020 Trade Secrets Scholars Workshop and the August 2020 IP Scholars Conference. We offer tremendous thanks to our wonderful research assistants, Madeeha Dean and Calvin Hannagan, who gathered much of the material we discuss, and to Stephanie Dorton for her helpful assistance in preparing this draft.

claims in both litigation and open-records disputes where there is a pressing public interest. Finally, drawing from the lessons of #MeToo and other workplace protection statutes, we examine potential legislative enactments in order to achieve an appropriate balance between secrecy and the public interest.

TABLE OF CONTENTS

INTRODUCTION

In March 2020, facing a pandemic of epic proportion, Congress enacted the Paycheck Protection Program (PPP) to administer government loans to businesses to help them stay afloat. The program was based on an earlier loan program provided by the Small Business Administration (SBA). Except for one significant difference. Although loans administered by the SBA are typically made public, the PPP loans—and the identities of their recipients—were designed to be entirely secret, even though dozens of publicly traded companies received them. "We believe that that's proprietary information," Treasury Secretary Steven Mnuchin testified, justifying this decision, "and in many cases

for sole proprietors and small businesses, it is confidential information."[1] The companies flimsily asserted that if such information were released, competitors might use it to glean information about employee salaries and hire workers away.[2]

Almost immediately, the Trump Administration faced an outcry from the public and Congress, prompting the *Washington Post* and other news organizations to file suit under the Freedom of Information Act (FOIA), seeking information on the identity of the grantees.[3] Within a few days, the Administration reversed course and agreed to release information for loans larger than $150,000.[4]

The Trump Administration's rapid reversal reflects a tacit recognition of the legal frailty of its arguments, particularly in light of the strong public interest favoring federal loan disclosure. But its position raises the important question of how companies and their allies in government could even hope to claim that such information is "confidential" in the first place, much less feel any confidence that they might succeed by offering such dubious arguments.

This story—and perhaps the Trump Administration's faith in such an outlandish claim—is illustrative of the critical problem this Article addresses. There has been a sea change in trade secrecy. Today, scattered across the legal landscape, assertions of "trade secrets" and "confidential information" are deployed in increasingly unusual contexts outside the traditional scenario of disputes over information used for marketplace competition, producing a crisis involving matters of public concern. A substantial threat to an informed democracy, we posit, involves the overbreadth of secrecy and confidentiality claims to conceal matters of public concern or other information that should ordinarily be publicly available.

---

1. Jonathan O'Connell, *Mnuchin Loosens Restrictions on Small-Business Loans to Ease Forgiveness, but Borrowers to Remain Secret*, WASH. POST (June 10, 2020, 2:07 PM), https://www.washingtonpost.com/us-policy/2020/06/10/mnuchin-small-business-paycheck-protection-program.

2. *See* Sharon Sandeen, Elizabeth Rowe & Ryan Vacca, University of New Hampshire School of Law Panel Discussion: Trade Secrets, Transparency, and Paycheck Protection Program Loans During a Pandemic (June 19, 2020) (discussing Amended Complaint for Declaratory and Injunctive Relief, WP Co. v. U.S. Small Bus. Admin., No. 1:20-cv-01240-ABJ, 2020 WL 6504534 (D.D.C. 2020), and concerns over claims of confidentiality as an exemption to the Freedom of Information Act (FOIA)) (notes on file with authors); *see also* Amended Complaint for Declaratory and Injunctive Relief ¶¶ 1, 45, *WP Co.*, No. 1:20-cv-01240-ABJ, 2020 WL 6504534 (news organizations bringing action under FOIA for PPP records after the SBA failed to produce); Defendant's Answer to Plaintiff's Amended Complaint for Declaratory and Injunctive Relief, *WP Co.*, No. 1:20-cv-01240-ABJ, 2020 WL 6504534, ECF No. 9.

3. *See* O'Connell, *supra* note 1.

4. *See* Marcy Gordon, *Administration Drops Secrecy Posture on Small Business Aid*, ASSOCIATED PRESS (June 19, 2020), https://apnews.com/article/46c1b6e2783db3b1394fcd4b43dba0fe [https://perma.cc/P2PJ-PP2Z] (noting the Trump Administration's reversal and agreement to publicly disclose the names of recipients of taxpayer-funded business loans, the amounts they received, and business-related demographic data); Alan Rappeport, *Treasury Dept. Agrees to Release Data on Small-Business Relief*, N.Y. TIMES (June 19, 2020), https://www.nytimes.com/2020/06/19/us/politics/treasury-small-business-ppp-loan-disclosure.html.

These claims arise in a wide variety of contexts. Companies submit aggregated data about employee injuries to the Department of Labor, but then claim that data as confidential information when journalists seek to obtain those same records from the government. A company files a lawsuit for trade secret misappropriation when a whistleblower retains files in order to report a potential Sarbanes–Oxley Act violation. Another sues a former employee for hiring his former coworkers, claiming that he misused trade secrets simply by offering them a job elsewhere. Still others try to block the release of records submitted to government agencies regarding employee diversity statistics, worker injury, and compliance with environmental requirements. Governments make automated decisions, relying on artificial intelligence in a wide range of sectors ranging from public benefits to offering evidence in criminal prosecutions, but then refuse to turn over source code when their decisions are challenged in court.

In the aggregate, these and other examples suggest that the nature of trade secret and confidentiality disputes in civil litigation, criminal prosecutions, and disputes under state and federal open-records statutes has changed in recent years.[5] Historically, federal and state trade secret statutes define trade secrets as competitive business information, and generally require parties to show proof of standing, economic value to competitors, and the use of reasonable security measures. In many cases, a trade secret is also expected to comprise information that is the product of substantial effort or innovation, essentially requiring a "direct relationship between the trade secret and the productive process."[6] When trade secret law operates as it should, it balances incentives to innovate with the interests of mobile employees and others to use business information that does not meet these requirements.

But as trade secret disputes have increased, so too have assertions of trade secrecy that do not fit this traditional, market-competitive fact pattern. Today, such claims extend to different types of information as well, as companies learn that labeling sensitive or embarrassing information as a "trade secret" or "confidential" can stall or silence calls for disclosure. Further, as the reach of software in government agencies and decisionmaking increases apace, it becomes even more difficult to strategize for greater transparency in a world that increasingly relies upon automated, black-box decisionmaking.

---

5. For the standard account of the growth in trade secret litigation since the 1990s, see David S. Almeling, Darin W. Snyder & Michael Sapoznikow, *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 301–02 (2009) (showing "exponential" growth in federal trade secret litigation since the mid-1990s) and 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, 67–68 (2010) (showing "modest" growth in state-court trade secret litigation cases). More recent and more granular data is harder to come by. A recent report suggests that overall trade secret filings increased sharply after the May 2016 enactment of the Defend Trade Secrets Act (DTSA) but has since leveled off. *See* RACHEL BAILEY, LEX MACHINA, LEX MACHINA TRADE SECRET LITIGATION REPORT 3 (Jason Maples ed., 2020). However, in the last two decades, anecdotal evidence for the growth in trade secret law can be seen by the number of law firms advertising a trade secret practice, the number of scholarly articles on trade secrecy, the DTSA, and the gradual enactment of the Uniform Trade Secrets Act (UTSA) by state legislatures (as of this writing, New York is the sole outlier).

6. 21 C.F.R. § 20.61(a) (2020).

Yet because these cases are easily viewed in isolation, and because attorneys and scholars necessarily focus on their own areas of specialization, the emergence of this pattern of overbreadth is easy to miss. Still, these seemingly disparate cases—rooted in different areas of law and different contexts—share an important common thread: increasingly aggressive attempts to use the law to shield information from the public eye that either does not fall within the traditional, market-competitive ambit of trade secrecy at all, or that faces a strong public interest for at least some degree of disclosure. All too often, the claimant treats its desire to avoid reputational harm as equivalent to an intellectual property right.

In this Article, we introduce a fundamental distinction that we believe is helpful in understanding these recent events. We argue that the case law reveals a trend line that is moving from trade secrecy to trade *seclusion*. Traditional trade secrecy claims, we describe, involve business information that is developed for use in marketplace competition and disputes over whether competitors misappropriated it. But today, secrecy is becoming unmoored from that marketplace context and is expanding into nontraditional subject matter with only attenuated connection to a competitive advantage in research and development, sales, or marketing.

We argue that corporate and government actors have pushed to transform the law of trade secrecy into one of the most—if not *the* most—powerful tools to ensure the concealment of information. The irony is that this has happened at the very same time that the opaque nature of algorithmic decisionmaking, coupled with the new interplay between government agencies and private technologies, has created a crisis regarding access to information by journalists, regulators, and others working in the public interest. If unchecked, these developments may result in a framework where crucial information is actively concealed through trade secrecy, foreclosing investigation and inquiry in the public interest. The effects on the flow of information to the public will undoubtedly be dramatic and far-reaching as a result.

To be sure, hiding information from the public is a not a new problem. For example, scholars have been concerned for many years about overdesignation of confidentiality regarding environmental records in FOIA requests. Recently, however, commentators have begun to identify and critique the expansion of nontraditional trade secrecy claims in the criminal, environmental, government infrastructure, and employee-related contexts, and have demonstrated how limiting these claims may be warranted.[7]

7. For early and foundational articles focusing on nontraditional trade secret claims, see David S. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure*, 59 FLA. L. REV. 135, 177–87 (2007) (examining case studies of private companies claiming trade secret rights where government agencies used their technologies for routers, voting machines, and citywide Wi-Fi) and Mary L. Lyndon, *Secrecy and Access in an Innovation Intensive Economy: Reordering Information Privileges in Environmental, Health, and Safety Law*, 78 U. COLO. L. REV. 465, 498–99 (2007) (examining trade secrecy claims in environmental records submitted to government agencies).

Yet beyond the trade secret community, calls for reform have been mostly invisible to the public eye and often limited to a particular sector. Because there has been little comparative analysis of these contexts and little recognition of the dramatic impact of these expanded secrecy claims, there is little in the way of normative proposals that could carry force across the range of problems we and others have identified. At the same time, however, scholars have begun to propose limiting doctrines for trade secret law, often borrowing from theories established in copyright, trademark, and patent law. This momentum creates a significant opportunity to bring this scholarship together, identify common patterns, and organize potential solutions for a unified approach.

To that end, we collect recent studies, discuss new cases, and identify additional concerns from a wide variety of nontraditional contexts. We argue that these disputes, taken in aggregate, illustrate a foundational—and largely unexplored—shift in trade secrecy toward open-ended concealment.

Using seclusion as the organizing theme (as opposed to garden-variety trade secrecy), we offer three contributions to the literature. Our first contribution, discussed in Part I, is descriptive—an exercise in pattern recognition. It is critical to investigate the reason a would-be information owner in a nontraditional context seeks seclusion, and to identify the concerns that arise from concealment. Drawing from recent case law, we discuss a range of issues involving different strands of trade secret and open-records law—corporate whistleblowing, government infrastructure, environmental activism, employee advocacy, and criminal prosecution, among others. Each of these sectors has been deeply affected by the rise of trade secrecy; the rise of nontraditional trade secret claims in each of these sectors, in turn, will have a dramatic effect on disclosure of information benefitting the public.

Each type of case can be paired with an important public concern. To understand what they share and discuss potential common solutions, we identify three core areas: (1) investigative concerns (appearing most often in environmentally oriented and criminal-prosecution cases); (2) delegative concerns (appearing most often in cases involving the delegation of a government function to a private party); and (3) dignitary concerns (appearing most often in cases focused on a workplace and employee well-being, but distinct from traditional trade secret claims against departing employees).

Second, drawing on these three themes, in Part II we analyze the common threads underlying exemplary studies and lawsuits. This deeper exploration of the patterns across such cases reveals striking ways in which trade secrecy has strayed from its traditional subject matter of business-competitive information. As we suggest, the further a claimant strays from traditional, marketplace-centered information, the stronger the public interest often becomes. Moreover, the strength of such arguments is strikingly thin compared to the strength of more typical trade secret claims, particularly regarding the seriousness of the public concern at issue.

To begin with, some of the information over which such assertions are made simply does not meet the test for trade secrecy (or "confidential" information) at all. And even in cases where there is a cognizable trade secret (say, as in source code for software relied on by government, or chemical data), the public interest in some degree of disclosure is just too great to ignore.

Third, also in Part II, we conclude with potential normative challenges to overreaching trade secrecy and confidentiality claims in these nontraditional contexts. Recent scholarship has articulated theories that courts and others can use to limit dubious trade secrecy claims in cases of strong public interest.[8] These proposals have drawn upon a range of ideas, involving concepts of misuse, thin trade secrecy, and fair use. Adding to this literature, we explore a set of additional solutions, ranging from revisiting the basic requirements of trade secret law to reforming standing and ownership issues, and offering other procedural means to challenge the deference given to trade secret claimants in the midst of a dispute.

In addition to case-specific solutions, we propose ways to restructure our system of trade secret law to recognize the dangers posed by nontraditional trade secrecy claims and provide means to weigh them against important public policy interests. To this end, we also offer potential legislative solutions in recognition of the public interests so often at stake. Such legislation could come in two forms. To begin with, legislatures might enact targeted bills to provide specific forms of information—workplace injury statistics or aggregated workplace diversity data—from being withheld as confidential or secret. This would be akin to recent legislative efforts in many states to promote workplace salary discussions, to prohibit nondisclosure contracts that would bury episodes of workplace sexual harassment, and to allow consumers to more easily repair devices they have purchased.

In addition, we can imagine amendments to state or federal trade secret and open-records statutes that would allow courts facing bids to conceal information in the types of nontraditional scenarios outlined in this Article to weigh the public interest for some form of disclosure against the nature of the information at issue and the degree to which it satisfies the tests for protectability. Because we expect trade secret claims to become ever more entangled in government and to arise in unpredictable types of disputes in the years to come, a broad balancing enactment may offer the best opportunity to provide courts with a flexible means to prevent abuses.

8. *See, e.g.*, Peter S. Menell, *Tailoring a Public Policy Exception to Trade Secret Protection*, 105 CALIF. L. REV. 1, 61–62 (2017) (describing how the Defend Trade Secrets Act of 2016 protects whistleblowers against trade secret claims); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018) (examining the use of technologies by the prosecution in criminal cases); Jamillah Bowman Williams, *Diversity as a Trade Secret*, 107 GEO. L.J. 1685 (2019) (examining corporate claims that workforce diversity data and company diversity strategies are trade secrets).

I. THE TRADITIONAL TRADE SECRECY CONTEXT AND NEW DEMANDS FOR SECLUSION

We begin with a description of the traditional contexts of trade secret disputes and the marketplace-centered statutory definitions of trade secret law to set the stage for the shift we observe toward trade secrecy claims in less traditional types of information.

A. THE ORIGINS OF TRADE SECRET LAW AND ITS MARKETPLACE CONTEXT

The origins of contemporary trade secret law are not reducible to a singular explanation, but cases nonetheless have tended to fall within two common scenarios. Rather than attributing a unitary origin story to the development of trade secret law, research efforts show a multiplicity of origins stemming from an overlapping web of tort, property, and contract principles.[9] As Katharina Pistor has discussed in recent work, we might think of the development of IP law—including trade secret law—as one form of "coding": an uneven, gradual process over the centuries by which practitioners try out different approaches to maximizing the exclusionary rights of their clients by coding assets as property.[10] Along these lines, Deepa Varadarajan has explained how courts placed many of the early industrial-era cases under the rubric of unfair competition law, treating it as an outcrop of this larger body of doctrine.[11] At the same time, the deeper origins of trade secret law also arose from different versions of employer control over worker mobility, limitations of the guild system in early English modernity, and prosaic property disputes in the area of

9. The disparate origins of trade secret law also help explain why its philosophical foundations remain a matter of spirited debate. Through a number of articles, largely published ten to twenty years ago, property-based conceptions emerged as the most common (though not the consensus) view, consistent with the UTSA—and, later, the DTSA. *See generally* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241 (1998) [hereinafter Bone, *A New Look at Trade Secret Law*]; Robert G. Bone, *The (Still) Shaky Foundations of Trade Secret Law*, 92 TEX. L. REV. 1803 (2014) [hereinafter Bone, *The (Still) Shaky Foundations of Trade Secret Law*]; Miguel Deutch, *The Property Concept of Trade Secrets in Anglo-American Law: An Ongoing Debate*, 31 U. RICH. L. REV. 313, 321 (1997); Charles Tait Graves, *Trade Secrets as Property: Theory and Consequences*, 15 J. INTELL. PROP. L. 39 (2007); Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311 (2008); Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L. REV. 1 (2007).

10. KATHARINA PISTOR, THE CODE OF CAPITAL: HOW THE LAW CREATES WEALTH AND INEQUALITY 108–31 (2019).

11. *See* Deepa Varadarajan, *Business Secrecy Expansion and FOIA*, 68 UCLA L. REV. (forthcoming 2021) (manuscript at 3) (on file with authors); *see also* Bone, *The (Still) Shaky Foundations of Trade Secret Law*, *supra* note 9, at 1811 n.47 (observing that, in the early twentieth century, trade secret appropriation "was considered a form of unfair competition, but the property conception was still influential"). For more information on the various statutes governing trade secret law, see Robert Denicola, *The Restatements, the Uniform Act and the Status of American Trade Secret Law*, *in* THE LAW AND THEORY OF TRADE SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH 18 (Rochelle C. Dreyfuss & Katherine J. Strandburg eds., 2011) and Charles Tait Graves, *Trade Secrecy and Common Law Confidentiality: The Problem of Multiple Regimes*, *in* THE LAW AND THEORY OF TRADE SECRECY, *supra*, at 77.

wills and trusts.[12]

Despite these varying origins, the typical trade secret case since modern cases first arose in the nineteenth century has involved one of two kinds of disputes. In the most common form of the traditional case, a company sues a departing employee—and perhaps also the new employer—to enjoin the use or disclosure of trade secrets, to seek damages for misappropriation of a trade secret, or occasionally even to prevent the employee from taking a new job with a competitor. In the other line of traditional cases, involving business-to-business conflicts, a company sues a former business partner after their relationship dissolves, alleging that it misused information the plaintiff shared. For the most part, until recent years, both patterns of cases remained largely consistent, even with the growth in the number and the complexity of such cases.[13]

As Varadarajan has noted, this context generated cases that were circumscribed by their limited subject matter, addressing manufacturing processes, designs, formulas, and the like.[14] In these cases, trade secret law focused on the protection of competitive information that businesses use to advance their marketplace positions—most commonly, technology and customer-related information. Trade secret statutes, in turn and even today, reflect these boundaries. In general, business information qualifies for trade secret protection if it meets four elements: (1) it must not be generally known to others in the same industry; (2) it must not be readily ascertainable from the use of limited time and effort; (3) it must have independent economic value to competitors; and (4) it must be reasonably guarded as secret.[15] Each of these limitations historically cabined the reach

12. *See, e.g.*, CATHERINE L. FISK, WORKING KNOWLEDGE: EMPLOYEE INNOVATION AND THE RISE OF CORPORATE INTELLECTUAL PROPERTY, 1800–1930, at 29–30, 175 (2009) (showing how restrictive covenants gained strength, in particular between 1895 and 1930); KAREN ORREN, BELATED FEUDALISM: LABOR, THE LAW, AND LIBERAL DEVELOPMENT IN THE UNITED STATES 71–79, 104–07 (1991) (describing the origins of the noncompetition and nonsolicitation covenant in English law and their importation into American law); Sean Bottomley, *The Origins of Trade Secrecy Law in England, 1600–1851*, 38 J. LEGAL HIST. 254, 274–75 (2017) (describing early efforts to seek relief against mobile employees under nascent trade secret law and how wills and trusts law and other property disputes helped define early trade secret law).

13. Pamela Samuelson, *First Amendment Defenses in Trade Secrecy Cases*, *in* THE LAW AND THEORY OF TRADE SECRECY, *supra* note 11, at 286 (describing a classic trade secret case, where defendants are described as: "(1) private profit-making firms or individuals who work for or with such firms (2) who intend to make private uses or disclosures of another firm's secrets (3) as to information that is neither newsworthy nor a matter of public concern and (4) who have breached an enforceable contract to maintain secrecy, abused the confidence under which they received another's trade secrets, and/or used improper means, such as bribery or fraud, to obtain the secrets (5) under circumstances likely to give rise to substantial and irreparable harm arising from the defendants' competitive uses of the secrets").

14. *See* Varadarajan, *supra* note 11.

15. *See, e.g.*, 18 U.S.C. § 1839(3)(A)–(B) (2018); UNIF. TRADE SECRETS ACT § 1(4)(i)–(ii) (amended 1985), 14 U.L.A. 538 (2005). Not every jurisdiction has an identical test for trade secrecy. The California legislature did not include the not-readily-ascertainable requirement, *see* CAL. CIV. CODE § 3426.1(d)(1)–(2) (West 2020), and New York still follows the 1939 Restatement of Torts formulation. But by and large, tests for trade secrecy in civil litigation are the same.

of trade secret law beyond competitive business information.[16] Indeed, because trade secrecy often shared the themes and vocabulary of early unfair competition law, it included something akin to a "standing" requirement because, as Sharon Sandeen has observed, courts were reluctant to entertain claims involving noncompetitors.[17]

The theme of competitive business information, as suggested above, underscores almost every definition, theoretical and statutory, of a trade secret. Jerome Reichman has explained, "[W]hat trade secrecy law protects is an entrepreneur's investment in applications of know-how to industry, which may or may not rise to the level of a non-obvious invention."[18] This "know-how," Reichman continues, quoting Stephen Ladas, "consists of information about how to achieve some technical or commercial advantage over competitors, typically by means of novel methods or processes of production."[19] This observation, we think, highlights the importance of viewing trade secrecy through a prism that focuses on the value of innovation over competitors.

A wide range of statutes and commentaries confirm these characterizations. Under the Defend Trade Secrets Act (DTSA), a "trade secret" is "all forms and types of financial, business, scientific, technical, economic, or engineering information."[20] That definition also covers the criminal portions of the statute as well—the Economic Espionage Act (EEA) of 1995.[21] Although the examples of types of

16. Moreover, as we discuss in Part III, federal law contains an express standing requirement, limiting the scope of such claims (also reflected in state common law). *See* 18 U.S.C. § 1839(4) (limiting claimants to owners and licensees).

17. *See* Varadarajan, *supra* note 11, at 10–11 (citing 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, 500 (2010)).

18. Jerome Reichman, *How Trade Secrecy Generates a Natural Semicommons of Innovative Know-How*, *in* THE LAW AND THEORY OF TRADE SECRECY, *supra* note 11, at 188.

19. *Id.* (quoting STEPHEN P. LADAS, PATENTS, TRADEMARKS AND RELATED RIGHTS: NATIONAL AND INTERNATIONAL PROTECTION 1616 (1975)). Indeed, Reichman goes so far as to even describe how, essentially, trade secret protection provides a first-mover advantage, offering an inventor a legally protected "natural lead time" over subsequent inventors who may eventually seek to reverse engineer an invention. *Id.* at 189. By doing so, he argues, trade secrecy law promotes competition while also gently stimulating third-party competitors to undertake their own process of innovation through reverse engineering. *Id.*

20. 18 U.S.C. § 1839(3) ("[T]he term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing . . . .").

21. *See* 18 U.S.C. §§ 1831–1832 (referring to same definition of "trade secret"). Indeed, before Congress added the civil DTSA portions of the statute in May 2016, federal courts interpreting the EEA in criminal cases looked to the civil UTSA for assistance in construing the elements of trade secrecy. *See, e.g.*, United States v. Chung, 659 F.3d 815, 825 (9th Cir. 2011) ("Until now, this court has had no occasion to interpret the EEA's definition, and the case law in other circuits is sparse. The EEA's definition, however, is derived from the definition that appears in the Uniform Trade Secrets Act ('UTSA'), a model statute which permits civil actions for the misappropriation of trade secrets. Thus, we consider instructive interpretations of state laws that adopted the UTSA definition without substantial modification." (footnote omitted)).

trade secrets listed in the statutory definition are not exhaustive, it is nonetheless notable that this language does not include attributes of employees, injuries or accidents, assaults or harassment, acts of wrongdoing, violations of law, embarrassing events, or employees' salaries. It would be more than a stretch to wedge such categories into a statute that does not list them, and—more importantly—does not list other things of the same nature among its examples.

Beyond the basic definition of trade secrecy, the text of the statute further demonstrates that it contemplates business information used for competitive purposes in the marketplace as the primary candidate for potential trade secrecy claims. A provision in the criminal portion of the statute renders illegal certain acts as to "[w]hoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce."[22] In turn, the DTSA clause permitting civil lawsuits refers to bringing "a civil action . . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce."[23] That would seem to all but rule out information falling within our category of dignitary concerns.

The DTSA's restrictions on injunctive relief also speak to a competitive business context. An emergency impoundment order must balance "any interruption of the business operations of third parties and, to the extent possible" must not "interrupt the legitimate business operations of the person accused of misappropriating the trade secret."[24] Ordinary injunctions also cannot "conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business."[25]

Turning to state law, the Uniform Trade Secrets Act (UTSA)—some version or close cousin of which has been adopted in forty-nine states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands[26]—likewise focuses on competitive business information. The 1985 model act contains a two-step description of the coverage of trade secrecy. A potential trade secret is, first, "information, including a formula, pattern, compilation, program, device, method, technique, or process."[27] Second, that information must be that which "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."[28] The limitation to "economic value"

22. 18 U.S.C. § 1832(a).

23. *Id.* § 1836(b)(1).

24. *See id.* § 1836(b)(2)(B)(ii).

25. *See id.* § 1836(b)(3)(A)(i)(II). This appears to be a direct reference to state statutes that prohibit noncompetition covenants, such as California Business & Professions Code Section 16600 and North Dakota Century Code Section 9-08-06. *See* CAL. BUS. & PROF. CODE § 16600 (West 2020); N.D. CENT. CODE ANN. § 9-08-06 (West 2019).

26. New York is the exception; it has no statute governing trade secret misappropriation litigation. North Carolina, Puerto Rico, and Alabama enacted UTSA-like statutes that use somewhat different language. Other states enacted variations to the 1979 or 1985 model versions of the UTSA as to terms such as the statute of limitations and preemption of overlapping tort claims.

27. UNIF. TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 538 (2005).

28. *Id.* § 1(4)(i).

points to a competitive marketplace context, and thus cabins general phrases such as "information" and "compilation."

Some states have altered that wording somewhat, but not in a manner that affects this analysis. Oregon refers to "information, including a drawing, cost data, customer list, formula, pattern, compilation, program, device, method, technique or process."[29] New Jersey refers to "information, held by one or more people, without regard to form, including a formula, pattern, business data compilation, program, device, method, technique, design, diagram, drawing, invention, plan, procedure, prototype or process."[30] Texas includes "financial data" and a "list of actual or potential customers" in its formulation.[31] But although these lists of categories are illustrative, no state's version of the UTSA expressly includes the types of nontraditional information described here, and all of them link general categories with the requirement that such information have independent "economic value."[32] This points to a commercial, competitive context, but not a concept that encompasses the nontraditional claims we have discussed.

New York is the only state that still uses the 1939 Restatement of Torts as the basis for its trade secret laws.[33] That formulation, too, points to a context of marketplace competition. It employs a six-factor balancing test to determine trade secrecy, including "the value of the information to [the owner and its] competitors," "the amount of effort or money expended . . . in developing the information," and "the ease or difficulty with which the information could be properly acquired or duplicated by others."[34] In particular, information that is "developed" would not appear to encompass such things as workplace injuries or environmental violations.

State criminal statutes for trade secret violations are more difficult to summarize than the federal criminal provisions of the EEA, or even the civil provisions of state UTSA enactments, because they are less uniform. But their coverage is similar to, and sometimes the same as, the UTSA. Some states follow a Model Penal Code formulation first seen in New Jersey, which defines trade secrecy as "[t]he whole or any portion of any scientific or technical information, design, process, procedure, formula or improvement which is secret and of value."[35] Other

29. OR. REV. STAT. ANN. § 646.461(4) (West 2020).

30. N.J. STAT. ANN. § 56:15-2 (West 2020).

31. TEX. CIV. PRAC. & REM. CODE ANN. § 134A.002(6) (West 2019).

32. There are minor variations. For example, Puerto Rico uses the phrase "independent financial value." P.R. LAWS tit. 10, § 4132(a) (2011). And North Carolina uses the phrase "commercial value." N.C. GEN. STAT. § 66-152(3)(a) (West 2020).

33. As of this writing, a bill has been introduced in the New York legislature to enact the UTSA. *See* S.B. 2468, 2019–2020 Reg. Sess. (N.Y. 2020).

34. *See* RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. LAW. INST. 1939).

35. *See* Kurt M. Saunders & Michelle Evans, *A Review of State Criminal Trade Secret Theft Statutes*, 21 UCLA J.L. & TECH. 1, 8–10 (2017) (providing a detailed summary of differing state statutes allowing for prosecutions of trade secret theft and analyzing origin of Model Penal Code language from an older New Jersey statute). An example is Texas. TEX. PENAL CODE ANN. § 31.05(a)(4) (West 2019).

states follow the UTSA definition.[36] A few others use a New York formulation that is premised on "secret scientific material."[37] But none of these appears to allow prosecutions based on the nontraditional categories of information discussed in this Article.

B. STRUCTURAL FACTORS IN THE MOVE TO NONTRADITIONAL CONTEXTS

Notwithstanding the traditional context of most disputes, the boundaries of trade secrecy began to expand, for a variety of reasons.[38] Part of why this could happen involves factors inherent to trade secret law that distinguish it from other categories of intellectual property. One factor is that the scope and subject matter of trade secret law is broader than other forms of intellectual property—copyright, as a comparative example, is limited to fixed expression, and patent protection is limited by subject matter and by PTO examination. Unlike copyright and patent law, trade secrecy's subject matter, even with its circumscribed boundaries, is strikingly open-ended. As noted above, the scope of trade secret protection, while not without boundaries, is nonetheless much broader than the coverage afforded by patent law and copyright law.[39]

Still, these formulations—however broad—do not include such things as workplace injuries, lawbreaking, or environmental pollution. And yet, in the cases we discuss below, companies readily characterize such categories as protectable trade secrets or "confidential" information. And although that might sound like a fanciful argument, in many of these cases, that is precisely the reasoning that those seeking to seclude such information offer. Sometimes the courts agree.

There is a second, structural factor making possible secrecy's expansion, linked to the first: claims of trade secrecy are self-defined until they are adjudicated otherwise, often after costly litigation that can take years. This factor allows for greater deference to secrecy over other public interests like transparency. Copyright and patent law, by contrast, are oriented (and incentivized) toward disclosure to the public.[40] Yet trade secrecy is oriented toward the opposite function and risks tautology—something is a trade secret because someone says so—as a result of its self-defining character. For example, under any version of the law, trade secrets need not be registered with the government and therefore can be asserted for the first time when initiating a legal dispute and identified after the dispute is underway. In other words, something may be deemed secret, and may

36. *See* Saunders & Evans, *supra* note 35, at 8–9. An example is California's criminal statute, which incorporates identical language from the California UTSA. *Compare* CAL. PENAL CODE § 499c(a)(9)(A)–(B) (West 2020), *with* CAL. CIV. CODE § 3426.1(d)(1)–(2) (West 2020).

37. *See* Saunders & Evans, *supra* note 35, at 9–10.

38. Varadarajan, *supra* note 11, at 13–14.

39. *See* 18 U.S.C. § 1839(3) (2018).

40. *See* Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV. 1183, 1212 (2019). Historically, until the Berne Convention, content could only be protected by copyright upon disclosure, thereby ensuring that only published material received protection. In the area of patent protection, disclosure has been essentially required upon grant of the patent (and, under recent statutes, even earlier). *See id.* And disclosure to the public is a core goal of patent law because it promotes follow-on innovation. *See* Jeanne C. Fromer, *Patent Disclosure*, 94 IOWA L. REV. 539, 541 (2009).

be the subject of a claim for protection, because it is subjectively asserted to be confidential without any oversight or pushback until the dispute has been adjudicated. As a result, in a broad array of legal contexts, claimants can choose their own narrative of trade secrecy to serve whatever their immediate goal may be. Perhaps due to this possibility, more and more parties have asserted trade secrecy or confidentiality as a general right to absolute seclusion, even when there is not a hint of competitive advantage at stake.

A third factor enabling the growth of nontraditional cases involves FOIA, which allows government actors to withhold requested information from the public if it falls under Exemption 4, a statutory exemption from disclosure for trade secrets.[41] If the default of FOIA is disclosure, subject to limited exemption, then trade secret law is precisely the opposite, positing the default of secrecy subject to limited and controlled disclosure.[42] FOIA also offers a second, broader exemption for "commercial or financial information [that is] obtained from a person and privileged or confidential."[43] This additional exemption is the focus of the FOIA disputes we discuss in this Article because it has led to an ever-growing number of conflicts between companies' desire for confidentiality and the public's need for disclosure and transparency.[44]

In summary, trade secret law—despite diffuse origins—consolidated around a nexus of marketplace competition. That nexus is reflected in all official formulations of trade secret law. At the same time, however, the structure of trade secret law is looser in important ways compared to other forms of intellectual property. As we now explain, companies are increasingly exploiting these gaps to assert trade secret rights in a growing range of nontraditional contexts.

II. FROM RELATIVE TO ABSOLUTE SECRECY

In recent years, we and other scholars have found issues arising in a wide variety of contexts, implicating environmental, criminal, administrative, and employee-mobility concerns as well as workplace conditions and whistleblowing. In

41. *See* Freedom of Information Act, 5 U.S.C. § 552(b)(4) (2018). Notably, FOIA includes a narrower definition of a trade secret than the DTSA, UTSA, and common law Restatement formulations, thus limiting the degree to which it might be used to shield information not traditionally encompassed by trade secret law. For purposes of a FOIA exemption to disclosure, a trade secret means "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 Research Grp. v. FDA, 704 F.2d 1280, 1288 (D.C. Cir. 1983); *accord* Ctr. for Auto Safety v. Nat'l Highway Traffic Safety Admin., 244 F.3d 144, 150–51 (D.C. Cir. 2001); Anderson v. U.S. Dep't of Health & Human Servs., 907 F.2d 936, 944 (10th Cir. 1990).

42. *See* David S. Levine, *The People's Trade Secrets?*, 18 MICH. TELECOMM. & TECH. L. REV. 61, 79 (2011).

43. 5 U.S.C. § 552(b)(4).

44. This exemption is also the subject of a 2019 Supreme Court decision that complicates the analysis because it could make it easier for companies to claim information as "confidential." *See* Food Mktg. Inst. v. Argus Leader Media, 139 S. Ct. 2356, 2366 (2019). For a useful analysis, see Sharon Sandeen, *High Court FOIA Ruling Has Trade Secrets Implications*, LAW360 (July 3, 2019, 10:16 AM), https://www.law360.com/articles/1175163/high-court-foia-ruling-has-trade-secrets-implications.

many such cases, the very nature of the information in question—workplace injury reports, for example—likely would not satisfy the definition of a trade secret. Yet in these nontraditional contexts, intellectual property arguments are deployed, not for the purposes of protecting property against competitors, but in the service of other values, namely concealment from the public for reasons other than harm suffered in marketplace competition.

These motivations involve more than just an open-ended desire for unlimited seclusion. Instead, as this Part shows, seclusion is linked to other, corollary concerns that require a deeper interrogation. We categorize these areas of concern to highlight the private interests they serve, and the public interests they harm. Categorization is fuzzy, of course, and some of the problems we illustrate in this Article may fall within one or more areas.

There are at least three different types of concerns that emerge from this examination. The first category involves cases that raise investigative concerns about the concealment of facts—in other words, claims of trade secrecy and confidentiality that companies or government agencies assert in order to forestall investigations by journalists, employee-whistleblowers, and others. The second category involves cases that raise concerns about the delegation of government functions, like voting, education, or criminal justice, to private entities. The third 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.

A. ANTI-INVESTIGATIVE CONCERNS IN CASES INVOLVING THE PUBLIC INTEREST

In an increasing array of contexts, companies or government agencies use trade secrecy and confidentiality agreements to prevent investigations by journalists, employee-whistleblowers, research scientists, and private parties. These incidents arise frequently in environmental disputes, but they can extend into clashes over the use of private technology in public infrastructure (discussed more in the next Section) and other efforts to suppress investigations into governmental or corporate practices in the public interest.

Pointedly, in all these cases, unlike most garden-variety trade secret disputes, the party seeking the information is not a competitor. Instead, the representative party is someone acting in the public interest, such as a journalist, a whistleblower, a research scientist, or a health professional. In such cases, trade secrecy often remains victorious even when the public interest in disclosure is readily apparent and even, at times, when there is a statutory responsibility to protect certain forms of disclosure. Finally, as we note below, much of the information that is sought involves basic facts, rather than products of innovation or substantial

efforts on behalf of the trade secret claimants.[45] In light of this distinction, trade secrecy risks becoming a vehicle for seclusion, not just a doctrine to promote innovation.

1. Data Secrecy in the Health and Environmental Contexts

In a recent article, Christopher Morten and Amy Kapczynski introduce a structural phenomenon that they describe as "data secrecy," which involves efforts by companies (and sometimes regulators) to keep health care safety information, including certain types of clinical research data, from the public.[46] The authors offer the example of Vioxx, which was a multibillion dollar drug for Merck before it was pulled abruptly from the market due to its link to heart attacks, strokes, and heart failure. Even though evidence showed that Merck and the Food and Drug Administration (FDA) were aware of these risks over three years before Vioxx's withdrawal, it did not make the data publicly available, leading to tens of thousands of deaths.[47]

As the authors describe, Vioxx is just one example of a widespread issue in the pharmaceutical industry, where trade secrecy essentially has enabled companies to seclude lifesaving information from the public. Again, the circularity of trade secrecy is the source of the problem. Because existing law allows a company to subjectively decide whether its clinical data constitutes confidential commercial information, this critical information is often kept from the public, including the scientific community.[48] As the authors point out, the information, at times, may satisfy the definition of a trade secret, but more often it involves information that the company would rather not make public for a variety of reputational reasons, such as the negative aspects of clinical data relating to "safety and efficacy."[49] Beyond clinical data, industry players have used trade secrecy to block state

45. By way of example, employee salaries or companies' potential violations of securities laws are facts and events that exist in the world; they are not the product of creative development efforts of the type intellectual property law seeks to incentivize.

46. *See* Christopher J. Morten & Amy Kapczynski, *The Big Data Regulator, Rebooted: Why and How the FDA Can and Should Disclose Confidential Data on Prescription Drugs*, 109 CALIF. L. REV. (forthcoming 2021) (manuscript at 2). Data secrecy has long been a focus of concern in the wake of the Hatch-Waxman Act. Drug Price Competition and Patent Term Restoration Act of 1984, Pub. L. No. 98-417, 98 Stat. 1585 (codified as amended at 21 U.S.C. § 355(j)–(k)); *see, e.g.*, Rebecca S. Eisenberg, *Data Secrecy in the Age of Regulatory Exclusivity*, *in* THE LAW AND THEORY OF TRADE SECRECY, *supra* note 11, at 467; Rebecca S. Eisenberg, *The Role of the FDA in Innovation Policy*, 13 MICH. TELECOMM. & TECH. L. REV. 345, 381, 383 (2007) (noting that data secrecy has been heavily criticized due to concerns of suppression of adverse effects in clinical trials and its effect on the flow of information).

47. *See* Morten & Kapczynski, *supra* note 46.

48. *See id.* at 5, 13–14, 22, 31–32, 35, 37 (focusing on safety-related data from companies' clinical study reports and FDA internal assessments from clinical trials and explaining that this "safety and efficacy data has little or no direct value to brand-name competitors . . . and thus will confer minimal or no competitive advantage to the company on whose behalf the FDA is currently maintaining secrecy"). We describe this phenomenon in greater detail in Part III with respect to FOIA.

49. *Id.* at 35.

regulators from acquiring pricing information,[50] and they have filed civil misappropriation lawsuits on the theory that prices constitute company trade secrets against a hospital consulting firm advising on price comparisons as well as a nonprofit that created a price benchmarking database for implantable medical devices.[51] We see analogous problems in environmental law and fracking regulation.

a. Trade Secrecy and Access to Environmental Information

This articulation of the notion of "data secrecy" provides us with a fruitful prism to explore a similar problem within environmental law, where "secret science" has also scuttled the investigatory capacities of journalists and scientists. In many statutes, including federal environmental statutes, that provide for the safety-enhancing forms of transparency, the law includes a variety of exemptions for trade secrecy.[52] These exemptions were readily enacted in the 1960s, as Mary Lyndon has explained, because early environmental challenges presented "few mysteries" and because trade secrets were perceived not as widespread but "as no more than an inconvenience to environmental management."[53]

Yet today, the number, variety, and complexity of environmental issues—and the processes of chemical production and distribution—have dramatically increased in the last few decades, altering the original balance of protection between trade secrecy, transparency, and public health.[54] Although chemical production has long raised public health considerations, hydraulic fracking, pesticides, and even cosmetics have also emerged as potential areas of concern. Moreover, because of an absence of federal regulation and the role of trade

50. *See* Robin Feldman & Charles Tait Graves, *Naked Price and Pharmaceutical Trade Secret Overreach*, 22 YALE J.L. & TECH. 61, 69–79 (2020) (documenting attempts by industry players called Pharmacy Benefit Managers (PBMs) to block pricing information); *see also* Robin Feldman, *Regulatory Property: The New IP*, 40 COLUM. J.L. & ARTS 53, 61–62 (2016) (describing the rise, in the life sciences industry, of quasi-trade secrets as a form of regulatory property in "data rights, in which other companies are prevented from using one's safety and efficacy data that were submitted to regulatory authorities and used as a basis for granting approval"). As pharmaceutical pricing, hospital pricing, and other medical costs remain a critical area of public concern, we expect additional studies challenging assertions of trade secrecy that operate to maintain high consumer costs.

51. *See* 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, 189–92 (2009) (describing lawsuits brought by a medical device manufacturer to prevent price comparisons and to maintain the high prices charged to hospitals, and addressing whether price information in the pharmaceutical context can be a trade secret). For a recent example of the intersections of trade secrecy and healthcare issues, see David S. Levine, *Covid-19 Should Spark a Reexamination of Trade Secrets' Stranglehold on Information*, STAT (July 10, 2020), https://www.statnews.com/2020/07/10/covid-19-reexamine-trade-secrets-information-stranglehold/ [https://perma.cc/WE3L-CHBL].

52. *See* Madeeha Dean, Note, *An Environmental FOIA: Balancing Trade Secrecy with the Public's Right to Know*, 109 CALIF. L. REV. (forthcoming Dec. 2021) (manuscript at 5, 9) (on file with authors) (summarizing statutes that provide exemptions).

53. *See* Mary L. Lyndon, *Trade Secrets and Information Access in Environmental Law*, *in* THE LAW AND THEORY OF TRADE SECRECY, *supra* note 11, at 443.

54. *See id.*

secrecy, these contexts have become somewhat impervious from investigation and disclosure.[55]

A study of these contexts over time reveals an important lesson: in many cases, the availability of trade secret exemptions produces an all-too-easy opening for near-absolute seclusion.[56] For example, under the Toxic Substances Control Act (TSCA), when a company seeks to produce a new chemical, it is required to file a notice with the EPA, but it is not required to perform health or safety studies on what it produces.[57] As an article in the *Intercept* notes, in 2007 the EPA reported that only about fifteen percent of new chemical notices carry any information about their potential health effects.[58] Why is this so? Even though the TSCA requires manufacturers to report information to the EPA if they reasonably believe that a substance they make or use "presents a substantial risk of injury to health or the environment," these companies can also withhold information about the substance by asserting confidentiality.[59]

---

55. *See id.* at 447 (studying the impact and rise of trade secrecy on environmental regulation and enforcement).

56. *See* Dean, *supra* note 52, at 11–12 ("Although trade secret exemptions in environmental laws attempt to balance intellectual property rights with reporting requirements, regulated entities can use the exemptions as loopholes to avoid oversight. The exemptions do not have clearly-defined boundaries and it is not readily apparent what information actually deserves protection as a trade secret or what standards the agency should use to reach its decision. Instead, Congress has given the EPA Administrator discretion to fill in the gaps and ultimately decide what should be withheld or released to the public.").

57. *See* Sharon Lerner, *A Chemical Shell Game: How DuPont Concealed the Dangers of the New Teflon Toxin*, INTERCEPT (Mar. 3, 2016, 3:51 PM), https://theintercept.com/2016/03/03/how-dupont-concealed-the-dangers-of-the-new-teflon-toxin [https://perma.cc/4Y72-JNBQ]. For example, the key statute involving chemical disclosure, the TSCA, directs the EPA to develop toxicity data and maintain a comprehensive inventory of chemicals. *See* 15 U.S.C. §§ 2601–2629 (2018). However, as Mary Lyndon has explained, it is "disabled by its own provisions" due to broad exemptions and minimal testing requirements. Lyndon, *supra* note 53, at 444; *see* 15 U.S.C. § 2613(c)(2).

58. *See* Lerner, *supra* note 57; *see also* Sharon Lerner, *New Evidence About the Dangers of Monsanto's Roundup*, INTERCEPT (May 17, 2016, 12:18 PM), https://theintercept.com/2016/05/17/new-evidence-about-the-dangers-of-monsantos-roundup [https://perma.cc/YR5D-9SGF] (discussing the impact of trade secrecy in concealing information about the potential dangers of herbicide Roundup).

59. Toxic Substances Control Act (TSCA) § 8(e), 15 U.S.C. § 2607(e); Lerner, *supra* note 57; *see* TSCA § 14(a) (prohibiting the EPA from disclosing any material that would fall within FOIA's Exemption 4 protections for trade secrecy to the public). In reviewing 100 reports by manufacturers, the Environmental Working Group found that one type of potentially harmful chemical had been withheld eighty-five percent of the time, even though it was linked to serious health effects, including death, kidney degeneration, maternal and developmental toxicity, among other issues. *See* Lerner, *supra* note 57. Many other environmental statutes have similar provisions for confidential business information. *See, e.g.*, Federal Insecticide, Fungicide, and Rodenticide Act of 1964 (FIFRA) § 10(a)–(b), 7 U.S.C. § 136h(a)–(b) (2018) (enabling applicant to designate information confidential if applicant believes that information to be a trade secret or confidential commercial or financial information); Federal Water Pollution Control Act (Clean Water Act) § 308(b), 33 U.S.C. §1318(b) (2018) (requiring public availability of records on effluent data, "except upon a showing satisfactory to the Administrator" that records would divulge methods or processes entitled to protection as trade secrets); Clean Air Act § 112 (r)(6)(Q), 42 U.S.C. § 7412(r)(6)(Q) (2018), *amended by* Act of Nov. 15, 1990, Pub. L. No. 101-549, 104 Stat. 2399 (allowing regulated parties to withhold information so long as a business has satisfactorily shown it would cause substantial harm to their competitive position); Emergency Planning and Community Right-to-Know Act of 1986 (EPCRA) § 322, 42 U.S.C. § 11042 (2018) (allowing

Further, under the Freedom of Information Act, manufacturers can resist disclosure of any information they decide falls under the Exemption 4 exceptions for trade secrets and for "commercial or financial information [that is] obtained from a person and privileged or confidential."[60] This provision was added to FOIA in 1966 and has remained ever since.[61] Typically, when submitting a request for information under FOIA to a federal agency, the agency decides if the requested information is authorized for release or if the request should be rejected. The FOIA includes nine exemptions; the most relevant here is Exemption 4.

As noted above, Exemption 4 creates a two-tier system for companies to claim exemptions from disclosure; there is an exemption not only for trade secrets but also for a looser category called confidential business information.[62] As one judge wrote, "FOIA is the legislative embodiment of Justice Brandeis's famous adage, '[s]unlight is . . . the best of disinfectants.'"[63] Yet at the same time the law recognized the value of transparency, Exemption 4 was driven by a recognition that "information, considered private and confidential in business life, should not be compromised simply because the information was transferred to government."[64]

As a result of this system, David Vladeck has argued, at the federal level, FOIA entitlements provide, at best, a piecemeal solution and, at worst, only an illusory right of access.[65] Because it is a request-driven statute, it is not oriented towards proactive disclosure of information to the public.[66] It thus requires initiating a legal dispute with an uncertain outcome, where an interested opponent may have superior resources. Moreover, commitment to FOIA transparency often varies with the political tides.[67] Finally, even though there are a litany of right-to-

anyone to withhold trade secret information from reporting, so long as the trade secrecy claim is substantiated in accordance with EPA regulations); *see* 40 C.F.R. § 2.208 (2014).

60. 5 U.S.C. § 552(b)(4) (2018).

61. Under one formulation, the second, broader exception applies if the information is considered by the defendant to be: "(a) commercial or financial, (b) obtained from a person, and (c) privileged or confidential." N.Y. Pub. Interest Research Grp. v. EPA, 249 F. Supp. 2d 327, 331–32 (S.D.N.Y. 2003).

62. *See* 5 U.S.C. § 552(b)(4) (2018) ("[T]rade secrets and commercial or financial information obtained from a person and privileged or confidential . . . .").

63. N.H. Right to Life v. U.S. Dep't of Health & Human Servs., 778 F.3d 43, 48–49 (1st Cir. 2015) (quoting LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT 92 (1914)); *see* FBI v. Abramson, 456 U.S. 615, 621 (1982); S. REP. NO. 813, at 3 (1965).

64. *See N.Y. Pub. Interest Grp.*, 249 F. Supp. 2d at 332.

65. *See* David C. Vladeck, *Information Access—Surveying the Current Legal Landscape of Federal Right-to-Know Laws*, 39 ENVTL. L. & POL'Y ANN. REV. 10773, 10779 (2009) ("The time has come to place an affirmative duty on government to use Internet technology to make environmental information accessible to the public without routinely having to use FOIA's request-and-wait procedures."); *see also* Dean, *supra* note 52, at 50 (suggesting an environmental FOIA to "require agencies to proactively disclose records in electronic form"). For an excellent, and critical treatment of FOIA, see David E. Pozen, *Freedom of Information Beyond the Freedom of Information Act*, 165 U. PENN. L. REV. 1097 (2017).

66. *See* Vladeck, *supra* note 65, at 10773.

67. *See id.* (describing an occasion when previous Attorney General John Ashcroft issued a directive to all federal agencies notifying them that the Department of Justice would readily defend any agencies who sought to withhold information from the public, as long as there was a plausible basis for the denial).

know laws in place to safeguard the public interest, they intrinsically conflict with exemptions for confidential business information, which comprise "the most frequently invoked justification for denying public access to environmental data."[68]

Indeed, decades of cases show that FOIA's original goal of increasing disclosure has been stymied by confidentiality exemptions, often at great risk to public health and safety. Indeed, although some courts have allowed for disclosure, others have not. In one case, discussed by Vladeck, a public interest organization was initially unable to access information in a FOIA case involving the cleanup of the Hudson River, which was severely contaminated with polychlorinated biphenyls (PCBs) released by the General Electric Corporation (GE).[69] GE had challenged the EPA's cleanup strategy, and both entities engaged in private, off-the-record meetings, eventually resulting in an outcome where GE would cover only a fraction of the cost of cleanup.[70]

When New York Public Interest Research Group (NYPIRG) filed a FOIA request to access information about these secret meetings, the EPA refused, citing Exemption 4 and noting that its records were marked "Privileged & Confidential."[71] After arguments over whether such information had commercial value, the court decided that the information did not reveal anything about the nature and character of GE's business, "or anything that a commercial business would want to protect for fear of competitive injury."[72] Instead, the court characterized the information as driven by a desire to convince the EPA to use a less expensive alternative.[73] The court noted that the Supreme Court had also emphasized that the exemptions to FOIA are also meant to be "'narrowly construed' in order that they do not swallow up this central purpose,"[74] particularly in light of the dominant interest in disclosure.[75]

That early decision set the balance in favor of disclosure, but it is important to note that case law—and agency practice—has been fairly mixed. In one case, when the Sierra Club requested documents under the Clean Air Act, the EPA withheld 18,000 pages out of a total of 21,685 pages under Exemption 4.[76] In another case, the District of Columbia Circuit found that Exemption 4 superseded a provision of the Clean Water Act requiring data on power plant emissions to be publicly available; this meant that even though citizens had a statutory *right to*

68. *Id.* at 10774.

69. *See id.* at 10776.

70. *See id.*

71. *See id.* at 10776–77 (discussing *N.Y. Pub. Interest Grp.*, 249 F. Supp. 2d at 329–30).

72. *Id.* at 10777 (quoting *N.Y. Pub. Interest Grp.*, 249 F. Supp. 2d at 333).

73. *Id.* (citing *N.Y. Pub. Interest Grp.*, 249 F. Supp. 2d at 333–34).

74. *See N.Y. Pub. Interest Grp.*, 249 F. Supp. 2d at 334 (quoting FBI v. Abramson, 456 U.S. 615, 630 (1982)).

75. *See id.* (citing Wash. Post Co. v. U.S. Dep't of Health & Human Servs., 865 F.2d 320, 324 (D.C. Cir. 1989)).

76. *See* Entergy Gulf States La., L.L.C. v. EPA, 817 F.3d 198, 201 (5th Cir. 2016) (primarily addressing the organization's right to intervene because its interests were not aligned with the EPA's interests, but noting the number of documents withheld on confidentiality grounds).

disclosure, they still could not obtain the information.[77] These examples demonstrate that expansive readings of FOIA Exemption 4, in favor of confidentiality, can impede access to information that otherwise would be available to the public.

b. Chemical Data Secrecy and Fracking

We see similar outcomes in the context of chemical data, where data secrecy poses conflicts with public health and safety. Although chemical data falls into traditional areas of trade secret protection in most cases, recent issues have suggested the emergence of concealment in a variety of new technologies affecting public health. Scholars have expressed concerns about the potential rise of trade secret claims in areas as diverse as hydraulic fracking, genetically modified foods, synthetic fragrances, e-cigarettes, cosmetics, and flame retardants.[78] In such situations, even when scientists and journalists are attempting to research the impacts of chemical production, companies have learned to deploy trade secrecy as a weapon against investigation.

For example, in the context of most chemical data, even though case law has found that common names and related information for inert ingredients (without the precise formulas) do not fall within Exemption 4, much of the applicable law still defers strongly to a claimant's determination.[79] According to one report from the Government Accountability Office, *ninety-five percent* of new notifications (and almost 18,000 chemicals) are designated under Exemption 4 and withheld from the public.[80] As a result of this designation, only a small fraction of government personnel have clearance to receive access to the product.[81] The confidentiality or secrecy designation makes it difficult to study chemicals and their effects; as one scientist argued: "Scientists can't search for contaminants if they don't know what they're looking for."[82] Studies of the health effects of various chemicals have been claimed under the exemption and kept from the public.[83] And even when chemicals are abandoned from use, often the impact remains; as Mary Lyndon observes, "The social cost of the original secret become greater

77. *See* Envtl. Integrity Project v. EPA, 864 F.3d 648, 649 (D.C. Cir. 2017) (noting Clean Water Act does not supersede Exemption 4). *But see* Graff v. Haverhill N. Coke Co., No. 1:09-cv-670, 2011 WL 13161211, at *2–3 (S.D. Ohio Feb. 28, 2011) (finding that emissions data was not a protectable trade secret). Case law is also mixed in its results. *See* Nat'l Ass'n of Home Builders v. Norton, 309 F.3d 26, 38–39 (D.C. Cir. 2002) (rejecting such a designation for owl-sighting data because it was noncommercial); Am. Airlines, Inc. v. Nat'l Mediation Bd., 588 F.2d 863, 870 (2d Cir. 1978) (adopting a confidentiality designation for information provided to the government concerning recruitment efforts by labor unions).

78. *See* Julie E. Zink, *When Trade Secrecy Goes Too Far: Public Health and Safety Should Trump Corporate Profits*, 20 VAND. J. ENT. & TECH. L. 1135, 1156–57 (2018) (listing these areas of concern).

79. *See* Nw. Coal. for Alts. to Pesticides v. Browner, 941 F. Supp. 197, 202 (D.D.C. 1996).

80. According to one Intercept report, the confidential business information designation has been used to withhold the name and identity of 17,585 different chemicals registered with the EPA. Lerner, *supra* note 57.

81. *See id.*

82. *See id.* (quoting David Andrews, Senior Scientist, Environmental Working Group).

83. *See id.*

with the passage of time, as the effect becomes more costly to identify and remedy."[84]

One may ask how today's corporate behavior is different from other contexts, such as the tobacco industry, where companies have often paid millions to silence or dilute research into the harmful effects of their products and to resist calls for disclosure. The difference here lies in the exploitation of the deference enjoyed by a would-be trade secret owner. Because regulated parties are able to designate certain information as a trade secret, they can ensure that the information remains private. Courts can be biased toward accepting the claimant's account of what does or does not count as a trade secret because the claimant presents that narrative, and courts may not be well-positioned to challenge such assertions without robust submissions by opponents showing otherwise.[85] Even in today's era, where government regularly touts the value of the "open data" movement, trade secrecy remains a right that is too often impenetrable.[86]

In addition, in many such cases, it is often difficult to disentangle assertions of trade secrecy from an underlying resistance to regulation and lack of regulatory oversight. One contemporary area involves a similar issue that has arisen regarding hydraulic fracturing (fracking): a practice that involves the high-pressure injection of fluids into bedrock formations for the purpose of oil or gas extraction.[87] The fluids that are used are mostly composed of water and sand, but gas drillers add numerous chemicals to the mix that are known for their environmental harms, as well as their carcinogenic effects, posing harms to livestock and

84. Lyndon, *supra* note 53, at 450; *see* Zink, *supra* note 78, at 1144–56. In one example involving the chemical perfluorooctanoic acid (PFOA), E.I. du Pont de Nemours & Co. knowingly suppressed information about its health risks for decades, even when another company reported its concerns to DuPont, and employees were known to regularly contract "Teflon flu," which involved symptoms of fever, nausea, diarrhea, and vomiting. Zink, *supra* note 78, at 1146. DuPont sought to keep the information secret for decades, even after its employees gave birth to children with birth defects. *See id.* at 1147, 1150 (detailing research and PFOA's link to testicular, pancreatic, and liver tumors as well as kidney cancer, thyroid disease, high cholesterol, preeclampsia, and ulcerative colitis). Eventually, DuPont settled after a prominent EPA investigation, agreeing to phase out its production and pay a hefty fine. *Id.* at 1149. Yet years after the settlement, two EPA investigators discovered, using nearby water samples, that DuPont's chemical replacements for PFOA likely had "the same chemical performance properties," suggesting similarity risks of toxicity as well. Lerner, *supra* note 57. Yet their work was stymied by the persistence of confidentiality designations that precluded their investigations. *See id.*

85. Zink tells a similar story about genetically modified organisms (GMO). Although the history of regulating GMOs is fairly complex due to overlapping agency jurisdictions, the GMO industry has managed to exempt itself from the "most important environmental and consumer protection laws." Zink, *supra* note 78, at 1164. As a result, companies can choose what research and information they wish to disclose, and can designate such information as a trade secret. *Id.* at 1164–65 (citing Elizabeth A. Rowe, *Patents, Genetically Modified Foods, and IP Overreaching*, 64 SMU L. REV. 859, 876–77 (2011)).

86. *See* Ayanna Alexander, *Pesticide Makers Back Public-Data Plan—But Not for Trade Secrets*, BLOOMBERG (April 27, 2018, 11:23 AM); *see also* Vladeck, *supra* note 65 (discussing FOIA and environmental law).

87. *See* Zink, *supra* note 78, at 1158.

humans such as burning sensations, gastrointestinal distress, and upper-respiratory ailments.[88]

In one incident, a fire erupted at a fracking plant, leaking thousands of chemicals into a tributary of the Ohio River, causing the deaths of more than 70,000 fish and risking the safety of the local drinking water for millions.[89] Yet despite these issues, it took Halliburton at least five days to reveal its chemical compounds to the EPA and its state equivalent, in part due to the state law supporting trade secrecy.[90] In fact, as one scholar writes, in the aftermath, "authorities responsible for local drinking water, as well as local residents, never even fully learned the identity of these secret 'proprietary' chemicals despite the high probability that the water supply had been tainted by them."[91] Indeed, despite the risks to the public, at least ten states allow fracking well operators to withhold trade secret content from *medical professionals* treating patients exposed to the fluid, making it difficult for them to treat patients harmed by chemical exposure.[92]

Fracking is an example of how trade secrecy exemptions, coupled with a patchwork of reduced disclosure requirements across states, can create a perfect storm to impede public oversight and investigation. Given that trade secret law is designed in part to defer to would-be owners' judgment, companies have swiftly learned to use trade secrecy as a shield to forestall inquiry. Further, because hydraulic fracking is uniquely exempt from all of the potential federal environmental laws—including the Clean Air Act and others—that could normally apply to such situations, companies are often able to evade calls for transparency by arguing that fracking "is a highly complex and competitive industry where trade secrets are critical assets."[93] Companies claim that if even the names of chemicals were released, competitors could reverse engineer their formulas, destroying their secrecy.[94]

In turn, state regulation is inconsistent, with some states relying on self-designation of trade secrets, others requiring an administrative determination by a state

88. *See id.* at 1158–59.

89. Elliot Fink, *Dirty Little Secrets: Fracking Fluids, Dubious Trade Secrets, Confidential Contamination, and the Public Health Information Vacuum*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 971, 973–74 (2019).

90. *Id.*

91. *Id.* at 974.

92. *See* Kellie Fisher, *Communities in the Dark: The Use of State Sunshine Laws to Shed Light on the Fracking Industry*, 42 B.C. ENVTL. AFF. L. REV. 99, 111 (2015); *see also* Matthew McFeeley, *Falling Through the Cracks: Public Information and the Patchwork of Hydraulic Fracturing Disclosure Laws*, 38 VT. L. REV. 849, 853 (2014). *But see* Robinson Twp. v. Commonwealth, 147 A.3d 536, 575–76 (Pa. 2016) (overturning act preventing medical professionals from disclosing the chemical composition of fracturing fluids and noting that such restrictions on health professionals are "enjoyed by no other class of industry").

93. Zink, *supra* note 78, at 1160 (quoting a representative from the industry); *see id.* at 1162 (noting how fracking is exempt from the Clean Air Act, Clean Water Act, and Safe Drinking Water Act, among other federal statutes).

94. *See* Fisher, *supra* note 92, at 110.

agency, and even fewer requiring substantiation of the trade secret.[95] Of the thirty-one states that have fracking activity, almost half do not have any disclosure requirements.[96] Even when submitting information, some states allow well operators to designate chemical information for exemptions to disclosure.[97] For example, in Texas, after the state adopted a disclosure law, companies claimed confidentiality protection 10,120 times in a total of 12,140 reporting instances tied to fracking; in one federal report from 2014, the Department of Energy found that trade secrecy was invoked eighty-four percent of the time in fracking cases.[98]

Finally, in 2015, the Bureau of Land Management (BLM), in the first federal regulation to address fracking and issues of secrecy directly, adopted a rule that, among other things, would require chemical disclosure and allow for trade secret exemption only after a BLM determination.[99] But, the rule's primary value lays in a clear refusal to defer to the private company in determining the scope of secrecy. By placing this determination in the hands of the BLM, rather than

95. *See* Melanie McCormick, *Conflicting Theories at Play: Chemical Disclosure and Trade Secrets in the New Federal Fracking Regulation*, 9 GOLDEN GATE U. ENVTL. L.J. 217, 218 (2016) (citing McFeeley, *supra* note 92, at 872–75, 887–88).

96. *See* NATHAN RICHARDSON, MADELINE GOTTLIEB, ALAN KRUPNICK & HANNAH WISEMAN, THE STATE OF STATE SHALE GAS REGULATION 1 (2013), https://media.rff.org/documents/RFF-Rpt-StateofStateRegs_ExecSumm_0.pdf [https://perma.cc/JJ3C-5DC3]; Isabelle Weber, *How State Regulations Hold Us Back and What Other Countries Are Doing About Fracking*, FRACTRACKER (Oct. 10, 2019), https://www.fractracker.org/2019/10/regulations-by-country [https://perma.cc/BA7M-A5KJ] (illustrating disclosure requirements by state in Figure 1); *see also* Fink, *supra* note 89, at 989–90 (citing T. Robert Fetter, Fracking, Toxics, and Disclosure 6–7 (Aug. 13, 2017) (unpublished manuscript), https://perma.cc/Q5XE-U5TD). Some states require the company to send a list of its chemicals to the state oil and gas commission, which then approves a list of chemicals that are deemed to be trade secrets. *See* Fisher, *supra* note 92, at 110. Others require a public disclosure of chemicals but enable disclosers to exclude chemicals that companies deem to be trade secrets. *Id*. at 110–11. In one case challenging a state agency's determination of trade secrecy under the rules for public disclosure, a court granted summary judgment to the fracking company, deferring to the agency's determination in favor of secrecy. *See* Powder River Basin Res. Council v. Wyo. Oil & Gas Conservation Comm'n, No. 94650, 2013 WL 8718518, at *9 (Wyo. Dist. Ct. Mar. 21, 2013), *rev'd*, 2014 WY 37, 320 P.3d 222 (Wyo. 2014). Although the case was eventually reversed by the Wyoming Supreme Court, which remanded for a closer factual determination of secrecy, it illustrates the high degree of deference enjoyed by companies even when another agency is tasked to determine secrecy.

97. *See* MATTHEW MCFEELEY, NAT. RES. DEF. COUNCIL, STATE HYDRAULIC FRACTURING DISCLOSURE RULES AND ENFORCEMENT: A COMPARISON 6, 12 (2012). At least seventy percent of disclosures made on FracFocus included at least one ingredient designated for a confidentiality exemption in 2015. *See* U.S. ENVTL. PROT. AGENCY, ANALYSIS OF HYDRAULIC FRACTURING FLUID DATA FROM THE FRACFOCUS CHEMICAL DISCLOSURE REGISTRY 1.0, at 17 (2015); *see also* McFeeley, *supra* note 92, at 862–63 (discussing states' use of FracFocus to facilitate well operators' disclosure of fracking chemicals).

98. Fink, *supra* note 89, at 1002; *see* U.S. DEP'T OF ENERGY, SECRETARY OF ENERGY ADVISORY BOARD TASK FORCE REPORT ON FRACFOCUS 2.0, at 5, 11 (2014) (describing exemption data from FracFocus). As of 2016, the EPA identified 1,606 chemicals in fracking fluid and wastewater but only had information on 173 of those chemicals, noting that the lack of cooperation by the drilling industry prevented an assessment of its impacts on drinking water. U.S. ENVTL. PROT. AGENCY, HYDRAULIC FRACTURING FOR OIL AND GAS: IMPACTS FROM THE HYDRAULIC FRACTURING WATER CYCLE ON DRINKING WATER RESOURCES IN THE UNITED STATES 9-8 to 9-10, 9-16 (2016).

99. *See* McCormick, *supra* note 95, at 226–27.

deferring to the claimant, the proposed rule took a path that may prove fruitful to follow in the future. Unfortunately, that rule was rescinded by the Trump administration two years later.[100]

2. Freedom of Information Act Cases after *Argus Leader*

Strikingly, in recent years, the Trump Administration effectively used its power to oppose calls for disclosure, aligning itself with private interests in sometimes extreme postures. Although there are many strategic reasons for the government's position, it is important to note that this outcome is also made possible by the deference to the information holder's claims of confidentiality that FOIA facilitates.[101] As a result, even though the purpose of FOIA is to avoid agency capture by disclosing information to the public, it has been less effective than originally hoped.[102]

Courts customarily defer to the agency's determination, with little role for judicial oversight. As a result, because courts are not expected to cast much scrutiny over such determinations, there are few "checks" in the system of deference, even when disclosure might be required by law.[103] Even though courts and agencies tend to speak of the need to "balance" interests, the system has been described as "unworkable" due to its underlying paradox: the information is needed because it is secret, but "[s]ecrecy prevents the development of the very information needed to make a balanced assessment."[104]

New developments may foreshadow an even less effective FOIA. As Varadarajan explains in her study, historically, the "trade secret" exemption under FOIA mostly has been limited to protecting information with a "direct relationship [to] the productive process," thus limiting its scope to technical information, or what we call traditional trade secret coverage.[105] And until recently, the second category secluding other forms of commercial information, also required evidence of "substantial competitive harm" flowing from competitors' affirmative use of the information upon disclosure.[106] These background limitations, she writes, functioned to limit at least some degree of corporate attempts to avoid disclosure.[107]

---

100. *See* U.S. DEP'T OF THE INTERIOR, BUREAU OF LAND MGMT., BLM RESCINDS RULE ON HYDRAULIC FRACTURING (Dec. 28, 2017), https://www.blm.gov/press-release/blm-rescinds-rule-hydraulic-fracturing [https://perma.cc/A6HY-4S4T] (noting rescission).

101. Another criminal statute, the Trade Secrets Act, prohibits government employees from disclosing information that comprises a trade secret, further contributing to government reluctance to share information. *See* Al-Amyn Sumar, *Unpacking FOIA's "Foreseeable Harm" Standard*, 35 COMM. LAW. 15, 19 (2020).

102. *See* Lyndon, *supra* note 53, at 463.

103. *See id.* at 444 ("Courts reviewing FOIA cases have tended to leave disclosure to agencies' discretion, while regulated firms have pressed agencies for broad confidentiality. . . . [A]gencies are poorly positioned to resist this pressure and often capitulate, even when they have a statutory mandate to disclose the information.").

104. *Id.* at 463.

105. Varadarajan, *supra* note 11, at 5 (alteration in original).

106. *Id.*

107. *See id.* at 5–6.

This changed when the Supreme Court handed down *Food Marketing Institute v. Argus Leader Media* in 2019.[108] In that case, a business association representing grocery stores resisted a newspaper's FOIA request for the identification of stores participating in a United States Department of Agriculture food stamp program.[109] The grocery stores argued that disclosure of food stamp acceptance might cause competitors to build new grocery stores nearby in order to increase their market share of low-income customers.[110] Ruling against disclosure, the Supreme Court explicitly rejected older circuit case law requiring a substantial competitive harm to support concealment. Instead, it cast a wide mantle of secrecy, directing that "where commercial or financial information is both customarily and actually treated as private by its owner and provided to the government under an assurance of privacy," it may be secluded under Exemption 4's confidentiality exception.[111] The decision therefore shifted the controlling test from a more objective measure of meaningful harm to a more subjective measure focused on the claimant's own practices.

While the decision notably does not analyze the role of trade secrecy under FOIA, its embrace of confidentiality, more broadly, aligns with an expansive notion of corporate seclusion, signaling a degree of collapse between the two categories.[112] Because the confidentiality exemption is so broad, companies can assert that any information outside the boundaries of trade secrecy is nonetheless "confidential." *Argus Leader* makes it easier for companies to claim the second exemption against disclosure by removing courts' abilities to test fanciful or exaggerated claims of harm.[113]

Effectively, the *Argus Leader* formulation emboldens government attorneys to advance a theory that, if credited by the courts, could give companies an unlimited veto power over FOIA requests. The result of *Argus Leader*, commentators have concluded, is a sizeable expansion of Exemption 4.[114] And there is evidence that it is effective at seclusion. At least one court concluded that Exemption 4 protected the Department of Defense's subcontracting information with Lockheed Martin because the information was customarily treated as confidential by the Defense Department; in its opinion, the court duly noted that it was "sympathetic to plaintiff's steep uphill battle under the new Exemption 4 standard," but was powerless in the face of *Argus Leader* to reach a different conclusion.[115]

In addition, as described above, when the Center for Investigative Reporting sought Department of Labor records showing companies' submissions regarding diversity data and workplace injury information in different cases, the

108. 139 S. Ct. 2356, 2366 (2019).
109. *See id.* at 2361.
110. *See id.*
111. *Id.* at 2366.
112. *See* Varadarajan, *supra* note 11, at 5–6.
113. *See Argus Leader Media*, 139 S. Ct. at 2366.
114. *See* Varadarajan, *supra* note 11, at 33.
115. *Id.* (quoting and discussing Am. Small Bus. League v. U.S. Dep't of Def., 411 F. Supp. 3d 824, 832 (N.D. Cal. 2019)).

government opposed the requests. It did so by relying on the boilerplate affidavits of various companies' representatives in the process. In each case, the government argued that this type of information fell within the ambit of "confidential" information because it comprised "information in which the establishments have a commercial interest, information that deals with commerce, and information that is related to business or trade."[116] Following *Argus Leader*, the government argued that the subject data "is confidential because it is 'customarily and actually treated as private by its owner.'"[117] It further classified workplace injury reports as "critical to [a company's] operational mission and commercial success."[118]

Consider, for a moment, the tautological nature of this argument—that the information is confidential because the party seeking seclusion declares it to be confidential. In one case, the government went so far as to argue, in the context of diversity data, that "[i]t would not make sense for the companies to undertake the extensive efforts described below to maintain the confidentiality of the reports if these companies did not believe that the data was directly related to various aspects of their business."[119] In another case, the government asserted that the information needed to be confidential because employers had represented to employees that it was confidential, not for any reason tied to the nature of the information.[120]

These arguments have significant implications. If courts were to accept such arguments, companies might be able to circumvent FOIA requests simply by declaring that the information at issue is commercial in nature because it has a connection to a workplace, and that it is confidential because the employer says so. As we discuss further in Part II, these post-*Argus Leader* formulations are especially problematic because they overlook the type of market-competitive information that is historically considered to be a trade secret, and because they could lead courts to credit an employers' assertions of confidentiality, unmeasured and largely without question, even for nontraditional types of information. But perhaps most troubling, these arguments jettison the very purpose of FOIA's exemptions, which is to aim for disclosure in cases of public interest. As one court noted, years before *Argus Leader*, Exemption 4 was actually "intended to

116. Defendant's Motion for Summary Judgment at 13, Ctr. for Investigative Reporting v. U.S. Dep't of Labor, No. 18-cv-02414-DMR, 2020 WL 2995209 (N.D. Cal. June 4, 2020), ECF No. 26.

117. *See id.* at 14–15 (capitalization omitted). The commenters included groups like the National Association of Manufacturers, the National Retail Federation, and the American Fuel & Petrochemical Manufacturers. *See id.* at 16 n.8.

118. Defendant's Motion for Summary Judgment at 12, Ctr. for Investigative Reporting v. U.S. Dep't of Labor, 470 F. Supp. 3d 1096 (N.D. Cal. 2020) (No. 3:19-cv-05603-SK), ECF No. 25 (workplace injury case against the Department of Labor).

119. Motion for Summary Judgment at 11, Ctr. for Investigative Reporting v. U.S. Dep't of Labor, 424 F. Supp. 3d 771 (N.D. Cal. 2019) (No. 4:19-cv-01843-KAW), ECF No. 24 (diversity data submitted to the EEOC).

120. *See id.* at 12 ("Part of why the confidentiality of the reports is taken so seriously is because when the companies collect the demographic information from potential employees in order to obtain the relevant data for the reports, they provide assurances to these individuals that the information will be held in confidence; the companies do not want to breach the trust with their employees.").

stimulate information-sharing with the government, not to shield government decision making from public scrutiny."[121]

3. Challenging the Whistleblower

Another factor hampering investigations in the public interest is the uncertain status of whistleblower protection when a company sues an employee for trade secret misappropriation. Given the deference afforded to the would-be trade secret owner, and the information asymmetry that it produces, often the only way to discover or investigate corporate wrongdoing is if an employee or other insider comes forward to report events behind company walls. This makes the enactment of whistleblower protection particularly important, but it has had only mixed results thus far. Despite recent legal protections for whistleblowers, secrecy can still remain paramount, harming the public interest in exposing wrongdoing.

In 2016, while enacting a new federal civil remedy for trade secret misappropriation, Congress recognized that trade secret protections can in some instances harm the public interest.[122] Thus, the DTSA included a clause aimed at protecting employee-whistleblowers who follow a prescribed path for the purpose of reporting a possible violation of law.[123] Specifically, if a whistleblower suspects that the company has broken a law and discloses a trade secret to an attorney or to law enforcement when reporting that potential violation, he or she receives immunity from a state or federal misappropriation claim.[124]

This provision was also meant to correct a serious issue that had arisen in state trade secret law before the DTSA's May 2016 enactment, where trade secret misappropriation claims were filed against would-be whistleblowers with varying and unpredictable results.[125] Senate Judiciary Committee Chairman Charles Grassley stated:

---

121. *See* Varadarajan, *supra* note 11, at 22.

122. *See* Press Release, Senator Chuck Grassley, Leahy-Grassley Amendment Protecting Whistleblowers Earns Unanimous Support in Judiciary Committee (Jan. 28, 2016), https://www.grassley.senate.gov/news/news-releases/leahy-grassley-amendment-protecting-whistleblowers-earns-unanimous-support [https://perma.cc/KAS9-9JU8].

123. *See* Defend Trade Secrets Act § 7(b)(1), 18 U.S.C. § 1833(b)(1) (2018) ("Immunity from Liability for Confidential Disclosure of a Trade Secret to the Government or in a Court Filing." (capitalization of articles, prepositions, and conjunction omitted)). This clause protects whistleblowers where they disclose information to a government official or their attorney, or in a court filing under seal, for the purpose of addressing a violation of law. *Id.* Notably, the immunity does not encompass disclosure to the media or self-publication on the internet.

124. *See id.* The provision was designed, in part, to follow Peter Menell's groundbreaking work outlining the need for a public policy exception to protect whistleblowing activity. *See generally* Menell, *supra* note 8; Peter S. Menell, *The Defend Trade Secrets Act Whistleblower Immunity Provision: A Legislative History*, 1 BUS. ENTREPRENEURSHIP & TAX L. REV. 398 (2017).

125. *See, e.g.*, Cafasso v. Gen. Dynamics C4 Sys., Inc., 637 F.3d 1047, 1062 (9th Cir. 2011) (granting summary judgment against employee, where employer had pursued counterclaim for breach of confidentiality agreement against employee for taking documents, and recognizing but not applying a public policy exception for whistleblowers, in part, because were it to have "adopt[ed] a public policy exception to confidentiality agreements to protect relators . . . those asserting its protection would need to justify why removal of the documents was reasonably necessary to pursue an FCA claim"); E.A. Renfroe & Co. v. Moran, 249 F. App'x 88, 92 (11th Cir. 2007) (upholding a preliminary injunction that

> Too often, individuals who come forward to report wrongdoing in the workplace are punished for simply telling the truth. The amendment . . . ensures that these whistleblowers won't be slapped with allegations of trade secret theft when responsibly exposing misconduct. It's another way we can prevent retaliation and even encourage people to speak out when they witness violations of the law.[126]

Essentially, "[t]he DTSA whistleblower immunity regime aims to hold companies accountable for possible misconduct by allowing authorities to scrutinize trade secrets" in a manner that retains their secrecy.[127] This DTSA provision strikes a delicate—and important—balance that enables disclosure for the purposes of law enforcement and investigation, but because the information needs to be disclosed to a lawyer or law enforcement, it disincentivizes wanton disclosure without advice of counsel or oversight by law enforcement.[128] It recognizes whistleblowers as "quasi-public actors," or "private attorneys general," as a result.[129]

Yet problems with interpreting this new clause arose in the first reported decision to address it. In *Unum Group v. Loftus*, a company sued a departing employee for taking documents under the DTSA, adding a Massachusetts trade secret claim and a conversion claim.[130] When the employee raised the DTSA immunity clause, however, the court labeled it an "affirmative defense" and entered a preliminary injunction requiring return or destruction of the documents. The court reasoned that although the employee had delivered the documents to his attorney, he had not yet filed a whistleblower lawsuit.[131]

---

prohibited former employees from disclosing or using copies of 15,000 insurance claim-related documents where employees had sought to expose fraudulent and potentially criminal activities related to the disposition of insurance claims and shared documents with a lawyer, a state attorney general, and the FBI); Xyngular Corp. v. Schenkel, 200 F. Supp. 3d 1273, 1318–19 (D. Utah 2016) (finding that employee's conduct was not immunized by separate whistleblowing activity and awarding sanctions where company had sued employee for breach of contract for taking "confidential" documents); United States *ex rel.* Alvord v. Lakeland Reg'l Med. Ctr., Inc., No. 8:10–cv–52–T–17EAJ, 2012 WL 12904676, at *3–6 (M.D. Fla. Sept. 14, 2012) (noting conflicting case law as to whether confidentiality contracts operate against employee-whistleblowers and denying dismissal as to whistleblower claim because defendant provided copies of the documents at issue to her attorney in connection with her FCA claim); JDS Uniphase Corp. v. Jennings, 473 F. Supp. 2d 697, 702 (E.D. Va. 2007) (finding that employee violated confidentiality contract under California law despite his argument that documents taken were necessary to pursue wrongful discharge claim and to act as whistleblower for alleged Sarbanes–Oxley violations).

126. *See* Press Release, Senator Chuck Grassley, *supra* note 122.

127. Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 130–31 (2019); *see* Peter S. Menell, *Misconstruing Whistleblower Immunity Under the Defend Trade Secrets Act*, 1 NEV. L.J.F. 92, 92 (2017).

128. *See* Katyal, *supra* note 127, at 139.

129. Menell, *supra* note 127, at 93.

130. 220 F. Supp. 3d 143, 145 (D. Mass. 2016). The decision does not identify what kind of whistleblower action Loftus planned. *See id.* at 146 n.2 The plaintiff also moved for a preliminary injunction quickly, such that the court heard it alongside the defendant's motion to dismiss. *See id.* at 145–47.

131. *See id.* at 147 ("[T]he record lacks facts to support or reject his affirmative defense at this stage of litigation. There has been no discovery to determine the significance of the documents taken or their

Peter Menell, whose work inspired the DTSA exception, strongly criticized the *Loftus* court for treating a statutory immunity as an affirmative defense that the defendant must establish in the course of litigation on the merits.[132] Indeed, establishing an affirmative defense requires a win on the merits at summary judgment or even trial—after perhaps a year or more of discovery and motion practice against a significantly more powerful opponent—a process which defeats the purpose of an immunity from suit. And although at least one court has squarely dismissed a DTSA misappropriation claim based on the statutory immunity,[133] others have followed *Loftus*, requiring former employees to establish immunity as an affirmative defense.[134]

In the meantime, despite the DTSA, employers have continued to bring state law trade secret misappropriation claims against whistleblower employees, again with mixed success.[135] What is most interesting about these recent cases is that

contents, and Loftus has not filed any potential lawsuit that could be supported by information in those documents.").

132. *See* Menell, *supra* note 127, at 95 ("[T]he court ignores the vaccine and subjects Loftus to the very disease that Congress cured: the imposition of substantial costs and adverse career repercussions by sharing, in confidence, company documents with counsel."). For a different perspective on immunity, see Kristine Craig, *The Pragmatic Disappointment of State Preemption: The 2016 Defend Trade Secrets Act and Its Failure to Protect Employee Whistleblowers from Federal Computer Crime Law*, 44 J. LEGIS. 284, 301 (2017) (arguing that Menell's conception of DTSA immunity as immunity from suit is overbroad and does not reflect the balance Congress sought to achieve with the whistleblower amendment); and James Pooley, *The Defend Trade Secrets Act: A Year Later*, 268 MANAGING INTELL. PROP. 38, 41 (2017) (noting issues surrounding whistleblower immunity).

133. *See* Christian v. Lannett Co., No. CV 16-963, 2018 WL 1532849, at *4 (E.D. Pa. Mar. 29, 2018) (dismissing former employee's DTSA counterclaim where the employee's sharing with her attorney some 22,000 documents from her former employer in support of her discrimination claim against the employer fit within the statutory immunity provision).

134. *See* Garcia v. Vertical Screen, Inc., No. CV 19-3184, 2020 WL 2615624, at *5 (E.D. Pa. May 22, 2020) (treating immunity as an affirmative defense, which may only be decided at the motion to dismiss stage where "the predicate establishing the defense is apparent from the face of the complaint" (quoting Bethel v. Jendoco Constr. Corp., 570 F.2d 1168, 1174 n.10 (3d Cir. 1978))); Argos USA LLC v. Young, No. 1:18-CV-02797-ELR, 2019 WL 4125968, at *6 (N.D. Ga. June 28, 2019) (citing *Loftus*, 220 F. Supp. 3d at 147) (refusing to dismiss trade secret misappropriation claims based on defendants' immunity argument); 1-800 Remodel, Inc. v. Bodor, No. CV 18-472-DMG (EX), 2018 WL 6340759, at *6 (C.D. Cal. Oct. 17, 2018) (citing *Loftus*, 220 F. Supp. 3d 147) (holding that, at the pleading stage, court could not assume that the immunity provision bars plaintiff's DTSA and California UTSA claims arising out of defendant's anticipated and actual disclosure of proprietary information).

135. *See* Erhart v. BofI Holding, Inc., No. 15-cv-02287-BAS-NLS, 2020 WL 1550207, at *6–17 (S.D. Cal. Mar. 31, 2020) (denying, in action where plaintiff-employer brought claims against defendant-employee under state tort law and Computer Fraud and Abuse Act, plaintiff-employer's motion for summary adjudication on defendant-employee's affirmative defenses because court found merit to a public policy exception to confidentiality agreements to protect whistleblowers who appropriate company documents, and that whistleblowers often need documentary evidence to substantiate their allegations, thus finding triable issues of fact regarding employee's conduct); Client Network Servs., Inc. v. Smith, No. PWG-15-2207, 2017 WL 3968471, at *5–6 (D. Md. Sept. 8, 2017) (denying motion for summary judgment for defendant-employee on former employer's breach of contract claim where defendant-employee had not reported suspected criminal wrongdoing to the authorities, but holding, however, that a Maryland contract would be invalid to the extent it barred an employee from making such a report); Anheuser-Busch Cos. v. Clark, No. 2:13-cv-00415-TLN-CKD, 2017 WL 1093907, at *7–10 (E.D. Cal. Mar. 23, 2017), *aff'd*, 764 F. App'x 594 (9th Cir. 2019) (denying defendant-employee's anti-SLAPP motion despite defendant-employee's assertion of California state

many of them appear designed to evade the DTSA. Although the DTSA's immunity provision applies to any "state trade secret law" as well,[136] in at least some of these post-2016 cases employers have proceeded under contract or tort law instead of an express claim for trade secret misappropriation, presumably to plead around potential whistleblower protection by avoiding a cause of action with the phrase "trade secret" in it.[137] In other words, these companies may be carefully selecting the causes of action they choose to press to evade a statutory immunity for the conduct they seek to suppress. As a result, employers' abilities to pursue nontraditional trade secrecy assertions against whistleblowers (rather than those seeking to use information for marketplace competition), and the degree to which employees can be protected from such claims, remains ambiguous.[138]

B. DELEGATIVE CONCERNS REGARDING GOVERNMENT INFRASTRUCTURE

Today, as several scholars have noted, government entities rely on an ever widening range of private parties for any number of purposes—from management of detention facilities, to the provision of voting machines, to relying on algorithms to calculate Medicaid benefits and bail amounts, and to assessing educator performance.[139] This tendency to rely on private vendors to perform government functions has been deemed "government by contract" by Jody Freedman and Martha Minow.[140] As Gillian Metzger has observed, "[p]rivatization is now virtually a national obsession."[141] In cases where a government is relying on a private

law whistleblower protection statute against former employer's trade secret claim because defendant had disclosed information to attorneys to further a class action litigation but did not report to government authorities).

136. 18 U.S.C. § 1833(b)(1) (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 . . . .").

137. For examples of such cases, see *supra* note 135. Attorneys representing employees in whistleblower actions where the employer brings a tort claim should consider raising UTSA preemption against functionally similar tort claims filed by the employer in order to bring the claim within the DTSA's statutory ambit. The UTSA preemption can block tort claims even when the plaintiff did not assert a trade secret misappropriation claim. *See* NetApp, Inc. v. Nimble Storage, Inc., 41 F. Supp. 3d 816, 839–40 (N.D. Cal. 2014) (rejecting plaintiff's argument that tort claims were not preempted because plaintiff did not allege an UTSA cause of action and observing that "such a rule would defeat preemption by allowing plaintiffs to intentionally omit CUTSA claims in favor of other claims").

138. For an exploration of U.S. laws regarding trade secrets and whistleblowing compared to some foreign jurisdictions, see Sharon K. Sandeen & Ulla-Maija Mylly, *Trade Secrets and the Right to Information: A Comparative Analysis of E.U. and U.S. Approaches to Freedom of Expression and Whistleblowing*, N.C. J.L. & TECH., Mar. 2020, at 1.

139. *See* Varadarajan, *supra* note 11, at 4.

140. *See* GOVERNMENT BY CONTRACT: OUTSOURCING AND AMERICAN DEMOCRACY (Jody Freeman & Martha Minow eds., 2009).

141. Gillian E. Metzger, *Privatization as Delegation*, 103 COLUM. L. REV. 1367, 1369 (2003); *see* Alfred C. Aman, Jr., *Globalization, Democracy, and the Need for a New Administrative Law*, 49 UCLA L. REV. 1687, 1700–03 (2002) (discussing democracy issues raised by privatization of prisons and social services for the poor); Matthew Diller, *Going Private—The Future of Social Welfare Policy?*, 35 CLEARINGHOUSE REV. 491, 491 (2001) (discussing "broad movement to 'privatize' government [poverty] programs"); Mathew Diller, *Introduction: Redefining the Public Sector: Accountability and Democracy in the Era of Privatization*, 28 FORDHAM URB. L.J. 1307, 1308 (2001) (describing privatization of government services, including "contracting out the delivery of services, divestiture of government owned resources and institutions, [and] the establishment of private communities with

party to accomplish a substantial government function, the government often uses trade secrecy as a shield to protect itself from investigative inquiry, raising public policy concerns "beyond competition or innovation."[142]

We discuss below the rise of trade secrecy claims in a variety of areas of delegation to private parties, some involving procurement and infrastructure, and others involving public functions—for example, software used in criminal prosecutions and automated decisionmaking. These cases fall into two basic categories. In the first kind of case, a third party, usually a private corporation, claims trade secret protection for its contractual work on behalf of the government, either in a criminal or civil context. In the second category, the government claims trade secret protection for its own activities. Both kinds of cases implicate public functions, impeding transparency through overbroad claims of trade secrecy.

As David Levine—one of the first to problematize such overreach—has explained: "Private businesses are continually displacing government in providing and operating public infrastructure, but utilizing commercial law standards and norms to do so, including the key tool of trade secrecy."[143] As a result, trade secrecy suppresses the public's right to transparency and full information.[144] To start, consider an example. In 2005, a voting machine company, Diebold Election Systems, refused to follow a North Carolina law that required electronic voting machine manufacturers to place their source code in escrow with a state board of elections approved agent.[145] The law was designed to ensure fair elections by providing for limited government oversight over the tabulation process.[146] However, Diebold chose to withdraw from servicing the state's elections altogether rather than reveal its source code.[147]

As this example shows, governance of our fundamental freedoms—the right to vote—has been outsourced to private companies, stripping the public (let alone the state) of the possibility of investigation or oversight, even with a protective order in place. Levine has used the useful metaphors of "confidentiality creep" and "opportunistic privacy" to describe the ongoing pattern of using privacy or confidentiality designations to seclude information supplied by private industry for use in government functions from the public, particularly regarding emerging technologies.[148] This story can be told in relation to many other basic government

quasigovernmental powers"); Mark H. Moore, *Introduction*, 116 HARV. L. REV. 1212, 1212 (2003) (introducing a symposium "focus[ed] on the increased 'privatization' of the public sphere").

142. *See* Varadarajan, *supra* note 11, at 4.

143. David S. Levine, *The Impact of Trade Secrecy on Public Transparency*, *in* THE LAW AND THEORY OF TRADE SECRECY, *supra* note 11, at 407.

144. *Id*. at 440.

145. *Id*. at 419.

146. *See id*. at 419–20. For an excellent article exploring the use of software-independent voting systems, compliance audits, and risk-limiting audits in elections, see Philip B. Stark & David Wagner, *Evidence-Based Elections*, 10 IEEE SEC. & PRIVACY 33 (2012).

147. *See* Levine, *supra* note 143, at 420.

148. David S. Levine, *Confidentiality Creep and Opportunistic Privacy*, 20 TUL. J. TECH. & INTELL. PROP. 11, 13, 15 (2017) (describing how secrecy can "creat[e] an empty space in which the information most needed to understand technological activity is held only by those with a vested interest in the

functions, which are becoming rapidly privatized and automated, relying on closed proprietary systems in areas of public benefits, electronic voting, and agency-gathered data, among others.[149]

1. Criminal Justice and the Secret Algorithm

In many facets of the criminal justice system, trade secrecy has presented both systemic and individualized sets of concerns, raising troubling constitutional questions regarding due process. Although the intermingling of private engagement with public functions is not entirely new, what is unprecedented is the degree to which trade secrecy, more recently, has impeded public oversight. This produces a delegation of a government function—law enforcement and prosecution—to a private entity, where trade secrecy grants even further immunity to the prosecution within the criminal justice system. Because fact-finding and investigation become insulated from adversarial scrutiny through trade secrecy, this delegation raises classic concerns about the reach of the Confrontation Clause of the Sixth Amendment in such contexts, as well.

Even before a case makes its way to a court, law enforcement tactics have relied on increasingly creative and troubling modes of surveillance, reporting, and prediction, much of which is shrouded in secrecy generally, and trade secrecy specifically. Today, Automated Suspicion Algorithms (ASAs) apply machine learning to data with the purpose of identifying individuals who may be engaged in criminal activity, conflicting with the requirement of individualized suspicion under the Fourth Amendment.[150] Aside from these constitutional concerns, trade secrecy makes it difficult to even discover, let alone investigate these technologies and their implications. For example, as Elizabeth Joh has discussed, some companies require police to sign nondisclosure agreements about new surveillance technologies like "stingrays" (cellphone surveillance tools), promising not to disclose that the technologies exist to the defendants, courts, legislators, and the public.[151]

Systemically, we can see numerous examples of how data secrecy in the criminal justice context represents a crucial obstacle to transparency and accountability. Over ninety jurisdictions use a service called ShotSpotter, which collects data on gunfire from sensors installed in particular neighborhoods.[152] ShotSpotter has taken the position that even the *data* that it generates regarding the location of these shots is a protected trade secret; in one instance, discussed by Hannah

technology's rapid dominance"). These concerns are deeply linked to Frank Pasquale's book, *The Black Box Society*, which extensively details how trade secrecy in search engines, healthcare, and credit scoring has dramatically impacted communities, often without any public transparency or accountability. *See generally* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2016).

149. *See* Danielle Keats Citron, *Open Code Governance*, 2008 U. CHI. LEGAL F. 355, 356–57.

150. *See* Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871, 886, 890–93 (2016) (discussing ASAs and individualized suspicion).

151. *See* Wexler, *supra* note 8, at 1366–67 (discussing Joh's pathbreaking work).

152. *See* Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265, 1283–84 (2020).

Bloch-Wehba, the company CEO maintained that its collected data does not comprise "crime data" and requested various municipalities nationwide not to release the data to investigators and journalists.[153] As a result, some municipalities agreed that the data was not a matter of public record and refused to release it to the public unless the individuals licensed the data from the company directly.[154]

These concerns are not limited to surveillance and predictive policing technologies; they extend to nearly every stage in the life cycle of a criminal justice case, including bail investigations, pretrial and trial evidence, sentencing, and parole. Today, algorithms, and the trade secrecy that envelops them, surface throughout many types of forensic technologies, including fingerprint analysis, ballistic analysis, firearm and cartridge matching analysis, facial recognition technologies, DNA analysis, and other AI-related tools.[155] In addition, algorithms that are used to sentence defendants or parole prisoners have raised significant issues of racial bias.[156] A ProPublica report studied Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), one of the most popular algorithms that is used to assess a defendant's risk of recidivism and subsequently sentence that defendant based on this risk.[157] When ProPublica tested the results from the proprietary algorithm used to predict recidivism, it discovered that the scores were wrong almost forty percent of the time, and seriously "biased against black defendants, who were falsely labeled future criminals at almost twice the rate of

153. *See id*. at 1284.

154. *See id*. Somewhat similarly, the Arnold Foundation offers public sector entities a "Public Safety Assessment" tool free of charge, but then requires participants to sign a memorandum of understanding that requires entities to agree not to classify its tool as a public record for FOIA purposes. *See id*. at 1286. Interestingly, as Bloch-Wehba has observed, the Arnold Foundation does not claim a property interest in the data provided by participating organizations, unlike ShotSpotter, but its assertion that the tool not be a matter of public record raises secrecy concerns. *See id*.

155. *See* Wexler, *supra* note 8, at 1363–64; *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-20-479SP, FORENSIC TECHNOLOGY: ALGORITHMS USED IN FEDERAL LAW ENFORCEMENT 3–4 (2020), https://www.gao.gov/assets/710/706849.pdf [https://perma.cc/RZ2Q-ZVML] (explaining how algorithms are used by law enforcement to assist with forensic analysis, including algorithms devoted to facial recognition, latent print examination, and DNA analysis).

156. *See* Erin Murphy, *Databases, Doctrine & Constitutional Criminal Procedure*, 37 FORDHAM URB. L.J. 803, 821–36 (2010). Sonja Starr's excellent work has demonstrated how evidence-based sentencing (EBS) has raised substantial constitutional concerns. *See* Sonja B. Starr, *Evidence-Based Sentencing and the Scientific Rationalization of Discrimination*, 66 STAN. L. REV. 803 (2014). For a related discussion of these issues, see Katyal, *supra* note 127, at 84–88.

157. *See* 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/649S-S3R3]. Although Northpointe refuses to disclose how it analyzes its data, it has revealed that the COMPAS analysis considers a subject's basic demographic information, criminal record, and family history, along with over 130 other questions. *Id*.; *see Algorithms in the Criminal Justice System: Risk Assessment Tools*, ELECTRONIC PRIVACY INFO. CTR. (Nov. 11, 2017) https://epic.org/algorithmic-transparency/crim-justice [https://perma.cc/UUG7-HDT2] (last visited May 10, 2021). Starr has pointed out that Northpointe has devised a separate set of question for women; she further discusses the constitutional implications of this differential usage by the state. *See* Starr, *supra* note 156, at 823–29, 823 n.76. Although these questions do not necessarily in themselves reveal a bias—because Northpointe refuses to reveal how the algorithm weighs these answers—the only way to assess the algorithm's bias is through its results, which have demonstrated racial disparities.

white defendants."[158] Trade secrecy assertions can hobble oversight of these technologies, with significant implications for the rights of defendants.

Despite the problems that ProPublica documented, the Wisconsin Supreme Court, in *State v. Loomis*, upheld the use of COMPAS in sentencing in July 2016, although it recognized the potential for overreliance on such tools.[159] In that case, in 2013, Eric Loomis was charged with crimes related to a drive-by shooting.[160] He was sentenced to eleven years in prison; the court considered the COMPAS risk assessment report that labeled Loomis a high risk for pretrial recidivism risk, general recidivism risk, and violent recidivism risk.[161] Loomis appealed the sentence on due process grounds.[162] The court rejected his concerns, noting that "to the extent that Loomis's risk assessment is based upon his answers to questions and publicly available data about his criminal history," the court found that he could verify the accuracy of his answers.[163]

Tellingly, however, the Wisconsin court did not discuss trade secrecy at all, even though Loomis was unable to determine how COMPAS arrived at its conclusion, because the company refused to reveal its proprietary algorithm. *Loomis* is just one example of how trade secrecy has created insurmountable obstacles for defendants caught in the criminal justice system. In an excellent article, Rebecca Wexler examines the substantial deference that courts have extended to trade secret owners in many of these areas, even though their processes, and the decisions that they reach, often implicate the difference between liberty and imprisonment.[164] Wexler has observed that in such cases, law enforcement agencies and software developers "will try to use intellectual property law as a shield against judicial scrutiny, preventing the courts from determining the constitutionality and lawfulness of new investigative technologies."[165]

---

158. Julia Angwin, *Make Algorithms Accountable*, N.Y. TIMES (Aug. 1, 2016), http://www.nytimes.com/2016/08/01/opinion/make-algorithms-accountable.html (arguing for greater transparency and accountability); *see* Angwin et al., *supra* note 157. ProPublica found that roughly "60 percent of those classified as higher risk went on to commit new crimes, a rate that was the same for both black and white defendants." Julia Angwin & Jeff Larson, *ProPublica Responds to Company's Critique of Machine Bias Story*, PROPUBLICA (July 29, 2016, 11:56 AM), http://www.propublica.org/article/propublica-responds-to-companys-critique-of-machine-bias-story [https://perma.cc/GV9P-Z6CP]. Yet when it looked at the forty percent of predictions that were incorrect, it found that "[b]lack defendants were twice as likely to be rated as higher risk but not re-offend. And white defendants were twice as likely to be charged with new crimes after being classed as lower risk." *Id.*

159. *See* State v. Loomis, 2016 WI 68, ¶ 120, 371 Wis. 2d 235, 881 N.W.2d 749.

160. *See id.* ¶ 11.

161. *Id.* ¶¶ 14, 16.

162. *See id.* ¶¶ 28–29; *see also* Mitch Smith, *In Wisconsin, a Backlash Against Using Data to Foretell Defendants' Futures*, N.Y. TIMES (June 22, 2016), https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html. Loomis argued the sentencing decision violated his right to due process because: (1) Northpointe would not reveal the source code so its validity could not be tested, (2) the judge relied on COMPAS's generalized risk based on defendants like Loomis, rather than considering him as an individual, and (3) the tool improperly considered gender in determining risk. *See Loomis*, 2016 WI 68, ¶ 34.

163. *Id.* ¶ 55.

164. *See* Wexler, *supra* note 8, at 1358–64.

165. *Id.* at 1365.

Consider the lines between privatization and public responsibilities in these contexts. We consider these issues, not just matters of evidentiary incompleteness or error (though they certainly are), but rather, as a troubling link between trade secret overbreadth and private delegation. Here, the government essentially delegates its responsibilities—factfinding, investigation, pretrial, trial, and sentencing administration—to a software program. Moreover, the private status of the manufacturer facilitates the striking dismissal of core constitutional protections regarding the right to confront witnesses at trial. And judges further aid this process by insulating the state's evidence, and related information, within an impermeable layer of trade secrecy.

Assertions of trade secret privilege in most states are covered by sections of the evidence code, which provides for protection from disclosure to the public as long as it will not "conceal fraud or otherwise work injustice."[166] Yet as Wexler has documented, the extension of trade secret privilege to these investigative technologies can cause significant injustice, foreclosing an examination of the many sources of potential error that emerge from an overreliance on computer programs in such contexts.[167]

These issues curtail the adversarial scrutiny that underlies our criminal justice system. Ironically, in many such cases, both state and federal courts often presume the reliability and accuracy of the techniques they rely upon.[168] And yet, computer scientists would argue exactly the reverse: that the programs themselves do not automatically or inherently ensure reliability.[169] As Christian Chessman writes, "computer programs are not more reliable than human statements because they *are* human statements—and no more than human statements."[170] Because they are tools of human design, they are often subject to human error, faulty assumptions, and mistakes, just like any other kind of evidentiary tool.[171] This is perhaps the strongest reason for why machine testimony deserves the benefit of adversarial scrutiny.[172] These errors are structural in nature, and they produce structural errors, as a result, because they stem from the nature of computer programming itself—ranging from accidental errors

166. *See, e.g.*, CAL. EVID. CODE § 1060 (West 2020). Courts have also interpreted this provision to include a requirement that the defense in a criminal case must also show that the trade secret is relevant and necessary to the defense in order to obtain disclosure under a protective order. *See* People v. Superior Court (Chubbs), No. B258569, 2015 WL 139069, at *6 (Cal. Ct. App. Jan. 9, 2015).

167. *See* Christian Chessman, Note, *A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 CALIF. L. REV. 179, 209–13 (2017) (analyzing problems with use of software in criminal prosecutions where the underlying code is unavailable for review, including when the trade secret privilege is asserted).

168. *See id.* at 184.

169. *See id.*

170. *See id.* at 186.

171. *See id.* at 184.

172. *See* Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 1989–2000 (2017) (describing results of comprehensive study of use of automated or machine-driven evidence in litigation and risks of human error in design, and proposing solutions based on decoupling such evidence from the hearsay rule).

(including technical coding errors) to outdated code, software rot, intentional and unintentional forms of bias baked into the code, failures of self-testing, and other processing issues.[173]

These arguments—about the fallibility of software processes and issues concerning data collection—are ones that have been heavily documented. Yet even though companies argue that their methods are so widely known that they are broadly accepted by the scientific community, they will go to enormous lengths to keep their source code confidential.[174] As a result, courts deny defendants access to the source code from software tools used to convict them, either on the grounds of trade secrecy or because the source code is held elsewhere by the contracting party—and is also a trade secret.[175] One of the earliest cases, *People v. Chubbs*, denied a death penalty eligible defendant the right to examine the source code used in a forensic software program, concluding that the code was a protected trade secret.[176] In that case, Cybergenetics, a software developer, maintained that it kept the source code secret for TrueAllele because of the "highly competitive commercial environment," and it provided defense experts with its methodology and underlying mathematical model, arguing that its source code was unnecessary to assess the program's reliability.[177] The court agreed, rejecting the prospect of a Sixth Amendment violation, holding that the Confrontation Clause did not require pretrial discovery of privileged information.[178]

This outcome is hardly an anomaly.[179] *Chubbs*, Wexler points out, led to a number of other courts following suit, cementing a shield for trade secrets in criminal proceedings.[180] In one case cited by Wexler, a Washington court

173. *See* Chessman, *supra* note 167, at 186–96.

174. *See* Katyal, *supra* note 40, at 1242–43, 1243 n.360 (citing Katherine L. Moss, Note, *The Admissibility of TrueAllele: A Computerized DNA Interpretation System*, 72 WASH. & LEE L. REV. 1033, 1071–72 (2015)); *see also* Stephanie L. DamonMoore, *Trial Judges and the Forensic Science Problem*, 92 N.Y.U. L. REV. 1532, 1536 (2017) (discussing "constraints on judges' abilities to recognize and address problems with forensic science"); William C. Thompson & Simon Ford, *DNA Typing: Acceptance and Weight of the New Genetic Identification Tests*, 75 VA. L. REV. 45, 59–60 (1989) (noting that asserting trade secrecy shields companies from scrutiny by the scientific community).

175. *See* Chessman, *supra* note 167, at 205 & n.194 (citing Moe v. State, 944 So. 2d 1096, 1097 (Fla. Dist. Ct. App. 2006)).

176. *See* People v. Superior Court (Chubbs), No. B258569, 2015 WL 139069, at *5–6 (Cal. Ct. App. Jan. 9, 2015).

177. *Id*. at *7.

178. *See id*. at *10.

179. Several other courts have reached similar conclusions on TrueAllele. *See* Commonwealth v. Foley, 38 A.3d 882 (Pa. Super. Ct. 2012); State v. Shaw, No. CR-13-575691, slip op. at 25–26 (Ohio Ct. Com. Pl. Oct. 10, 2014) (denying defendant's motion where court had "previously established that the TrueAllele methodology and the State's witness [were] reliable without the use of the source code"); *see also* Moss, *supra* note 174, at 1061–70 (collecting cases). Yet, according to experts, TrueAllele's match statistic values dramatically diverge from the findings of other competitors. *See* Brief of the Innocence Project, Inc. et al. as Amici Curiae Supporting Respondents at 13, People v. Johnson, No. F071640 (Cal. Ct. App. July 11, 2019); *see also* Chessman, *supra* note 167, at 198 (discussing how widely a random match probability (RMP) calculated by TrueAllele diverged from an RMP calculated by a conventional DNA lab using the same data).

180. *See* Wexler, *supra* note 8, at 1362 & n.80.

concluded that the defense had failed to show that access to the source code was materially necessary, concluding that "the usefulness of disclosing the source code [was] outweighed by a substantial risk of financial harm" to the software owner.[181] Several other cases have followed this reasoning, concluding that source code is proprietary and therefore essentially immune from investigation by the defendant.[182]

Denying source code availability makes it literally impossible for the defendant to present a full and complete defense; "[i]t's akin to asking a mechanic to certify a car as in good working condition without allowing them to look under the hood."[183] In *People v. Carter*, the court found that the there was no need to turn over the source code for the DNA matching software, Forensic Statistical Tool (FST), which was developed by New York City, in part because it was proprietary, and because it was never in the possession of the District Attorney.[184] Even though an expert had showed that the use of FST was potentially flawed, causing uncertainty as to thousands of cases relying on the tool, it remained subject to a protective order until ProPublica filed a motion to intervene and vacate the order.[185]

---

181. *Id.* at 1361 & n.73 (quoting State v. Fair, No. 10-1-09274-5-SEA, slip. op. at 9 (Wash. Super. Ct. Jan. 12, 2017)).

182. *See, e.g.*, People v. Lopez, 23 N.Y.S.3d 820, 829 (N.Y. Sup. Ct. 2015) (refusing to turn over actual program software to the defendant because it is proprietary). In a recent New Jersey case, the prosecution purported to allow access to TrueAllele source code by a defense expert witness—thus on the surface offering something common in civil trade secret litigation—but the defense argued that cumbersome conditions imposed on the expert and the absence of "software dependencies" and development materials. *See* Letter Brief in Support of Defendant-Appellant's Motion for Leave to Appeal at 3–4, State v. Pickett, 246 A.3d 279 (N.J. Sup. Ct. App. Div. 2021); *see also* Amended Letter-Brief and Appendix on Behalf of the State of New Jersey at 12, State v. Pickett, 246 A.3d 279 (N.J. Super. Ct. App. Div. 2021) (collecting nationwide cases denying source code review for TrueAllele and arguing against appeal from the trial court's ruling against the defendant).

183. *See* Amicus Curiae Brief of Electronic Frontier Foundation in Support of Defendant and Appellant Billy Ray Johnson at 17, People v. Johnson, No. F071640 (Cal. Ct. App. July 11, 2019). On appeal, even though the court recognized that the software had the potential to produce "arguably inconsistent results," it upheld the conviction because the evidence overwhelmingly confirmed the appellant's guilt. *See Johnson*, No. F071640, 2019 WL 3025299, at *10.

184. *See* No. 2573/14, 2016 WL 239708, at *7 (N.Y. Sup. Ct. Jan. 12, 2016). The Office of the Chief Medical Examiner had developed its own probabilistic genotyping tool, the FST, and then refused to turn over the source code to experts until a protective order was issued. *See* Bloch-Wehba, *supra* note 152, at 1287–88. When FST was disclosed for analysis in another case, the source code, according to the Electronic Frontier Foundation, revealed that a previously undisclosed portion "incorrectly tipped the scales in favor of the prosecution's hypothesis that a defendant's DNA was present in a mixture," and differed from the actual code used in the lab. *See* Amicus Curiae Brief of Electronic Frontier Foundation in Support of Defendant and Appellant Billy Ray Johnson, *supra* note 183, at 12–13. Eventually, the city relented on its claims that the code was proprietary, and turned it over to ProPublica, who then published the code to the public. *See* Bloch-Wehba, *supra* note 152, at 1288. Notably, in September 2016, New York City decided to retire FST, a previous in-house tool, in favor of STRmix, which has made its source code publicly available. *See* Brief of the Innocence Project, Inc. et al., *supra* note 179, at 19 (citing ACCESS TO STRMIX™ SOFTWARE BY DEFENCE LEGAL TEAMS, ESR (Apr. 28, 2016, 9:00 AM), https://www.strmix.com/assets/STRmix/STRmix-PDFs/Defence-Access-to-STRmix-April-2016.pdf [https://perma.cc/LPR8-EW32]).

185. *See* Bloch-Wehba, *supra* note 152, at 1288.

As a general matter, consider how the circularity of the argument for trade secrecy contributes to the problem. Here, courts that deny access to source code are essentially siding on the side of trade secrecy's circularity, refusing to give a defendant the ability to challenge whether the source code constitutes a trade secret—let alone challenge the validity of its findings.[186] Essentially, these findings improperly "credit[] the evidence without subjecting it to scrutiny," thus hampering an effective defense.[187] As Chessman argues, however, it is impossible to tell whether the source code is a trade secret without some kind of disclosure, and private, pecuniary interests have never been recognized as "state interests" in the criminal prosecution process.[188] Indeed, in some cases, after an investigation, courts have concluded the information might not even satisfy the definition of a protected trade secret at all.[189]

Finally, in some cases states will argue that they lack possession of the source code and therefore cannot turn it over for investigation.[190] By not taking the source code, the state is practically able to immunize itself from investigation regarding its forensic techniques, weaponizing trade secrecy to accomplish its goal of seclusion. In one example, a defendant was unable to acquire the source code to challenge his breathalcohol score because the source code was held by the manufacturer and considered to be a trade secret.[191] For this reason, the court refused to require it to be turned over because it was essentially out of the boundaries of the discovery order.[192] In another case, law enforcement *deliberately* avoided taking possession of the source code in order to assist prosecutors and avoid turning the code over to defense counsel and its expert.[193] Throughout these examples, we see how claims of trade secrecy impede access and oversight, with troubling implications for the criminal justice system.

2. Private Contracts, Public Infrastructure, and Due Process

The same issue identified above—problematic assertions of trade secrecy in aspects of government—extends to the civil context as well, particularly in the area of public benefits. Government has become increasingly intermingled with private industry through delegation throughout infrastructure involving

186. *See* Chessman, *supra* note 167, at 211. Similar refusals to compel source code have occurred in the context of the Intoxilyzer, which is used to measure alcohol intoxication. *See* Natalie Ram, *Innovating Criminal Justice*, 112 NW. U. L. REV. 659, 662 (2018). In a similar context involving Alcotest, a popular breath test device, the company refused to sell its device to nonlaw enforcement entities to enable independent verification on trade secrecy grounds. *See id.* at 672 (citing State v. Chun, 943 A.2d 114 (N.J. 2008)).

187. Chessman, *supra* note 167, at 211.

188. *See id.* at 209–10.

189. In one case, the New Jersey Supreme Court found that the source code for the Alcotest 7110 was not a trade secret because it was composed of general algorithms and did not satisfy the required showing. *See id.* at 210 (discussing *Chun*, 943 A.2d 114).

190. *See id.* at 213–14.

191. *See* State v. Kuhl, 741 N.W.2d 701, 705, 708–09 (Neb. Ct. App. 2007), *aff'd*, 755 N.W.2d 389 (2008).

192. *See id.* at 708–09.

193. *See* Moe v. State, 944 So. 2d 1096, 1097 (Fla. Dist. Ct. App. 2006)

telecommunications, government operations, energy, Medicare, Medicaid, welfare programs, public education, and prisons.[194] Particularly where such government decisionmaking relies on software, the result risks overextending trade secrecy into government functions, insulating them from inquiry. Showing just how widespread trade secret and confidentiality-based objections to public disclosure in government infrastructure have become, a recent empirical study detailed the results of forty-two open-records requests in twenty-three states that cited concerns over trade secrecy as a barrier to access municipal information.[195] As Robert Brauneis and Ellen Goodman eloquently noted in that study, "[t]he risk is that the opacity of the algorithm enables corporate capture of public power."[196]

These observations are important because they underscore a similar core issue associated with the comingling of private entities with public government functions throughout infrastructure: due process of law. Automated decisionmaking essentially delegates government functions to third party, private entities who can rely, even more after *Argus Leader*, on trade secrecy to obscure their inner workings. As one of us has argued previously, this commingling of artificial intelligence and government function creates a "crisis of transparency," where "private businesses now play the roles that government used to play but can utilize the principles of trade secret law to insulate themselves from the very expectations of accountability under which that government operated."[197]

Today, as several scholars have observed, machine learning algorithms have been deployed in deciding who the Internal Revenue Service should audit, managing and setting social security and other public benefits, interpreting DNA evidence, assessing teacher performance, and a host of other areas.[198] The idea of delegation in the administrative state has been thoroughly explored by Danielle Citron in an early article, *Technological Due Process*, which described automated decisionmaking as "de facto delegations of rulemaking power."[199] In a later work, Citron and Ryan Calo explain that administrative agencies have come to

194. *See* Levine, *supra* note 7, at 141–42.

195. *See* Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103, 103–04 (2018) (describing concerns about use of artificial intelligence algorithms by state actors in conduct such as hiring and firing, parole decisions, and creditworthiness decisions, and reporting results of an empirical effort involving "forty-two open records requests in twenty-three states" where assertions of trade secrecy were a barrier to access).

196. *Id*. at 109; *see* Will Knight, *The Dark Secret at the Heart of AI*, 120 MIT TECH. REV. 55, 55 (2017) ("No one really knows how the most advanced algorithms do what they do.").

197. Katyal, *supra* note 40, at 1237–38.

198. *See* Bloch-Wehba, *supra* note 152.

199. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1294 (2008); *see* DANIEL FREEMAN ENGSTROM, DANIEL E. HO, CATHERINE M. SHARKEY & MARIANO-FLORENTINO CUÉLLAR, GOVERNMENT BY ALGORITHM: ARTIFICIAL INTELLIGENCE IN FEDERAL ADMINISTRATIVE AGENCIES 6 (2020); Ryan Calo & Danielle Keats Citron, *The Automated Administrative State: A Crisis of Legitimacy*, 70 EMORY L.J. 797, 816–17 (2021) (observing that almost half of all federal agencies are exploring artificial intelligence methods in their work); Cary Coglianese & David Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, 105 GEO. L.J. 1147, 1154 (2017).

rely on increasingly automated decisionmaking as a way of navigating an increasingly complex work.[200]

The rise of automated decisionmaking has significant costs regarding due process. It "impair[s] individualized process, making decisions about individuals without notice and a chance to be heard, and embedding rules that lack democratic imprimatur."[201] Delegations to private industry are especially troubling, several scholars have argued, because they circumvent the general practices of notice-and-comment rulemaking and other forms to ensure deliberative participation.[202] Less clear, but equally important, is the way in which trade secrecy concretizes the absence of due process—not only foreclosing transparency but also accountability and explainability. In these situations, trade secrecy—and the deference afforded to trade secrets' owners—creates a double bind of deference, where the deference enjoyed by the trade secret owner can be readily mapped and extended to the results of these instruments of automated decisionmaking as well.

Although a comprehensive study of the ways in which trade secrecy operates in these contexts has been hard to uncover—again, in no small part due to trade secrecy—several recent cases have offered a glimpse of the instrumental role it has played in concealing complicated automated decisions. In one case, the Arkansas Department of Human Services (DHS) decided to replace its system of individualized nurse-led evaluations for home care services to a nonprofit that licenses its "Resource Utilization Group system" to various state agencies; the system is a machine learning algorithm that uses classifications and statistical calculations to arrive at a result.[203] The new system, while promising efficiency, also "produced arbitrary and illogical results," according to Calo and Citron.[204] For example, the algorithm would indicate that a person had "no foot problem" if the person was a foot amputee, even though they would need more assistance rather than less, and underestimated the cost of multiple conditions.[205]

After a number of physically disabled Arkansas residents discovered that their home care had been reduced by forty-three percent under adoption of the new system, they sued in court, leading to an injunction that prevented DHS from using an automated system until it was able to explain its reasoning and eventually culminating in a ruling that observed that the state had "failed to follow [its

200. *See* Calo & Citron, *supra* note 199, at 801.

201. *Id.* at 819.

202. *See, e.g.*, Deirdre Mulligan & Kenneth Bamberger, *Procurement as Policy: Administrative Process for Machine Learning*, 34 BERKELEY TECH. L.J. 773, 781 (2019) (discussed in Calo and Citron, *supra* note 199, at 817).

203. *See* Calo & Citron, *supra* note 199, at 820–21 (discussing Ark. Dep't of Human Servs. v. Ledgerwood, 530 S.W.3d 336, 340 (Ark. 2017) (affirming finding that state had not provided adequate notice of changes to program, where "Appellees claimed that they (1) had been forced to go without food, (2) remained in soiled clothes or have gone without bathing, (3) missed key exercises, treatments, or turnings, (4) faced an increased risk of falling, (5) have become more isolated in their homes; (6) have suffered worsened medical conditions directly due to a lack of care; and (7) have considered moving to nursing homes")).

204. *Id.* at 821.

205. *Id.*

own] rulemaking procedures" by failing to provide adequate notice to affected parties of the switch to the new methodology.[206]

We can see, in the Arkansas case, how a lack of notice and comment can contribute to arbitrary results. In such cases, however, there is an additional complication stemming from trade secrecy, which can preclude investigation altogether. For example, in a similar case from Idaho, when employment of AI-related tools cut individuals' home care hours, the American Civil Liberties Union (ACLU) was not able to discern the reason for the final result due to trade secrecy.[207] In that case, an Idaho court agreed to disclose the methodology to the plaintiffs, but only on the condition that the trade secret remain protected and that the "details of the budget-setting methodology . . . may not be discussed or revealed to anyone, in any manner, except for purposes of administrative appeal and judicial review."[208]

Bloch-Webha has referred to the compromise solution of a protective order as "atomized disclosure" and criticized it for its First Amendment and due process implications, in addition to its inefficiency.[209] As Bloch-Wehba has argued, in these and other areas, these methods of algorithmic decisionmaking demonstrate a core conflict between these methods (and the vendors who supply them), private individuals who may wish to challenge these decisions, and the general public interest.[210] Because these determinations involved closed code, with little explanation for their outcomes, they represent a fundamental challenge to due process and transparency.[211]

The effects of trade secrecy on privatized, automated decisionmaking can literally mean the difference between life and death. In another case, a twenty-seven year old woman with cerebral palsy and severe developmental disabilities in West Virginia had her Medicaid funds slashed from $130,000 to $72,000 when the third party, which administered the program on behalf of the state, began using a confidential algorithm that it did not make publicly available, thus making it impossible for her to stay in her family home.[212] When she challenged the determination in federal court, the court observed that the algorithm had failed to satisfy due process requirements, given that the vendor had failed to employ

206. *See id*. at 26–27.

207. *See id.* at 823 (citing Jay Stanley, *Pitfalls of Artificial Intelligence Decisionmaking Highlighted in Idaho ACLU Case*, ACLU (June 2, 2017, 1:30 PM) https://www.aclu.org/blog/privacy-technology/pitfalls-artificial-intelligence-decisionmaking-highlighted-idaho-aclu-case [https://perma.cc/3JF6-XCA4]).

208. *See* Bloch-Wehba, *supra* note 152, at 1279 (quoting Declaration of Katherine Takasugi at 7, K.W. *ex rel*. D.W. v. Armstrong, No. 1:12-CV-22-BLW (D. Idaho Aug. 2, 2012), ECF No. 25-1).

209. *Id*.

210. *See id*. at 1274.

211. *See id*.

212. *See id*. at 1277–78 (citing Michael T. v. Bowling, No. 2:15-CV-09655, 2016 WL 4870284, at *2 (S.D. W. Va. Sept. 13, 2016) (granting in part plaintiffs' request for preliminary injunction to reinstate certain benefits and noting that "[t]he APS Algorithm is proprietary to [third party vendor] APS and, as such, the exact factors it considers, the weight it accords to each factor, and its overall methodology in determining each member's budget are not publicly available information")).

"ascertainable standards," and had provided "no information as to what factors are incorporated into the APS algorithm" nor an "individualized rationale" for its outcome.[213] The district court concluded that the lack of transparency created an "unacceptable risk of arbitrary and 'erroneous deprivation[s].'"[214]

Similar due process concerns have also surfaced in the context of public education, where proprietary algorithms have been used to assess teacher performance. In one case, a private company, SAS, developed a statistical model called the Educational Value-Added Assessment System (EVAAS) to assess teacher performance in the Houston Independent School District, resulting in the dismissal of twelve teachers.[215] Importantly, in that case, trade secrecy of the source code prevented *even the school district* from having access to the proprietary algorithm.[216] After the case was filed, in the context of discovery, the court entered a protective order but made the source code and related materials available to an expert who concluded that the teachers were unable to "meaningfully verify" their scores under the EVAAS system.[217]

Neither the teachers nor the district had access to the algorithms, and the plaintiffs' expert was unable to replicate the scores, even with some degree of access to the algorithm itself. On the district's motion for summary judgment, the court noted that not only were errors possible, but that an error with respect to one teacher's score would affect the scores of other teachers as well.[218] Ultimately, the court viewed itself as facing a conundrum: either it disclosed the third-party software maker's trade secrets, thereby destroying its value, or it deprived the teachers of their due process.[219] It ruled against the policy adopting use of the software instead, noting tellingly: "When a public agency adopts a policy of making high stakes employment decisions based on secret algorithms incompatible with minimum due process, the proper remedy is to overturn the policy, while leaving the trade secrets intact."[220]

213. *Id.* at 1278.

214. *Id.* In response, when the state developed a new system that replaced the proprietary algorithm with a process that disclosed "a number of clearly identified variables based on a combination of a member's living situation" and their answers to specific queries, also making it possible for members to challenge the accuracy of the inputs, as well as the entire system itself, the injunction was lifted. *Id.*

215. *See* Hous. Fed'n of Teachers v. Hous. Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1175 (S.D. Tex. 2017); *see also* Bloch-Webha, *supra* note 152, at 1281–82 (discussing the statistical model's role in assessing teacher performance).

216. *See* Bloch-Wehba, *supra* note 152, at 1282.

217. *See id.* Notably, when the teachers' union posted a case update on their website, SAS moved for contempt, arguing that the blog post violated the protective order because the protective order (in their view) was meant to "prevent Plaintiffs and all of Plaintiffs' experts from *continuing any public discourse against EVAAS*." *Id.* at 1282–83. Although the court rejected SAS's argument, noting that if it adopted SAS's "overly broad" determination, it would "inhibit legitimate discussion," this example gives a strong sense of the transparency and disclosure issues at stake. *See id.* at 1283.

218. *See id.* at 1283.

219. The court did not appear to consider access under a protective order, as is commonplace in other civil misappropriation cases.

220. *Hous. Fed'n of Teachers*, 251 F. Supp. 3d at 1179.

In the end, the court agreed with the due process concerns, noting that the generalized explanation was insufficient for an individual to meaningfully challenge the determination, and the case settled a few months later.[221] But at all times, just as the court noted, the trade secrecy remained unchallenged, placing a paramount value on property and seclusion, instead of government accountability.

3. Government Secrecy, Public Functions, and Disclosure

Finally, a third set of problems arise regarding transparency in contexts where the government can and has asserted its *own* trade secret protection as an exemption under the FOIA.[222] The phenomenon of government trade secrecy, initially described by David Levine as an "anomaly," is a growing concern due to the increased movement of government in commercial activities, such as servicing student loans and the like.[223]

The issue of government trade secrets implicates a fundamental question of whether a government can claim the same kind of protection enjoyed by private parties with respect to trade secrecy. Does the government owe a greater responsibility of disclosure to the public? Historically, some states had a longstanding policy that trade secret protection should automatically not attach to public entities when the function at issue is considered a governmental function, rather than one associated with a private entity.[224] Yet with the states' gradual adoption of the UTSA, which explicitly recognized that governmental entities could possess trade secrets, more and more states began to extend the boundaries of trade secrecy for government functions.[225]

This creates a foundational conflict between commercial interests in secrecy for competitive advantage and the tenets of transparency that we normally associate with government accountability. When government trade secrets are asserted, rather than being used as a sword in a misappropriation action, Levine argues that they "have always been used as a shield to public disclosure."[226]

Ironically, and perhaps not coincidentally, these issues have become especially concerning because many states have passed right-to-know laws and procurement policies that, coupled with FOIA, expand the responsibilities for public disclosure.[227] In such situations, the government is impersonating a contradiction in terms: it is functioning both as a private party and, to some extent, as a representative of the people's will. Scholars, too, have weighed in on this question. Richard Epstein has argued that governments should be permitted to classify information, just as any other private party, as long as the government-related information

221. *See id*. at 1182–83.

222. *See* Levine, *supra* note 42, at 67–68, 73, 78–81.

223. *See id*. at 67.

224. *See* State *ex rel*. Besser v. Ohio State Univ., 721 N.E.2d 1044, 1049 (Ohio 2000); Hoffman v. Pa. Game Comm'n, 455 A.2d 731, 733 (Pa. Commw. Ct. 1983).

225. *See Besser*, 721 N.E.2d at 1049 (relying on in camera proceedings to distill trade secrets from otherwise disclosable information).

226. Levine, *supra* note 42, at 68, 74.

227. *See* Vladeck, *supra* note 65, at 10773.

possesses the traditional requirements of trade secrecy.[228] Yet Richard Posner has argued, in a related vein, that the government claim to privacy is weaker than that of a business entity when "the government does not engage in entrepreneurial activity."[229]

While the issue of the extent to which a government can assert trade secrecy on its own behalf is complicated, deserving of a much lengthier discussion than this Article, one core value deserving of greater attention is the distinction between governance and commercial functions.[230] Extending this observation, we might distinguish between a variety of different circumstances in which the government seeks secrecy: (1) government itself engaging in traditional governance functions, but seeking conventional trade secret protections for its own activities; (2) government contracting with a private party for certain government functions (as discussed above), but seeking conventional trade secret protections for the company's actions; and (3) government engaging in entrepreneurial or innovative activity that actively competes with other private parties for commercial activities. The strength of the arguments for secrecy may vary depending on the circumstances, along with the arguments and expectations for due process and disclosure. The interest in disclosure also might vary depending upon who is most affected by the claim of secrecy.

In one set of cases, we see an even greater move toward trade secrecy where the government acts as a commercial provider, in a manner that is equivalent to a private party. In such situations, the government may owe an even stronger responsibility to provide access and information to the public due to its higher level of accountability. In the worst of situations, courts offer the same level of trade secret protection to a private party, and in the best of situations, a protective order is used to allow investigation.[231] Yet in all cases except one that we could find, the government is allowed to keep information from the wider public due to trade secret protection.

One of the most interesting and fruitful points for analysis lies in a core distinction, often made in the law, between a traditional government function and a private one. We might expect a greater degree of accountability to accompany the former function than the latter. Yet here, too, trade secret arguments have been

228. *See* Richard A. Epstein, *Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalism*, 52 STAN. L. REV. 1003, 1044 (2000). But Levine has persuasively argued that the traditional, utilitarian justifications for the creation of intellectual property rights are inapposite in the context of government trade secrecy, for as he writes, "There is no direct evidence that state governments are incentivized to serve the public by the availability of trade secrecy protection or that they license their trade secrets." *See* Levine, *supra* note 42, at 70–71, 74 (discussing Epstein's approach). As Levine notes when discussing changes in Ohio trade secret law, the Ohio version of the UTSA includes government bodies among those who can own trade secrets. *See* OHIO REV. CODE. ANN. § 1333.61(C) (West 2020) (defining "person" to include "governmental entities"); Levine, *supra* note 42, at 71 n.34, 73–74, 76 (citing similar UTSA language in California, North Carolina, and Utah).

229. *See* Richard A. Posner, *Privacy, Secrecy, and Reputation*, 28 BUFF. L. REV. 1, 51 (1979).

230. *See* Levine, *supra* note 42, at 77–84.

231. *See* State *ex rel*. Besser v. Ohio State Univ., 721 N.E.2d 1044, 1050 (Ohio 2000) (requiring in camera inspection to determine if trade secret information is exempt from disclosure).

victorious, enabling the government to obtain, at times, the same level of protection a private party enjoys (and in some cases, even more protection). In one case, a court applied trade secrecy to protect the confidentiality of testing questions administered to students, holding that they are not public records and therefore exempt from disclosure as trade secrets.[232]

In a second line of cases involving secrecy, a government might contract with a private company and then seek trade secret protection over its government functions. In one prominent case from the D.C. Circuit, where McDonnell Douglas Corporation sought an injunction restraining the Air Force from publicly releasing the pricing for a variety of services linked to satellite launches, the court remanded for a closer determination of trade secrecy, calling it "strange" to suggest that a price charged to the government for goods is a protected trade secret.[233]

Similar issues have emerged from the public benefits cases explored above, which again, demonstrate the inextricable link between due process and transparency in government contract cases with a private vendor. Although scholars have only been able to uncover a few cases in litigation, it is no understatement to suggest that these cases "may represent the tip of the iceberg."[234] As one lawyer for the ACLU explained, speaking about an Idaho case involving Medicare benefits:

> My hunch is that this kind of thing is happening a lot across the United States and across the world as people move to these computerized systems. Nobody understands them, they think that somebody else does—but in the end we trust them. Even the people in charge of these programs have this trust that these things are working.
>
> And the unfortunate part, as we learned in this case, is that it costs a lot of money to actually test these things and make sure they're working right. It cost us probably $50,000, and I don't think that a state Medicaid program is going to be motivated to spend the money that it takes to make sure these things are working right. Or even these private companies that are running credit predictions, housing predictions, recidivism predictions—unless the cost is internalized on them through litigation, and it's understood that "hey, eventually somebody's going to have the money to test this, so it better be working."[235]

As this lawyer suggests, these cases may only be resolved in favor of providing due process if people attempt to try to challenge the results of agency decisions. Without litigation challenging their decisions, as well, governments may not be incentivized toward investing in these systems. But because of trade secret

232. *See* State *ex rel.* Perrea v. Cincinnati Pub. Sch., 123 Ohio St. 3d 410, 2009-Ohio-4762, 916 N.E.2d 1049, at ¶¶ 11, 34.

233. *See* McDonnell Douglas Corp. v. Widnall, 57 F.3d 1162, 1167 (D.C. Cir. 1995). As with so many older FOIA cases, *Argus Leader* may well lead to contrary results today.

234. *See* Calo & Citron, *supra* note 199, at 834.

235. *See* Stanley, *supra* note 207 (quoting Richard Eppink, ACLU director of Idaho).

protections, they may never even know what algorithms—or vendors—to challenge and why.

Finally, in a third line of cases where the state is behaving as a private party, the government is able to own trade secrets just as any other party. In one case involving the question of whether lists of ticket buyers for a state school's athletic event counted as trade secrets, Connecticut's Freedom of Information Commission found that "public agencies are engaged in governance, not trade" and that the state school's principal function was "not trade, but rather education, a traditional governmental function."[236] The commission also found that because the university is publicly subsidized, these arguments weigh strongly in favor of disclosure.[237] As the commission argued, sensibly, government is held to a higher standard than a private party, given the public source of its funding.

Yet this argument did not survive on appeal, in no small part because the state open-records statute and the UTSA permitted government agencies to own a trade secret.[238] Instead, the state Supreme Court ruled in favor of parity between the government and a private party.[239] As a policy matter, the court then warned that the state would lose its ability to reap financial benefits for its activities "if any member of the public could obtain such information simply by filing a request under the act."[240] Because the legislature created a statutory scheme to enable the state university to own and control its intellectual property, the court reasoned that there seemed to be no reason to treat its management of the IP any differently than a private owner.[241]

At best, in these situations, courts have chosen to utilize an in camera review of the documents to balance the interest in disclosure with trade secret protection. In one case, *Parsons v. Pennsylvania Higher Education Assistance Authority*, a journalist attempted to obtain information about government travel to seminars and conferences, and performance and finance audits from the Pennsylvania Higher Education Assistance Agency (PHEAA).[242] PHEAA, a government organization, is in the student loan services industry, competing with private industry to purchase loans, service loans, and sell and lease computer services (among other responsibilities).[243] The court rejected the idea that the PHEAA could

236. Univ. of Conn. v. Freedom of Info. Comm'n, No. HHBCV094021320S, 2010 WL 2106972, at *4 (Conn. Super. Ct. Apr. 21, 2010), *aff'd*, 36 A.3d 663 (2012) (reasoning that, unlike a private business engaged in trade alone, a university's "cultural and athletic activities . . . are incidental to its primary governmental function of education.").

237. *See id.* at *2 (citing Pelto v. Connecticut, No. FIC 2008-341, ¶¶ 39–41, 47 (Conn. Freedom of Info. Comm'n May 13, 2009)).

238. *See* Univ. of Conn. v. Freedom of Info. Comm'n, 36 A.3d 663, 664, 668–69 (Conn. 2012).

239. *See id.* at 668. In the absence of any ownership limitations, the court ruled: "If the information meets the statutory criteria, it is a trade secret and the entity creating that information would be engaged in a trade for purposes of the act even if it was not so engaged for all purposes." *Id.*

240. *Id.* at 669.

241. *See id.*

242. 910 A.2d 177, 181 (Pa. Commw. Ct. 2006).

243. The PHEAA denied these requests on the grounds of trade secrecy, asserting that disclosure of such information would harm its competitive advantage, enabling competitors to see PHEAA's

conduct itself as a private entity with respect to trade secret protection, offering an in camera review of any proposed redactions in order to balance the public's interest in disclosure.[244]

Notably, in many such cases, courts rarely examine the substantive basis for the trade secret. But when they do, at times, they have concluded against protection. For example, a court in Pennsylvania refused to extend trade secret protection to subscriber mailing lists from a state-owned game magazine, reasoning that the magazine involved a government function because it comprised a "useful governmental means of conveying [game-related] information," and was thereby subject to state disclosure laws.[245] As with the criminal prosecution and infrastructure contexts, government assertions of trade secrecy shroud important matters from oversight.

C. DIGNITARY CONCERNS REGARDING EMPLOYEES

Our third category is dignitary concerns—those concerning corporate claims of trade secrecy or confidentiality where the purported property right lies in attributes of employees' bodies, wages, and other aspects of their personhood. These claims tend to center on cases involving employer–employee relations, where the employer claims control over information about its workforce either to stifle worker mobility or to render its internal practices toward employees opaque to journalists or regulators.

In many ways, this constellation of cases, at first glance, might be construed as the least "nontraditional" of those we have explored because they resemble the common fact pattern involving an employee who seeks to switch jobs and join a competitor. But our focus is not on these traditional claims brought by a former employer, whether under trade secret law or the restrictive covenants permitted in most states. Instead, we highlight here nontraditional claims of trade secrecy that stray beyond the normal boundaries of the DTSA and UTSA—and thus share something in common with the larger pattern we identify in this Article.

The difference, we argue, lies in the subject matter of what is being claimed as a trade secret. For example, civil misappropriation claims asserting that employee salaries—or even employee identities—constitute an employer's trade secrets have nothing to do with incentivizing innovation. They instead have everything to do with throttling employee discussions of working conditions and better salaries elsewhere—in the aggregate, issues of great public interest. The general discourse around employee mobility focuses on the viability of noncompetition

marketing strategy, because it included information about business initiatives, customers, marketing methods and product development, among other areas of information. *Id.* at 182.

244. *Id.* at 185–87. The Pennsylvania state court, however, rejected PHEAA's assertions, reasoning that even though PHEAA's activities are profit-generating, it "does not change the fact that it is a public corporation and a government instrumentality and that its earnings are public moneys about which the public has a right to know." *Id.*; *see* State *ex rel.* Besser v. Ohio State Univ., 721 N.E.2d 1044, 1050 (Ohio 2000) (requiring *in camera* inspection where a public entity claimed a trade secret exemption).

245. Hoffman v. Pa. Game Comm'n, 455 A.2d 731, 733 (Pa. Commw. Ct. 1983).

covenants and the ambiguous boundaries between information an employee is allowed to transport from job to job and the former employer's trade secrets.[246] For example, and using the well-publicized *Waymo*/*Uber* litigation for a probing analysis, Camilla Hrdy has highlighted a "paradox" in the treatment of information employers disclose to employees: some of it is protectable as a trade secret; some is unprotectable information that is generally known; and some is a fuzzy category of skills, knowledge, and experience that employees can transport from job to job even if it is not publicly available.[247] We supplement such analyses here with a focus on a different category of civil misappropriation claims that seek to seclude salary and workplace comparisons from employee discussion.

1. Nontraditional Claims in Employee Mobility Cases

One type of the nontraditional trade secret claims we identify in this Article is seen in civil trade secret and employee mobility lawsuits. The claim is that an employer owns trade secrets in the salaries of its employees. A similar claim is that the employer also owns trade secrets in performance reviews and even employees' identities.[248] In lawsuits where a former employer sues a departing employee for trade secret misappropriation, breach of a restrictive covenant, or both, the employer raises these additional types of trade secret claims, often alongside more common trade secret claims involving customer lists and technology.[249]

246. *See, e.g.*, Charles Tait Graves, *Analyzing the Non-Competition Covenant as a Category of Intellectual Property Regulation*, 3 HASTINGS SCI. & TECH. L.J. 69 (2011) (collecting and critiquing scholarly commentary on employee restrictive covenants over several decades, and arguing that such covenants operate as a covert and mainly standard-free version of trade secret law); Camilla A. Hrdy, *The General Knowledge, Skill, and Experience Paradox*, 60 B.C. L. REV. 2409 (2019) (discussing the common law doctrine that carves out one part of what employees learn on the job as nonpublic but not protectable as the employer's trade secrets).

247. *See* Hrdy, *supra* note 246, at 2416–17.

248. Such claims are an outgrowth of, but not the same as, restrictions on employee mobility under more traditional trade secret claims and under the law of restrictive covenants. Such restrictions are by no means new. For studies on this history, see FISK, *supra* note 12; ORREN, *supra* note 12; Bottomley, *supra* note 12.

249. *E.g.*, Capstone Logistics Holdings, Inc. v. Navarete, No. 17-cv-4819 (GBD), 2018 WL 6786338, at *3 n.4, *12, *31–32 (S.D.N.Y. Oct. 25, 2018), *aff'd and remanded in part*, 796 F. App'x 55 (2d Cir. 2020) (issuing preliminary injunction against former employees on a host of contract, trade secret, and tort causes of action for taking employee contact and salary information found to be "confidential" and protectable and hiring employees away); DigitalGlobe, Inc. v. Paladino, 269 F. Supp. 3d 1112, 1116, 1120, 1128 (D. Col. 2017) (denying motion for preliminary injunction to enforce noncompetition covenant, but noting that employer claimed "confidential information"—which the court deemed a motion to protect trade secrets—in salary information); Denson Int'l Ltd. v. Liberty Diversified Int'l, Inc., No. 12-3109(DSD/JSM), 2015 WL 5123262, at *13 (D. Minn. Sept. 1, 2015) (granting summary judgment to defendant where plaintiff's list of purported trade secrets—employee "salaries" among them—failed largely for lack of specificity); Marlite, Inc. v. Canas, No. 5:09CV1401, 2009 WL 7272686, at *11 (N.D. Ohio July 22, 2009) (granting preliminary injunction against former employee that included prohibition on using trade secrets, such as "lists of employees and salary information"); First Health Grp. Corp. v. Nat'l Prescription Adm'rs., Inc., 155 F. Supp. 2d 194, 227, 237 (M.D. Pa. 2001) (finding that plaintiff's trade secrets were likely to include its "staff salary structure"); Sunbelt Rentals, Inc. v. Head & Enquist Equip., LLC, 620 S.E.2d 222, 227, 229 (N.C. Ct. App. 2005)

For example—and in a case notable for mistakes in applying California law—a federal court in Los Angeles considered a motion to dismiss where a former employer alleged that a former employee had relied upon "confidential employee contact and salary information" when attempting to hire away former coworkers.[250] The employer complained that in some cases it "had to pay bonuses to some of these employees in order to retain them."[251] The court denied the motion, reasoning that the employer had stated a claim because the former employee had used "confidential" information in contacting and seeking to hire others.[252] Note again the subtle, unquestioned treatment of trade secrecy in such contexts. The decision does not question whether contact information or salaries are the property of an employer, and does not comment on the employer's apparent desire to use trade secret law as a salary-suppression device.[253] In another unusual fact pattern, an employer defeated a discrimination lawsuit by showing that it had terminated an employee for discussing coworkers' salaries to other employees—when the employee handbook deemed such salary information "confidential."[254]

Not every such claim succeeds. In a recent case in Florida, a federal district court rejected a claim that mere employee identities were trade secrets for the

(affirming damages award where plaintiff's claimed trade secrets included "employees' salaries" and employees were accused of "*en masse*" hiring from defendant); Gallagher Healthcare Ins. Servs. v. Vogelsang, 312 S.W.3d 640, 644–45, 651–52 (Tex. App. 2009) (finding employee salary information to be among categories of information protected as trade secret when enforcing noncompetition covenant against former employee). These cases should be distinguished from situations where a fiduciary solicits coworkers for a new venture while still employed. *See, e.g.*, Bancroft-Whitney Co. v. Glen, 411 P.2d 921, 925 (Cal. 1966) (describing how an officer worked with a competitor while still employed to hire employees and sabotage potential raises for coworkers so that they would be more likely to leave).

250. *See* Luck v. OTX Acquisition Corp., CV 10-1671 SVW (PJWx), 2010 WL 11595817, at *4–5 (C.D. Cal. Aug. 3, 2010) (ruling on breach of contract and Business & Professions Code Section 17200 causes of action). The ruling contained important mistakes in applying California law. It badly misconstrued California's law of broad UTSA preemption of claims over "confidential" information, demonstrating a strong bias in favor of the employer. *See id.* at *7–8 (misconstruing K.C. Multimedia, Inc. v. Bank of Am. Tech. & Operations, Inc., 171 Cal. App. 4th 939, 90 Cal. Rptr. 3d 247 (2009), to conclude that UTSA preemption applies only when the plaintiff successfully establishes a trade secret, and that if it does not, it gets a second bite at the apple through an alternative claim for "confidential" information). Its approval of employee nonsolicitation covenants, following a 1985 California decision which had incorrectly relied on Georgia law, is bad law in the wake of AMN Healthcare v. Aya Healthcare, 28 Cal. App. 5th 923, 936, 239 Cal. Rptr. 3d 577, 587–88 (2018) (finding coworker nonsolicitation clauses invalid under California law). Given these errors, it is perhaps less surprising that the court was willing to accept claims that salary information belongs to the employer.

251. *Luck*, 2010 WL 11595817, at *4.

252. *See id.* at *12.

253. Employers' efforts to claim employee salary information as a trade secret has an important link to growing policy debates over salary disparities. Such intellectual property hinders open discussion of salaries and thus may contribute to unequal or unduly low pay for some employees. *See* Orly Lobel, *Knowledge Pays: Reversing Information Flows and the Future of Pay Equity*, 120 COLUM. L. REV. 547 (2020) (discussing recent legislative reforms regarding many types of workplace salary disparities and noting that transparency aids in such efforts).

254. *See* Jordan v. Olsten Corp., 111 F. Supp. 2d 227, 238 (W.D.N.Y. 2000).

purposes of stating a misappropriation claim.[255] But it still suggested that similar information might be protectable on a motion to amend.[256] The court offered, in dicta, that "[a]lthough information compiled about an employee—such as a performance review or a salary recommendation—might constitute a trade secret, the plaintiffs allege misappropriation of the employee's identity only."[257]

As we discuss further in Part III, these nontraditional civil trade secret misappropriation claims aimed at employee salaries, reviews, and mere identities are vulnerable to a host of challenges—not least whether the employer has a property right sufficient to give standing to sue over such information in the first place. An analogy helps illustrate the point. Under any version of trade secret law, it is widely accepted that no company holds trade secret rights in the general knowledge, training, skills, and experience of its workforce, even though such information relates directly to a competitive business context.[258] For example, when a Pennsylvania employer sought to enjoin a departing employee on the thesis that it owned trade secrets in how a customer wanted a number to be placed on a purchase order, and also that the customer preferred Excel over PDF, the court rejected its request, reasoning that the employee's "subject[ive] knowledge obtained while in the course of employment" is not the employer's trade secret.[259] Or, as one California court memorably observed, "a stable of trained and talented at-will employees does not constitute an employer's trade secret."[260] These

255. *See* ProV Int'l, Inc. v. Lucca, No. 8:19-cv-978-T-23AAS, 2019 WL 5578880, at *3 (M.D. Fla. Oct. 29, 2019) (granting motion to dismiss with leave to amend after finding that the amended complaint had alleged no facts demonstrating—or even suggesting—that the identities of the plaintiffs' employees constituted trade secrets, and elaborating further that "the amended complaint alleges no facts suggesting that the plaintiffs concealed the identity of the plaintiffs' employees or that the plaintiffs prohibited employees from disclosing the company for whom the employees worked").

256. *See id*. It then denied the request for injunctive relief because "the plaintiffs' allegations undermine the likelihood of irreparable harm because the plaintiffs admit that by increasing employee salary the plaintiffs have thwarted most of the defendants' solicitation effort." *Id*. at *5.

257. *See id*. at *3.

258. For a thorough exploration of this sometimes-elusive concept across the decades in case law and commentary, see Hrdy, *supra* note 246; see also Oxford Glob. Res. v. Consolo, No. CA024763BLS2, 2002 WL 32130445, at *5 (Mass. Super. Ct. May 6, 2002) ("Oxford cannot prevent Consolo from using his own skills, knowledge, or talent or prevent him from ordinary competition, but it may enforce its legitimate business interests by prohibiting the disclosure of confidential and proprietary information."). For a recent ruling applying the principle to grant summary judgment where a former employer's vague trade secret claims were no more than the general knowledge of the trade, see Calendar Research LLC v. StubHub, Inc., No. 2:17-cv-04062-SVW-SS, 2020 U.S Dist. LEXIS 112361, at *18–19 (C.D. Cal. May 13, 2020).

259. *See* Razor Tech., LLC v. Hendrickson, No. 18-654, 2018 U.S. Dist. LEXIS 74918, at *27–28 (E.D. Pa. May 3, 2018); *see also* Ret. Grp. v. Galante, 176 Cal. App. 4th 1226, 1237 98 Cal. Rptr. 3d 585, 592 (2009) ("[A] former employee may use general knowledge, skill, and experience acquired in his or her former employment in competition with a former employer . . . ."); Triton Constr. v. E. Shore Elec. Servs., No. 3290–VCP, 2009 WL 1387115, at *21–22 (Del. Ch. May 18, 2009) (noting that costs of labor, material, and equipment were publicly discoverable and therefore not trade secrets); Robert Half of Pa., Inc. v. Feight, No. 1667, 2000 WL 33223697 (Pa. Ct. Comm. Pl. June 29, 2000) (distinguishing between well-known sales techniques and trade secrets).

260. Metro Traffic Control, Inc. v. Shadow Traffic Network, 22 Cal. App. 4th 853, 862, 27 Cal. Rptr. 2d 573, 579 (1994).

principles apply with even greater force to the nontraditional types of trade secret claims at issue here.

Indeed, the seminal article by Camilla Hrdy reminds us that employees' general skills, knowledge, training, and experience constitute a distinct category of nonprotectable information. They are different from information that is publicly available, or readily ascertainable, but that otherwise might have been protectable.[261] Unlike information that might qualify for trade secrecy but for being publicly available, this doctrine "mandates that even if the information was developed by the plaintiff-employer, and is completely unknown to others outside the company, it can still fall into the unprotectable skill and knowledge of the employee against whom trade secret law is being used."[262] For our purposes, this is a useful comparison: if employers cannot claim property rights in this category of business-focused information gained from marketplace competition—for example, an employee's view of the best way to deploy .NET or Java or any other software programming language—the case for trade secrecy is even *weaker* for employee attributes having no such direct connection to the commercial goals of the business, such as salaries, identities, and performance evaluations.

Even more notably, the cases discussed above directly conflict with recent legislation in a host of states that permit employees to discuss and raise questions about coworker salaries, thereby undercutting the notion that salary information belongs to an employer as a protected trade secret.[263] Most of the state enactments are similar. By way of example, the Delaware salary transparency statute limits contract terms, job requirements, and termination or discipline aimed at discussing salaries in the workplace.[264] Many such statutes followed in the wake of a 2014 executive order from the Obama Administration, which explained the policy goals underlying it:

261. *See* Hrdy, *supra* note 246, at 2450 ("[M]any courts today are apparently operating under the incorrect assumption that the General Knowledge, Skill, and Experience Exclusion is largely the same as the not generally known or readily ascertainable requirement.").

262. *Id*. at 2456.

263. Some of these state statutes are broader than others, but the general gist is that employers cannot use contracts to prohibit such discussions and inquiries. *See, e.g*., CAL. LAB. CODE § 1197.5(k)(1) (West 2020); COLO. REV. STAT. § 24-34-402 (West 2020); CONN. GEN. STAT. ANN. § 31-40z (West 2020); DEL. CODE ANN. tit. 19, § 711(i) (West 2020); ME. REV. STAT. ANN. tit. 26, § 628 (2019) (limiting the prohibition to cases where "the purpose of the disclosure or inquiry is to enforce the rights granted by this section"); MINN. STAT. ANN § 181.172 (West 2020); NEV. REV. STAT. ANN. § 613.330.2.(c), 3.(c) (West 2020).

264. *See* DEL. CODE ANN. tit. 19, § 711(i)(1)–(4) (West 2020) ("It shall be an unlawful employment practice for an employer to: (1) Require as a condition of employment that an employee refrain from inquiring about, discussing, or disclosing his or her wages or the wages of another employee. (2) Require an employee to sign a waiver or other document which purports to deny an employee the right to disclose or discuss his or her wages. (3) Discharge, formally discipline, or otherwise discriminate against an employee for inquiring about, discussing, or disclosing his or her wages or the wages of another employee. (4) Nothing in this section creates an obligation for an employer or employee to disclose wages.").

> When employees are prohibited from inquiring about, disclosing, or discussing their compensation with fellow workers, compensation discrimination is much more difficult to discover and remediate, and more likely to persist. Such prohibitions (either express or tacit) also restrict the amount of information available to participants in the Federal contracting labor pool, which tends to diminish market efficiency and decrease the likelihood that the most qualified and productive workers are hired at the market efficient price.[265]

It thus provided that contractors for the federal government "will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant."[266]

To be sure, these statutes are not explicitly about intellectual property law. Still, the restriction on contract terms that forbid disclosing or discussing salary information appears to be aimed at the confidentiality clauses that are ubiquitous in employment agreements and generally cover information that falls into traditional categories of trade secret law. That exclusion undermines the notion that salary information can be secluded as an employer's trade secret.[267] Nevertheless, lawsuits over employee salaries (or identities) are a troubling example of trade secret law's creep into nontraditional categories of information. Using the workplace transparency statutes as an example, we will discuss the possibilities of such specific legislative enactments to combat nontraditional trade secret claims below.

2. Diversity Data as Secrecy

A different context where employers press nontraditional trade secrets is seen where companies disclose data about workplace diversity to the government and then resist disclosure to journalists. As we have suggested throughout this

265. Exec. Order No. 13,665, 79 Fed. Reg. 20,749 (Apr. 8, 2014).

266. *Id.*; *see* Tinley Park Hotel & Convention Ctr., LLC, 367 N.L.R.B. No. 60, 2019 WL 172167, at *1 (Jan. 8, 2019) (ordering hotel to cease imposing a rule that would have prohibited employees from discussing their wages and other terms of employment). Notably, NLRB regulations have long frowned upon employers who prohibit their employees from sharing wage information. *See, e.g.*, 29 U.S.C. §§ 151–159 (2018); Tex. Instruments, Inc. v. NLRB, 599 F.2d 1067, 1073–74 (1st Cir. 1979) (affirming NLRB finding that company violated regulations by barring employees from sharing wage information during labor campaign, where employer had argued that disclosure would cause others to "raid" its employees, although the employer had disclosed wage data to its own nearby competitors). The difference is that such NLRB actions often arise in labor-organizing contexts which are distinct from employers seeking to claim trade secrets in salary information to stop one-off hiring instances where a former employee seeks to hire former coworkers for a new job.

267. There may be a more direct way to tie these new enactments to state trade secret statutes. In California, for example, case law dictates that newer statutes are deemed to have been enacted by the legislature with full knowledge of existing statutes and judicial decisions, and are not presumed to overthrow long-established principles of law in the absence of clear intent to do so. *See, e.g.*, Young v. Gannon, 97 Cal. App. 4th 209, 223, 118 Cal. Rptr. 2d 187, 198–99 (2002) (stating rules for interpreting statutes); Gaetani v. Goss-Golden W. Sheet Metal Profit Sharing Plan, 84 Cal. App. 4th 1118, 1127, 101 Cal. Rptr. 2d 432, 438 (2000) (same).

Article, private and public entities have attempted to recast a wide variety of contexts—clinical data, chemical data, municipal data, and data about criminal prosecution and public benefits—as trade secrets. And this tendency can extend to even the most personal of circumstances, involving employer efforts to recast employee attributes—like salaries—as corporate property. But these tendencies can extend to a wider collection of aggregated data, and not just courtroom attacks on individual employees who have changed jobs and sought to hire their friends and former coworkers. Indeed, companies sometimes attempt to block the release of records submitted to government agencies that aggregate facts about their workforces. Indeed, this may be the area where corporate arguments for seclusion are the most dubious. Here, companies—and the government lawyers aligned with them to try to block disclosure—offer dubious propositions about why the information at issue is supposedly confidential and how its release would supposedly subject them to harms inflicted by competitors, even when their goal is palpably to block potentially unfavorable media coverage.

One example is diversity data, or the aggregated record of the race or ethnicities of employees in the workplace. This is an issue brought to light by Jamillah Bowman Williams in a comprehensive 2019 article outlining how companies have sought to block the release of the information they have submitted to the government, contending that disclosure would somehow reveal secret strategies to recruit diverse candidates and cause competitors to hire these employees away from them.[268] As she details, a number of prominent companies have asserted that internal diversity data is a trade secret.[269] Microsoft made this argument in a sex discrimination lawsuit to prevent its diversity data from becoming public; IBM made a similar argument in a lawsuit seeking to prevent a former employee from taking a job at Microsoft, arguing that her knowledge of diversity data would cause competitive harm.[270] Many technology companies have utilized Exemption 4 under FOIA for the same purpose.[271]

The arguments made in favor of seclusion demonstrate how far such claims stray from traditional goals of trade secret law to protect business information developed for marketplace competition. The first rationale has to do with the idea of investment—that the company has invested significant resources in developing its diversity initiatives.[272] But spending money on something does not make it a trade secret; expenditures are not even a factor in the elements of establishing a trade secret under the DTSA and the UTSA. The second is that the information

268. *See* Williams, *supra* note 8.

269. *See id*. at 1697–98.

270. *See id*. (discussing Moussouris v. Microsoft Corp., No. 15-cv-1483 JLR, 2018 WL 1159251, at *11–12 (W.D. Wash. Feb. 16, 2018)); *id*. at 1699 (discussing IBM v. McIntyre, No. 18-cv-01210, 2018 WL 1325712 (S.D.N.Y. Mar. 8, 2018)). As Williams reports, the special master in the former "distinguished between information—like strategies—that may be used to enhance the business of competitors and information—like data—that only has the potential to cause reputational damage," and found that the treatment of information as confidential did not render it a trade secret. *Id*. at 1698.

271. *See id*. at 1688.

272. *See id*. at 1697.

should be protected because disclosure supposedly risks enabling competitors to mimic diversity initiatives and recruit talent away from the company.[273] A third argument is the risk that, upon disclosure, diversity data might be "misconstrued by outsiders and cause unnecessary disruption to [a company's] business or improperly confuse and/or influence [the company's] customers, employees, or potential employees," harming its interests.[274] And a final rationale is, in classic circular fashion, that the information should be kept confidential because the employees supposedly expect the (aggregated and anonymized) data to remain confidential.

At the heart of these flimsy arguments is the same concern that underlines so many of the issues identified in this Article: the desire to use trade secrecy to conceal nontraditional forms of information whose disclosure might lead to reputational harm, exposure of wrongdoing, or simply greater latitude for employees to seek better jobs (and perhaps better salaries) elsewhere. If diversity data is kept confidential, the public may never learn about, or debate strategies for, reducing diversity problems inside companies and industries.[275] As Williams explains, diversity data regarding technology companies is minimally reported and difficult to find, despite efforts by legislators and shareholders to require or encourage disclosure.[276] When CNN attempted to report on diversity data from twenty influential technology companies in 2011, only three agreed to share their data. Seventeen others refused. When CNN turned to FOIA, filing requests for diversity data that companies had disclosed to the Department of Labor, several companies filed objections under Exemption 4, and thus the government disclosed the data from only five companies.[277]

Such efforts at data seclusion can be contradictory. Facts about the ethnic or racial background of employees are not the traditional subject matter of trade secret law, because such facts have no (or little) plausible connection to developing information for use in the marketplace.[278] And it is equally dubious that strategies for recruiting diverse employees would constitute a protectable trade secret either; after all, it is likely that companies and diversity consultants are using the same or similar strategies and processes to retain employees.[279] Moreover, despite these claims to secrecy, companies often publicize their diversity initiatives.[280] Such inconsistent conduct speaks volumes about the motives behind efforts by some companies to seclude diversity data.

---

273. *See id.*

274. *Id.* at 1697 (quoting Moussouris v. Microsoft Corp., No. 15-cv-1483 JLR, 2018 WL 1159251, at *12 (W.D. Wash. Feb. 16, 2018)).

275. *See id.* at 1688.

276. *See id.* at 1693.

277. *See id.* at 1693–95 (listing seventeen companies).

278. *See id.* at 1696 (noting that a "numerical 'count'" of data looks very different from the traditional type of trade secret, which normally aims to protect the products of either "innovation or substantial effort").

279. *See id.* at 1700 (noting the case of IBM, which has displayed its diversity initiatives, programming, and related strategies with great pride).

280. *See id.* at 1706.

The Center for Investigative Reporting has recently faced such arguments when seeking diversity data records on behalf of a journalist. In 2019, the center filed suit to seek the release of workplace diversity data submitted to government agencies (EEO-1 reports).[281] In response, government lawyers defended the confidentiality exemption on behalf of companies who offered trade-secret-style intellectual property arguments for seclusion.[282]

Again, these arguments are notable not just for their weakness, but for their generic and conclusory propositions of harm without empirical support. Indeed, quoting directly from corporate declarations, attorneys for the Department of Labor contended that "disclosure of the information would 'provide [the company's] competitors insights into its strategy, operations, recruiting, and labor costs' . . . 'if EEO-1 information were regularly released, [] it would allow competitors to discern shifts and strategies for the business going forward, in a highly competitive field.'"[283] Another company resisting disclosure claimed that "[t]he report also includes crucial information about the diversity of [the company's] workforce, which competitors could use to target the Company's talent."[284] And yet another contended that the reports "communicate [the company's] experience and expertise in the field of how to structure the workforce to have a well-run, profitable, and efficient company."[285]

In this case, the district court granted the center's motion for disclosure, finding, among other things, that these corporate arguments were "conclusory declarations" which sometimes featured a "verbatim rationale," and that "other declarations misrepresent the breadth of information found in the EEO-1 reports."[286] The government's vague assertions in the case palpably demonstrate how intellectual property-type arguments are being squeezed into the service of other objectives. Each company hoped to avoid potentially negative media coverage—likely about their relative lack of diversity—but could not offer such a crass motive out loud. The case is currently on appeal.[287]

3. Harms as Secrets

Finally, corporate claims to trade secrets and "confidential" information about employee attributes have become so extreme that companies have even attempted to treat harms suffered by employees as trade secrets. These are perhaps the most unbelievable of extreme secrecy assertions: episodes of workplace harassment and injury where the employer acts as a possessor of intellectual property rights

281. *See* Complaint for Injunctive Relief, Ctr. for Investigative Reporting v. U.S. Dep't of Labor, 424 F. Supp. 3d 771 (N.D. Cal. 2019) (No. 4:19-cv-01843-KAW), ECF No. 1.

282. Motion for Summary Judgment at 1–2, *Ctr. for Investigative Reporting*, 424 F. Supp. 3d 771, 2019 WL 8353504, ECF No. 24.

283. *Id.* at 10–11 (first alteration in original).

284. *Id.* at 11.

285. *Id.*

286. *Ctr. for Investigative Reporting*, 424 F. Supp. 3d at 777–78.

287. *See* Ctr. for Investigative Reporting v. U.S. Dep't of Labor, 424 F. Supp. 3d 771 (N.D. Cal. 2019), *appeal filed* (9th Cir. Aug. 5, 2020).

and thus is able to cause harm (or have its employees cause harm to coworkers), all while suppressing reporting on those harms. Although recent court decisions rejecting such arguments, together with new laws against suppressing information about workplace harassment, are encouraging signs that such facile positions should not succeed, the danger remains.

One example concerns injuries in the workplace. Much like diversity data, companies have also offered notably implausible arguments in their efforts to prevent the release of aggregated workplace injury data. For example, in 2018 and 2019, the Center for Investigative Reporting brought two actions in support of journalists who had sought records under FOIA from the Department of Labor concerning aggregated workplace injury data that companies had submitted to the Occupational Health and Safety Administration (OSHA). The center pointed out that "[f]or decades, OSHA has disclosed these records in response to FOIA requests."[288] OSHA had even announced a rule in 2016 requiring large employers to provide additional workplace injury information.[289]

Yet in a stunning move, the Trump Administration resisted disclosure at the behest of those companies, asserting instead that the information fell within FOIA's "confidentiality" exemption.[290] Rather than taking a position on behalf of the public interest in disclosing facts about workplace injuries, the government's arguments instead spoke largely in the voice of a would-be intellectual property owner, predicting that competitors would somehow divine meaningful information from the injury reports in order to inflict marketplace harm.

The government quoted various corporate declarants directly, speculating that the required reports would "reveal a company's flow of orders and likely provide an employee head count," warning that "'[a]ny competitor could take this information and use it to their advantage.'"[291] Its assertions led to fanciful conjecture about rivals doing detective work to unearth supposedly meaningful information from OSHA injury disclosures, including the business' "overall capacity and

288. Opposition to Defendant's Motion for Summary Judgment and Notice of Cross Motion and Cross Motion for Summary Judgment at 1, Ctr. for Investigative Reporting v. U.S. Dep't of Labor, No. 4:18-cv-02414-DMR (N.D. Cal. June 19, 2020), ECF No. 30. It also noted that, pursuant to OSHA's own regulations, "(i) companies are required to post OSHA Reports in the workplace, (ii) companies disclose OSHA reports to *all* employees upon request, and (iii) the Reports contain no secret or private information, as most employees know who gets sick and injured at work." *Id.* at 2 (citing OSHA regulations). We thank Victoria Baranetsky of the Center for Investigative Reporting for alerting us to these cases and providing helpful information about them.

289. *See* Improve Tracking of Workplace Injuries and Illnesses, 81 Fed. Reg. 29,624 (May 12, 2016). The Trump Administration rolled back this rule in 2019. *See* 84 Fed. Reg. 380 (Jan. 25, 2019).

290. *See* Opposition to Defendant's Motion for Summary Judgment and Notice of Cross Motion and Cross Motion for Summary Judgment, *supra* note 288, at 14 (citing Improve Tracking of Workplace Injuries and Illnesses, 78 Fed. Reg. 67,254 (Nov. 8, 2013)).

291. Defendant's Motion for Summary Judgment at 17, *Ctr. for Investigative Reporting*, No. 4:18-cv-02414-DMR, ECF No. 26. Another posited that "[m]any businesses consider employee head count and hours worked to be proprietary information. This information could be used to determine business processes as well as company approaches to operations and security." *Id.*

productivity"[292] and its "general liability costs,"[293] and a warning that "[p]roviding a competitor with information that could help assess a firm's insurance costs could be the difference between winning and losing a bid."[294]

We have little doubt that the real reason behind the resistance to revealing workplace injury information was simple: to conceal the reports, and thereby protect the reputation of the employer from potentially negative press, or to reduce opportunities for labor organizing. Notably, none of these goals was attributable to protecting the safety of the company workforce. In fact, just the opposite was discussed. The government argued that without context regarding the source of injuries, the public might "conclude, incorrectly, that the mere fact that injuries and illnesses occurred in their facilities necessarily means they have unsafe workplaces," enabling competitors to somehow "obtain leverage during legal and other disputes."[295] It continued, "although the data [will] have limited meaning when examined in isolation," the government warned, "release of the data will cause unfair and irreparable harm to employers' reputations."[296] In a similar case, it took the same position on behalf of Amazon, again offering strained conjectures about what seemingly omniscient competitors might glean from such injury data.[297]

Like its arguments about insurance rate visibility, these assertions are notable for their lack of specificity, empirical support, and any real explanation why competitors would use injury data to improve their position in the marketplace. Perhaps least credible of all, the government suggested, without explanation, that workplace safety was *itself* a rationale for suppressing disclosure.[298] In both cases, the district court rejected these specious arguments, finding that the type of

---

292. *Id.* at 18 ("Armed with total hours worked plus an establishment's employee count, a business' overall capacity and productivity can easily be determined.").

293. *Id.* at 19 (predicting that "[a]n employer's rate of accidents, hours worked, and number of employees[,] are all factors that influence general liability insurance costs" (alterations in original)).

294. *Id.* at 19 (alteration in original). Notably, even if these arguments had any basis in reality, the OSHA statements do not include insurance rates, and bare injury data alone could not be used to calculate insurance rates because so many other factors would be part of an insurance agreement. Perhaps most important, the notion that rivals could gain anything through the prospect of guessing one another's insurance rates is extremely dubious to begin with—an extreme position that should elicit alarm and not deference.

295. *Id.*

296. *Id.*

297. *See* Defendant's Motion for Summary Judgment at 12, 16, Ctr. for Investigative Reporting v. U.S. Dep't of Labor, 470 F. Supp. 3d 1096 (N.D. Cal. 2020) (No. 19-cv-05603-SK), ECF No. 25 [hereinafter "Amazon's Motion for Summary Judgment"] ("Data regarding injury and illnesses, including lost time, permits Amazon to evaluate and predict costs associated with worker's compensation, employee absences, and short- and long-term disability and assists Amazon in measuring economic effectiveness and in maximizing efficiency."); *see also id.* ("The total injuries and illnesses are listed by category, and this information could be used to profile Amazon's injury trends at individual fulfilment centers, which Amazon considers to be sensitive and proprietary information.").

298. *See id.* at 13 (concluding that "[t]his information is also important for the enhancement of worker safety and the protection of its workforce"). The statement has the feel of lawyers drawing up a list of arguments for a corporate representative to repeat in an affidavit rather than something reflecting any real-world facts.

information at issue was not "confidential" for FOIA purposes where the Department of Labor's own regulations permitted employees to receive and share such information without restrictions.[299] As one judge in the Northern District of California ruled in June 2020, comments from employers seeking seclusion "do not speak to how the owners keep and treat the [injury data]; instead, they focus on the reasons why the owners oppose the release of the information."[300]

The question remains, however, why the Trump Administration assisted companies in time-consuming and burdensome efforts to block journalists, making such strained arguments in favor of seclusion.

Another example of workplace harms, albeit one where the tide may have turned in favor of disclosure, concerns efforts by employers to suppress information about workplace sexual harassment through mandatory arbitration clauses and nondisclosure clauses in settlement agreements.[301] Starting in 2017, #MeToo demonstrated that many alleged harassers were able to continue their careers because employee-victims had been silenced and had their ability to pursue cases in court restricted.[302]

In reaction to public outrage and media scrutiny, at least thirteen states enacted laws on these issues between 2018 and 2020. Some of these statutes prohibited or placed conditions upon mandatory arbitration in sexual harassment cases;[303]

---

299. *See* Ctr. for Investigative Reporting v. U.S. Dep't of Labor, 470 F. Supp. 3d 1096, 1112 (N.D. Cal. 2020) ("The Court finds that Amazon's broad disclosures required under the regulations to all current employees, former employees, and employees' representatives, with no restrictions on their further disclosures, defeats the DOL's effort to demonstrate confidentiality."); Order on Cross Motions for Summary Judgment at 10, Ctr. for Investigative Reporting v. U.S. Dep't of Labor, No.18-cv-02414-DMR, 2020 WL 2995209, at *1 (N.D. Cal. June 4, 2020), ECF No. 41.

300. Order on Cross Motions for Summary Judgment, *supra* note 299, at *4 (granting summary judgment in favor of the Center for Investigative Reporting, as records were not customarily treated as confidential because employers were duty-bound to share them with employees); *see also* Magistrate Judge's Report and Recommendation at 2, 13–14, 16–22, Pub. Citizen Found. v. U.S. Dep't of Labor, No. 1:18-cv-00117-EGS/GMH (D.D.C. June 23, 2020), ECF No. 37 (ruling in favor of release of workplace injury and illness data and rejecting notion that information was customarily confidential because some companies subjectively believed it so while other companies do not).

301. For commentary on the harms caused by confidential harassment settlements, see Minna J. Kotkin, *Reconsidering Confidential Settlements in the #MeToo Era*, 54 U.S.F. L. REV. 517, 525 (2020) (noting how confidentiality may create a false sense that harassment cases are less prevalent, or a thing of the past, and may reduce the deterrent effect of large settlement payments or litigation judgments). For related commentary, see Taishi Duchicela, *Rethinking Nondisclosure Agreements in Sexual Misconduct Cases*, 20 LOY. J. PUB. INT. L. 53 (2018) (arguing against use of nondisclosure agreements in such cases); Matthew Durham & Sarah Odia, *Non-Disclosure Agreements in the World of #MeToo*, 27 NEV. LAW. 16 (2019) (describing current status of nondisclosure agreement legislation in Arizona, California, and Nevada); Kathleen McCullough, *Mandatory Arbitration and Sexual Harassment Claims: #MeToo- and Time's Up-Inspired Action Against the Federal Arbitration Act*, 87 FORDHAM. L. REV. 2653 (2019) (arguing that federal action is needed); and Joan C. Williams, Jodi Short, Margot Brooks, Hilary Hardcastle, Tiffanie Ellis & Rayna Saron, *What's Reasonable Now? Sexual Harassment Law After the Norm Cascade*, 2019 MICH. ST. L. REV. 139 (2019) (studying norm changes after #MeToo).

302. *See* Katie Robertson, *Condé Nast to Limit the Use of NDAs*, N.Y. TIMES (Feb. 21, 2020), https://www.nytimes.com/2020/02/21/business/media/conde-nast-nda.html (noting that Harvey Weinstein and others used nondisclosure agreements to silence victims).

303. *See* ARIZ. REV. STAT. ANN. § 12-720 (2020); MD. CODE ANN., LAB. & EMPL. § 3-715 (West 2020); VT. STAT. ANN. tit. 21, § 495h (West 2021); WASH. REV. CODE § 49.44.210 (2018).

some prohibited or restricted confidentiality agreements in sexual harassment cases;[304] and some also prohibited the use of nondisclosure agreements that would encompass sexual harassment as a condition of employment.[305] These events illustrate not only how companies have attempted to use confidentiality contracts and other tactics to prevent disclosure of facts regarding workplace assaults and harassment but also how the glare of media and public attention can result in rapid change.

As we will discuss below, the information we classify as dignitary concerns does not fit easily, or at all, into the standard definitions of trade secrecy (or "confidential" business information in the FOIA context). An analogy may be useful. It would be dubious to contend that personal data from website users and consumers—the type of information protected by the privacy laws, and by website terms and conditions—is or could be classified as a DTSA trade secret. If someone entered his or her salary into a website which collected that data, for example, that salary information would not thereby become the website's property absent some contractual transfer. That is so because it is not created by the business for competitive purposes. Rather, the salary information is collected from users and reflects their attributes and facts about them. They can freely disclose it to whomever they wish. Its connection with a workplace does not transform it into the company's trade secret. But at least some of the information companies may claim as trade secrets or otherwise confidential information—diversity data, workplace injury data, salary and performance information, or episodes of harassment that harm employees—should fail to qualify for intellectual property protection for similar reasons. A company does not own facts about employees as trade secrets simply because they show up for work every day, much less because they suffer harm at the workplace.

III. RECUPERATING SECRECY FROM SECLUSION

In our three rubrics—investigative concerns, delegative concerns, and dignitary concerns—we have identified a broad constellation of collisions between trade secret laws, open-records laws, and the public interest, often where the information in question is only dubiously classified as a company's intellectual

304. *See* CAL. CIV. PROC. CODE § 1001 (West 2020); NEV. REV. STAT. § 10.195 (West 2020); N.J. SESS. LAW SERV. Ch. 39 §§ 10:5–12.8 (West 2019); OR. REV. STAT. ANN. ch. 462, § 3 (West 2018); TENN. CODE ANN. § 50-1-108 (West 2020).

305. Ch. 820 ILL. COMP. STAT. ANN. 101-0221 / § 96/1-25 (West 2020); N.Y. GEN. OBLIG. LAW § 5-336 (McKinney 2020); VT. STAT. ANN. tit. 21, § 495h (West 2021); VA. CODE ANN. § 40.1-28.01 (West 2020). In tandem, many companies and law firms changed their policies along the same lines. *See, e.g.*, Elana Lyn Gross, *NBCUniversal Releases Former Employees from Nondisclosure Agreements, Spurring the Conversation*, FORBES (Nov. 4, 2019, 5:02 PM), https://www.forbes.com/sites/elanagross/2019/11/04/nbcuniversal-releases-former-employees-from-nondisclosure-agreements-spurring-the-conversation; Angela Morris, *Why 3 BigLaw Firms Ended Use of Mandatory Arbitration Clauses*, ABA JOURNAL (June 1, 2018, 12:15 AM), https://www.abajournal.com/magazine/article/biglaw_mandatory_arbitration_clauses [https://perma.cc/XB3F-SRMG]; Robertson, *supra* note 302; Daisuke Wakabayashi & Jessica Silver-Greenberg, *Facebook to Drop Forced Arbitration in Harassment Cases*, N.Y. TIMES (Nov. 9, 2018), https://www.nytimes.com/2018/11/09/technology/facebook-arbitration-harassment.html.

property. And we have grouped each by the threat posed to public health, exposure of wrongdoing, and employee interests—each of which implicates public interest considerations. The inevitable question is whether there are common methods to approach these problems and to challenge the deference too often given to would-be information owners—or whether, by contrast, each problem requires a unique response not susceptible to a unified approach. A related question is whether the framing of such solutions benefits from a focus on trade secret law, rather than other vantage points in other areas of the law.[306]

Within trade secret law, we believe there are indeed common approaches, even while some problems are also conductive to case-specific solutions. Those interested in pushing back against the expansion of trade secret law into nontraditional areas can articulate means by which legislatures, regulators, and courts can define and rebut trade secret and confidentiality claims over information that is not a trade secret at all. The same is true for information that may qualify as a trade secret, but the purpose of asserting secrecy is not to vindicate the interests promoted by the trade secret statutes, but to suppress information about corporate wrongdoing, control employee attributes, and the like.[307] This requires a mix of practical arguments that litigants can make and judges can apply, today, in courtrooms without any change to existing laws. It also calls for the introduction of theories of how to approach overreaching trade secret claims with the limiting tools that have long been employed by courts in other areas of intellectual property law.

Below, we first detail general insights on both the causes and the solutions of trade secret overbreadth. We then outline potential avenues for reform that focus on (1) a renewed dedication to straightforward elements of trade secret and open-records laws to challenge nontraditional claims that should not be seen as trade secrets or "confidential" corporate property at all—such as standing to bring a claim, the boundaries of trade secrecy definitions, and the concept that employers cannot claim rights in information falling within general employee skills and knowledge; and (2) theories that can limit overreaching claims, either within existing trade secret law—such as the bad faith remedy for improper claims—or reflecting recent scholarship on borrowing limiting doctrines from other areas of intellectual property law, such as trade secret fair use and thin trade secrecy. Finally, we move to potential legislative solutions to curb the abusive assertion of nontraditional trade secret claims.

306. We readily accept that gathering the problems identified here as "nontraditional" trade secrecy assertions is just one possible approach, as some of our commentators have pointed out. Still, we believe that the trade secret focus is what best highlights the problem all these issues share: increasingly aggressive efforts to use IP language, and IP legal tactics, to seclude ever-growing categories of information.

307. As Vicki Cundiff noted at a July 2020 Trade Secrets Scholars Workshop, there is a difference between cases involving a private commercial concern and those involving information that is intimately intertwined with public interests, and focusing early on what is claimed as a trade secret can help distinguish them.

A. NAMING THE PROBLEM

The preceding Section might lead anyone to ask how it is possible that we have arrived at such a troubling crossroads between secrecy and transparency. At the same time, there is something about even traditional trade secret litigation that makes it easy to understand why it would be tempting to stretch its boundaries. As we discussed above, there was no unitary, centralized origin point for trade secret law, which invites interested parties to create ambiguity over its purposes. In addition, unlike forms of intellectual property that require some form of registration and identification before a dispute begins—patents, copyrights, and (sometimes) trademarks—that which is claimed as a "trade secret" in a dispute is infamously protean.[308] Even in ordinary civil cases, plaintiffs may change their definition of the alleged trade secrets as the case proceeds, and perhaps even reach juries with something amorphous.

A sense that trade secrets are a category wide open for subjective interpretation may help explain why some are pushing to enlarge the definitional boundaries. Simply put, when in-house or outside counsel are asked to come up with ways to seclude information to protect the company's reputation from a poor public relations cycle, or to increase company power at the expense of the workforce, small wonder that the loose, make-it-up-as-you-go nature of trade secret claims are so appealing. Both the intrinsic architecture of trade secret law and its contemporary treatment before courts and commentators has added to the problem.

1. The Tangled—and Instrumental—Justifications of Trade Secret Law

In an influential series of discussions several years ago, a number of scholars debated the legal basis for trade secrecy and whether its dominant character stems from theories of property, contract, or other sources of law. Some, like Mark Lemley (and ourselves), tend to view trade secret theory as a largely property-oriented body of law, circumscribed by a number of important limitations.[309] Others find bases for trade secret law in contract or in utilitarian theory, leading them to question its necessity as a body of law.[310]

We are drawn to property as the most appropriate and sensible basis for trade secret protection, and not only because the UTSA and DTSA center upon that approach. Property has boundaries, and thus being able to define an intellectual property claim so that it can be contested can protect weaker parties, such as mobile employees, in a dispute.[311] As its architecture suggests, the purpose of trade secrecy is to offer an instrumental sort of protection that functions, ideally, not as

308. *Cf.* Robin Feldman, RETHINKING PATENT LAW 3 (2012) (positing the bargain theory of patents and arguing that a patent can never grant a clearly bounded set of rights, but merely provides an opportunity to bargain with certain rules in place).

309. *See* Lemley, *supra* note 9, at 313.

310. *See, e.g.*, Bone, *A New Look at Trade Secret Law*, *supra* note 9, at 243; Bone, *The (Still) Shaky Foundations of Trade Secret Law*, *supra* note 9, at 1803.

311. *See* Graves, *supra* note 9, at 59 ("Property has boundaries, after all.").

an end to itself, but rather to keep information from the public eye for the purpose of innovation, entrepreneurship, and commercialization.[312]

Compelling as the property-centered conception of trade secret law is, however, each of these prisms—property, contract, and tort—reflects an incomplete set of considerations as applied to the problems we discuss. For example, many of the complications surrounding the relationship between trade secrecy and the flow of information stem from a fundamental discomfort over what kind of property trade secrets comprise—that is, whether they are akin to a patent, copyright, a piece of real estate, or something else.[313] Exploring this comparison would certainly help navigate the impact of trade secrecy on the flow of information, particularly in relation to other concerns. On this point, the California Supreme Court has concluded that because trade secrets are property, which trumps First Amendment interests, they are immune from challenge under First Amendment principles.[314] But, as Pam Samuelson has persuasively reasoned, contrary arguments can be made in favor of the primacy of First Amendment interests nevertheless.[315]

Although a complete examination of the relationship between the First Amendment and trade secret law is beyond the scope of this Article, it is important to recognize that, like trademark and copyright law in previous decades, the state of trade secret law demonstrates the need for a serious reckoning—a need to reconcile its expansion with the importance of safeguarding the flow of information from censorship and concealment. Indeed, the deleterious impact of trade secret protection on the public's access to information has been noted by other scholars, notably Robert Bone, who recognized that the architecture of trade secret law—particularly its reasonable secrecy requirements, which focus on self-help—actively facilitates concealment over disclosure.[316] It is essential, therefore, to reconsider the roots of trade secret law in terms of its effect on the broader flow of information and the risk of opacity.

The cases we have discussed throughout this Article demonstrate the extreme results of Bone's observation. It is all too easy to focus on the role of trade secret

312. *See* Graves, *supra* note 9, at 41 (asserting that the justification for trade secret law in a property lens is to support the infrastructural nexus for innovation by granting weak property rights, to leave room for mobility and the formation of new businesses); Posner, *supra* note 229, at 8 ("[A] creator of ideas will often seek secrecy in order to enable him to appropriate the social benefits of his creations; and secrecy often requires solitude.").

313. *See* Samuelson, *supra* note 13, at 279.

314. *See id.* at 278 (discussing DVD Copy Control Ass'n v. Bunner, 75 P.3d 1, 13–14 (Cal. 2003)); *see also* EDUARDO MOISÉS PEñALVER & SONIA K. KATYAL, PROPERTY OUTLAWS 75 (2010) (observing that in *Bunner* "the [California] Supreme Court upheld [a] preliminary injunction against [a] free-speech challenge, just as the Second Circuit had"); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1063 (2000) ("Calling a speech restriction a 'property right,' though, doesn't make it any less a speech restriction, and it doesn't make it constitutionally permissible.").

315. *See* Samuelson, *supra* note 13, at 279.

316. Bone, *The (Still) Shaky Foundations of Trade Secret Law*, *supra* note 9, at 1809 (noting that self-help can prevent disclosures before they happen, whereas litigation often tries to contain information after it has already been disclosed and is therefore less effective).

law in adjudicating disputes between competitors and transactional partners. This observation suggests that trade secrecy operates in a dyadic framework that is characterized by competitors as parties to a traditional dispute. In these traditional circumstances, as a whole, trade secret protection is considered more advantageous than excessive, extralegal means of secrecy because even a limited, protected confidential relationship between potential partners still facilitates *some* dissemination of knowledge.[317] In that context, trade secret law does something more than ordinary contract law, because it allows courts to "infer the existence of a confidential relationship from [the] circumstances" of the transaction.[318]

However, in the cases we discuss, we see an even greater set of public interest concerns because most of the parties are not competitors, but third parties. Here, the party seeking the secret is not a potential partner or competitor, but an investigator, scientist, journalist, or member of the broader public—part of a much wider swath of stakeholders than the traditional framework of trade secret law envisioned. They are not seeking to do business with the party claiming trade secret rights, but to share important information with the public or with law enforcement. In our accounting of the nontraditional cases we have collected, disclosure operates in the opposing direction where third parties are concerned. In this fashion, the intrinsic structure of trade secret law can make it difficult to discuss nontraditional cases and their special problems. As a result, none of the prisms normally used to justify trade secrecy—property, contract, or tort law—can fully grapple with the concerns raised by these contemporary, reputation-driven cases.

2. Contemporary Causes of Overbreadth

In addition to the structural aspects of trade secret law discussed above, there are important contemporary causes for trade secret overbreadth in these atypical cases. The first reason involves the much more extensive visibility that is associated with trade secrecy in the corporate realm as trade secret lawsuits have become more prominent. This has produced two effects, linked to one another. The first involves a greater tendency among companies to turn to trade secret law to do the work of concealment. In turn, the success of these cases has a further effect: because these cases result in the desired concealment, the public never receives the benefit of the information nor is it made aware of the role that trade secret law has played in its seclusion.

A second reason for these atypical cases simply reflects the growing dominance of software—not merely in the ways in which governments rely on software providers but in the types of data that companies now aggregate and store,

317. *See* Lemley, *supra* note 9, at 335–36 (arguing that: trade secret law operates as a substitute for costly physical and contractual controls, which companies would otherwise have to rely upon to prevent others from misappropriating their information; trade secrecy actually winds up encouraging disclosure and more dissemination of information; and, ultimately, "a world without trade secret protection is likely to have more, not less, secrecy").

318. *Id*. at 337.

often for regulatory reporting purposes as well as the machine learning tools used by prosecutors in criminal law. Moreover, as we have examined in this Article, the expansion of trade secrecy to areas of basic, publicly available information further demonstrates the benefits of weaponizing trade secret law for concealment.[319] Given the indeterminacy associated with defining a trade secret, there are few obstacles to prevent trade secret owners from overplaying their hands.[320]

A third cause is the relative infirmity of FOIA. The Supreme Court's 2019 *Food Marketing Institute v. Argus Leader Media* decision has potentially made it easier for companies to seek an exemption from disclosure when labeling information "confidential." *Argus Leader*'s conflation of trade secrecy with confidentiality essentially removes any distinction between the two.[321] Varadarajan notes perceptively that *Argus Leader* has essentially conflated the two categories of FOIA:

> By removing the constraint of "substantial competitive harm" and replacing it with a test that more or less aligns with a firm's reasonable secrecy efforts, *Food Marketing*'s practical effect is to collapse the two categories. For all practical purposes, there is now one broad category that fixates primarily on whether requested information is, in fact, public, and if not, whether the submitter treats the information as secret. For why would a submitter or agency defending nondisclosure try to squeeze through a small definitional hole (i.e., FOIA's narrow definition of "trade secret"), when a far larger one has become available (i.e., the expanded definition of "confidential" commercial information)?"[322]

Because the legal right of a trade secret has become so indeterminate under *Argus Leader*, this risks a serious distortion of wide areas of information that concern the public interest.

A final factor may also be the relative lack of public awareness—even among the legal community—about the problems overbroad trade secret claims can pose. Indeed, an immediate difficulty in framing the problems this Article addresses is that trade secret law may not be an area commonly seen as one embedded with public policy concerns. Among practitioners, trade secret law does not carry elite status in the manner of antitrust law or internet regulation, and thus rarely sees the sustained policy discussion common in some other fields.

319. *See id.* at 338 ("If any idea, no matter how public, is subject to a claim of legal rights, individuals and companies will reasonably worry about using any information they do not themselves develop. If I could sue you for repeating my explanation of trade secret law, the result is not likely to be wide discussion of that explanation, even if I have no intention of actually suing you for discussing my idea.").

320. *See id.* (foreshadowing risks for trade secret owners and observing, specifically, that "[i]f [one] can get ownership rights in any information, no matter how public, the result will be to deter, not promote, the dissemination of that information").

321. *See* Varadarajan, *supra* note 11, at 5–6.

322. *Id.* at 35.

Practitioners often take both sides of trade secret disputes—a disincentive to discussions about the appropriate limits of the law because the next case one takes may require advocating the opposite position one just argued on behalf of a previous client. Among law schools, trade secret law remains in the background in course offerings and journal publications compared to other areas of intellectual property and technology law. It is also possible that among the judiciary, familiarity with tedious cases featuring accusations of employee downloading or failed corporate collaboration may downplay any notion that broader societal issues could be at stake. The growth of trade secret and confidentiality claims beyond the traditional scope of trade secret law is not surprising given these events. Yet bringing these cultural factors to the surface is important if reforms are to succeed.

B. QUESTIONING DEFERENCE TO THE TRADE SECRET CLAIMANT

To challenge nontraditional trade secrecy and confidentiality claims, we begin with a return to the basics. It would give too much deference to a company pushing an aggressive claim of secrecy or confidentiality with a genuine intellectual property viewpoint when the real motive is to prevent oversight or conceal wrongdoing. Many such claims are a stretch, and the proponents know it. That is why their arguments—as seen in our examples of workplace injury and diversity data disputes above—are so palpably incredulous.

Indeed, in many of the situations we have identified, the information asserted as a trade secret falls outside the scope of the types of information trade secret law is supposed to protect.[323] The same is true for information claimed as "confidential" in the FOIA context. For example, information about corporate negligence or malfeasance does not meet the standard tests for trade secrecy because competitors cannot take it and use it in their own business. Similarly, information about employee attributes—salaries, performance, or the harmful experience of an injury or harassment at work—is not property that an employer owns, and it is information that employees can freely share with others. Arguably, in at least some cases, attributes or know-how might reasonably be viewed as the *employee*'s proprietary information, rather than information that belongs to the employer.[324] As seen in the recent wave of changes in corporate practices regarding nondisclosure agreements and mandatory arbitration in workplace sexual harassment complaints, illuminating how information is wrongfully claimed as confidential can lead to different outcomes.

In these instances, those who contest such claims may best begin by challenging the assertion of trade secret rights at its foundation, denying that any such protection is possible for that category of information. Such unusual assertions of secrecy should be viewed with great suspicion at the outset. Indeed, in so many of

323. As Jeanne Fromer commented on an earlier draft of this Article, one consequence of information not qualifying as a trade secret is that it precludes any need for a takings analysis where regulation leads to public disclosure.

324. We are grateful to Mark Lemley for this observation.

these cases, these actors are scrambling to block the release of information that might embarrass the company through a bad PR cycle, that might allow employees to more easily move on and join another firm, or that could lead to regulatory fines. Because these motives will not be spoken out loud in briefs or affidavits, the arguments instead speak with the indignant voice of an intellectual property owner. That is a disguise, not an argument backed by any deep insight about the nature of trade secret law. Said differently, a desire to avoid reputational harm is not a sufficient basis to establish intellectual property rights and should not be treated as the same thing. In many cases, then, one must ask if the information being claimed as a trade secret falls within what trade secret law is supposed to encompass.[325]

1. Standing to Claim Rights in Nontraditional Information

We begin our strategic proposals for combatting nontraditional trade secret claims with the observation that standing—that is, whether a party has sufficient property interest in intellectual property to be permitted to sue or otherwise claim rights in it—can pose an important obstacle to companies seeking to claim such trade secret rights. Statutory standing is not a frequently litigated question in trade secret law.[326] In the typical fact pattern, there is no question that if the plaintiff establishes that a valid trade secret exists in ordinary competitive business information, it is the owner of that information. In highlighting nontraditional claims, however, the concept of standing is useful to illustrate why such claims stray from the norm.

The DTSA contains an expressly property-centric statutory standing requirement. Only a trade secret "owner" may bring a misappropriation lawsuit.[327] That means those with "legal or equitable title, or license in" the trade secret.[328] The

325. Of course, even gathering publicly available industry data still can result in a threatening lawyer letter. There is no panacea for legal bullying. *See, e.g.*, Kevin Carey, *Risky Strategy by Many Private Colleges Leaves Them Exposed*, N.Y. TIMES (May 26, 2020), https://www.nytimes.com/2020/05/26/upshot/virus-colleges-risky-strategy.html (reporting that when a start-up sought to publish an aggregation of public data to render estimates about the shaky financial status of certain colleges, it had to change plans upon receipt of a legal letter demanding that it "refrain from publication").

326. The standing issues discussed here are distinct from the burst of cases after the DTSA's enactment over its coverage of fact patterns that began before that nonretroactive statute was made law in May 2016. That type of standing question is receding now that the federal statute has been law for several years. *See, e.g.*, Pawelko v. Hasbro, Inc., No. 16-00201-JJM, 2018 WL 6050618, at *6 (D.R.I. Nov. 19, 2018) (granting summary judgment on DTSA claim where plaintiff alleged that defendant had disclosed alleged trade secrets in patent applications years before May 2016, and thus lacked statutory standing); Cave Consulting Grp., Inc. v. Truven Health Analytics Inc., No. 15-cv-02177-SI, 2017 WL 1436044, at *5 (N.D. Cal. Apr. 24, 2017) (same result on motion to dismiss).

327. *See* 18 U.S.C. § 1836(b)(1) (2018); *see also* 18 U.S.C. § 1835 (referring to "Rights of Trade Secret Owners" with respect to motions to seal during litigation).

328. 18 U.S.C. § 1839(4) ("[T]he term 'owner', with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed . . . ."). One important side note: Congress' comments to the statute state, perhaps confusingly, that the DTSA "shall not be construed to be a law pertaining to intellectual property for purposes of any other Act of Congress." *See* Defend Trade Secrets Act, Pub. L. No. 114-153, § 2(g), 130 Stat. 376, 382 (2016). This ungainly language, however, is not a general declaration that trade secret law is based on something other

result is that entities that do not have such rights to the information at issue cannot be parties to federal trade secret misappropriation causes of action.[329]

Under state law, the UTSA generally does not use the "owner" terminology.[330] Instead, standing requirements in UTSA jurisdictions as well as current or former Restatement jurisdictions have developed through court rulings, with a result similar to the DTSA's express terms. That is, owners as well as licensees have standing to bring misappropriation actions.[331] In addition, companies that have sufficient rights of possession also may bring suit.[332] Notably, all the latter cases

---

than an intellectual property theory. Rather, it ensures that Internet content providers can be immune from trade secret claims for content posted by their users under Section 230 of the Communications Decency Act, 47 U.S.C. § 230, which does not provide that safe harbor for "intellectual property" claims. *See* 47 U.S.C. § 230(e)(2); Craft Beer Stellar, LLC v. Glassdoor, Inc., No. CV 18-10510-FDS, 2018 WL 5084837, at *5 (D. Mass Oct. 17, 2018) (explaining interplay between CDA and DTSA and finding website immune from DTSA claim where users posted content that the plaintiff claimed contained its trade secrets).

329. *See* uSens, Inc. v. Shi Chi, No. 18-cv-01959-SVK, 2018 U.S. Dist. LEXIS 175570, at *8–9 (N.D. Cal. Oct. 11, 2018) (denying motion for preliminary injunction in part because plaintiff "has not shown that it is the owner of the alleged trade secrets" and instead submitted confusing evidence about a "related" business).

330. An exception, Nevada, defines "owner" much like the DTSA. *See* NEV. REV. STAT. ANN. § 600A.030.3 (West 2020) ("'Owner' means the person who holds legal or equitable title to a trade secret."). The Restatement (still the law in New York) includes "the value of the information to [the owner] and [its] competitors" as a factor in assessing trade secrecy, but as noted here, Restatement jurisdictions have permitted looser standing conceptions. *See* RESTATEMENT (FIRST) OF TORTS § 757, cmt. b (AM. LAW INST. 1939).

331. *See, e.g.*, Metso Minerals Indus. v. FLSmidth-Excel LLC, 733 F. Supp. 2d 969, 977, 979 (E.D. Wis. 2010) (finding nonexclusive license sufficient to confer standing); Williamson v. Rexam Beverage Can Co., 497 F. Supp. 2d 900, 906–07 (S.D. Ohio 2007) (finding that prior owner lacked standing to bring trade secret claim and that only current assignee could raise the claim); Memry Corp. v. Ky. Oil Tech., N.V., No. C-04-03843 RMW, 2006 WL 3734384, at *7–8 (N.D. Cal. Dec. 18, 2006) (finding that exclusive, irrevocable, royalty-free license conferred sufficient ownership indicia for standing); Funk v. Limelight Media Grp., Inc., No. 1:06CV-72-M, 2006 WL 2983058, at *6–7 (W.D. Ky. Oct. 16, 2006) (finding that shareholders lacked standing to sue company's acquiror for alleged misappropriation of acquired company's information); Callaway Golf Co. v. Dunlop Slazenger Grp. Ams., 318 F. Supp. 2d 205, 211 (D. Del. 2004) (finding that, under California UTSA, plaintiff lacked standing to assert claim over third party's information); Alcatel USA, Inc. v. Cisco Sys., Inc., 239 F. Supp. 2d 645, 659–60 (E.D. Tex. 2002) (finding that plaintiff could not pursue trade secret claim where employee of defendant's predecessor-in-interest, not plaintiff, owned software at issue); Althin CD Med., Inc. v. W. Suburban Kidney Ctr., 874 F. Supp. 837, 842–43 (N.D. Ill. 1994) (finding that trade secret sublicensee lacked standing because only licensor had right to sue under applicable contract); Bus. Trends Analysts v. Freedonia Grp., Inc., 650 F. Supp. 1452, 1458 (S.D.N.Y. 1987) (finding that exclusive licensee had standing to bring trade secret claim); Water Mgmt., Inc. v. Stayanchi, 472 N.E.2d 715, 718 (Ohio 1984) (finding that plaintiff lacked standing where secret belonged to plaintiff's customers).

332. *See* Advanced Fluid Sys., Inc. v. Huber, 958 F.3d 168, 180 (3d Cir. 2020) (finding sufficient possessory interest for statutory standing under Pennsylvania UTSA where plaintiff created technical information for another entity and transferred ownership under a form of invention assignment contract, but also remained in rightful possession of that information to perform services for the owner); DTM Research, LLC v. AT&T Corp., 245 F.3d 327, 331, 333 (4th Cir. 2001) (affirming that mere possession of secret may be enough for standing, even if another might own the same secret, and even if plaintiff possesses the secret under a claim by another that the secret was misappropriated); Cargill, Inc. v. Sears Petroleum & Transp. Corp., 388 F. Supp. 2d 37, 66–67 (N.D.N.Y. 2005) (treating standing as an "unnecessary distraction" and holding that plaintiff "with legitimate, nontransitory possession" could pursue a claim where two "closely aligned corporate affiliates" were plaintiffs and one possessed but did not own the asserted trade secrets). These decisions are questionable because the further one is removed

involved traditional and typical forms of information, used for ordinary marketplace purposes.

Although standing disputes in trade secret law are uncommon, the requirement raises the question of whether companies truly have the ability to assert trade secret rights in many of the categories of information discussed here. Certainly under the DTSA, no company owns or licenses the types of information we have classified as dignitary concerns in Section I.C. And although state law can allow standing for lawful possession, that looser concept still centers on property rights in competitive business information. Simple possession, in the vernacular sense that a company may possess records of employee salaries and injuries, is not the same thing as the possessory business rights seen in the handful of cases permitting such standing. This is especially the case if the employees at issue do not object to disclosure or are themselves the targets of litigation claims over such information.

Similarly, one might ask what property right exists in the fact of an environmental violation or other legal wrongdoing. The fact of an event or occurrence is not necessarily the same thing as the information underlying it. In that sense, the event or occurrence cannot be bought or sold, or licensed, on any commercial market. True, some of the information potentially at issue—say, the chemical formula of a pollutant wrongfully leaked into a nearby waterway—could qualify as a traditional trade secret. But that does not speak to the fact of the wrongdoing itself.

To our knowledge, standing is not a point that has been asserted in disputes over nontraditional information claimed as trade secrets. We propose that it should be, because it may prove to be a powerful deterrent to improper assertions of trade secrecy. Highlighting the standing issue in cases where the party seeking or disclosing information is not a would-be competitor but instead a journalist or a whistleblower may prove especially helpful to demarcate why these contexts are outside the ordinary marketplace competitive context.

2. Revisiting the Economic Value and Reasonable Measures Requirements

Two other basic elements of establishing a trade secret claim over information—that the information have independent economic value to competitors, and that the would-be owner used reasonable security measures to guard it—also could provide significant arguments to overcome the deference too often granted to those seeking seclusion of nontraditional information.

First, every party must establish a type of value to demonstrate that an item of information is a "trade secret" under the DTSA and the UTSA. In the abstract, of course, anything might be said to have "value," even if one can quickly find it on the Internet. But the value element of a trade secrecy claim is something different: it means information that is secret and that would have economic value to

from the original owner, the more difficult it would seemingly be to establish the use of reasonable security measures. In any event, such questions are not pertinent to the questions presented here.

competitors. The requirement of independent economic value resembles the patent requirement for usefulness. But this requirement tends to be a very low threshold, usually satisfied by a "sweat of the brow" showing.[333] The DTSA refers to "economic value."[334] The UTSA does as well.[335] And as discussed above, state criminal trade secret statutes vary, but speak to competitive marketplace information, if not explicitly to "economic value."[336]

Because much of the nontraditional information we discuss above is not material that a business creates for marketplace competition—events of wrongdoing, regulatory violations, or employee attributes—it also lacks that type of economic value. If, for example, there are incidents of racial discrimination at a company, others could use such information when recruiting diverse talent. Thus, a competitor may feel schadenfreude over the legal troubles or media embarrassment of a rival and may even spread such information as a form of marketing, but that is not the same thing as the competitive "economic value" of marketplace information contemplated by the trade secret statutes, which is premised on value driven by trade secrecy, not value in general.

Second, every formulation of trade secret law requires that the claimant demonstrate that it used reasonable security measures to safeguard the claimed trade secret.[337] In a traditional context, this typically means exploring whether the party used nondisclosure agreements when sharing the information with others, or published it without restrictions.[338]

In a nontraditional context, more fundamental questions arise because the party asserting trade secrecy may never have had the ability to suppress disclosure of the information in question. For example, nobody could reasonably argue that an

333. *See* Michael Risch, *Trade Secret Law and Information Development Incentives*, *in* THE LAW AND THEORY OF TRADE SECRECY, *supra* note 11, at 166–67.

334. *See* 18 U.S.C. § 1839(3)(B) (2018) ("[T]he 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. . . .").

335. *See, e.g.*, CAL. CIV. CODE § 3426.1(d)(1) (West 2020) (defining trade secret under California UTSA as information that "[d]erives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use").

336. *See supra* notes 35–37 and accompanying text.

337. *See* 18 U.S.C. § 1839(3)(A) (2018) ("[T]he owner thereof has taken reasonable measures to keep such information secret . . . ."); UNIF. TRADE SECRETS ACT §1(4) (amended 1985), 14 U.L.A. 538 (2005); RESTATEMENT (FIRST) OF TORTS § 757, cmt. b (AM. LAW. INST. 1939) (listing, among other factors, "the extent of measures taken by [the owner] to guard the secrecy of the information").

338. *See, e.g.*, Foster v. Pitney-Bowes Corp., No. 11-7303, 2013 U.S. Dist. LEXIS 17061, at *20–21 (E.D. Pa. Feb. 7, 2013) (granting motion for judgment on the pleadings as to trade secret claim where plaintiff submitted the claimed secret in a patent application, which had been published); Hoffman v. Impact Confections, Inc., 544 F. Supp. 2d 1121, 1126 (S.D. Cal. 2008) (granting summary judgment because plaintiff's voluntary, unprotected disclosure of information negated trade secrecy); Gemisys Corp. v. Phoenix Am., Inc., 186 F.R.D. 551, 557–58 (N.D. Cal. 1999) ("[T]he law is clear that '[i]f an individual discloses his trade secrets to others who are under no obligation to protect the confidentiality of the information . . . his property right [in the information] is extinguished.'" (first and third alteration in original)).

employee does not have the right to disclose his or her ethnicity to whomever she chooses. The same would be true for the facts of workplace injuries, or an employee's salary—indeed, an employee may need to disclose his or her salary to a prospective new employer to negotiate for a higher salary in situations where he or she has bargaining power to do so. As we discussed above, laws permitting employees to freely discuss salaries or workplace safety facts further undermine trade secrecy assertions over such information.[339] Professional biography websites, such as LinkedIn, and social media amplify such disclosures, as do specialized sites like Glassdoor that publish anonymous employee testimonials about workplace conditions.[340]

As such, companies lack control at the most basic level over who discloses such information, when, and to whom. Although this consideration does not apply to every form of information we discuss, it offers a formidable obstacle to trade secrecy assertions in several contexts.

3. Challenging the Ubiquitous "Compilation" or "Combination" Argument

If proponents of broader disclosure of nontraditional information claimed as trade secrets or "confidential" information raise some or all of the arguments above, they are almost certain to encounter this rejoinder: because "compilations" (sometimes called "combinations") can be trade secrets even if their constitutive elements are not, in isolation, trade secrets, a company can still claim a bundled set of nontraditional information as a trade secret. That is, companies can be expected to argue that if they gather together and record diffuse information, such as diversity data or workplace injury data, the resulting collection is a compilation or combination trade secret. For example, in a recent FOIA action over workplace injury data, the government argued against disclosure, in part, on the grounds that "[t]he official forms are more than a list of accidents; the collective data are comprehensive and accurate in a way that workplace rumors, gossip, and innuendo cannot even closely approximate."[341]

This argument should not succeed because it contains a logical fallacy. It is true, and well-established, that a party can hold a valid trade secret in a combination of elements, even where each item contained within the set is not a trade secret on its own, so long as the set represents a "unified process." The intellectual property is the interrelationship formed through the unity of the elements, not

339. *See, e.g.*, CAL. LAB. CODE § 1197.5(k)(1) (West 2020) ("An employer shall not prohibit an employee from disclosing the employee's own wages, discussing the wages of others, [or] inquiring about another employee's wages . . . ."); 29 C.F.R. § 1904.35 (2020) (providing for disclosure of workplace injury information to, and by, employees).

340. *See Search Company Reviews and Ratings*, GLASSDOOR, https://www.glassdoor.com/Reviews/index.htm [https://perma.cc/5JR8-WYYN] (last visited May 11, 2021) ("Search ratings and reviews of over 600,000 companies worldwide. Get the inside scoop and find out what it's really like from people who've actually worked there.").

341. *See* Defendant's Opposition to Cross-Motion for Summary Judgment at 10, Ctr. for Investigative Reporting v. U.S. Dep't of Labor, No. 4:18-cv-02414-DMR (N.D. Cal. June 6, 2020), ECF No. 31.

each element alone.[342] This combination concept can be dangerous even in an ordinary business case, as litigants engage in a gerrymandering of sorts to claim a "combination" that just happens to overlap with some parts of an opponent's otherwise different product or technology.[343]

But the combination concept does not work in some nontraditional scenarios, including those centering on dignitary concerns such as workplace injury reports and company diversity data. If the elements making up the claimed combination are not themselves viable candidates for trade secrecy—because they fall outside the scope of potential trade secrets—the superset formed by aggregating such facts would share the same fundamental defect. A list of facts that are not candidates for trade secrecy because they fall outside the statutory definitions is not the same thing as a combination of elements of business information that, one by one, may be publicly known, but where the unified process among them forms a secret with economic value for marketplace competition.

We can turn again to the concept of employee general knowledge, skills, training, and experience as an analogy. An employer could not sum up the total of points of skill and training an employee gained on the job and then claim the aggregate as a "trade secret" in order to render such information protectable. For example, an employer could not claim that because an employee learned to become proficient in programming certain types of algorithms, and also learned how to offer discounts in customer negotiations, those two unprotectable skills add up to a protectable "combination trade secret." If a category of information is definitionally outside the scope of potential trade secrecy, it does not become intellectual property because a company gathers and compiles it in a document.

4. Pressing for Specific Identification

In civil litigation over trade secret misappropriation claims, disputes about whether the plaintiff has adequately identified each of its claimed trade secrets are common—even routine. As a federal court in Louisiana recently noted, there is now a "legion of cases joining th[e] consensus" that the plaintiff must provide at least a reasonably particular identification before it can first undertake discovery.[344] Thus, "'catchall' descriptions, a 'list[] [of] categories of alleged

342. For an exploration of this concept with nationwide citations, see Tait Graves & Alexander Macgillivray, *Combination Trade Secrets and the Logic of Intellectual Property*, 20 SANTA CLARA COMPUTER & HIGH TECH. L.J. 261 (2004).

343. In perhaps the best-known illustration, a party claimed a trade secret in a five-element combination, but then learned during discovery that the defendant had not actually received all five elements from the plaintiff. So the plaintiff had its expert witness assert instead a four-element combination trade secret claim in an effort to avoid summary judgment. The court rejected this shape-shifting effort. *See* Am. Airlines, Inc. v. KLM Royal Dutch Airlines, Inc., 114 F.3d 108, 110–12 (8th Cir. 1997) (affirming rejection of "sham" claim "manufactured" to try to match the defendant's own work).

344. *See* JJ Plank Co., LLC v. Bowman, No. 3:18-CV-00798, 2018 U.S. Dist. LEXIS 123792, at *7 (W.D. La. July 23, 2018) (collecting cases); *see also* Coda Dev. S.R.O. v. Goodyear Tire & Rubber Co., No. 5:15-cv-1572, 2019 U.S. Dist. LEXIS 202114, at *11 (N.D. Ohio Nov. 21, 2019) ("[G]iven the nature of and burdens imposed by trade secret cases, many courts across the country recognize the

trade secrets in broad terms,' or 'a listing of concepts that [the plaintiff] asserts constitute its trade secret information'" tend to be insufficient.[345]

Pushing a company asserting trade secret rights in nontraditional information to specifically define what, in precise terms, it claims to be a trade secret on an item-by-item basis could go a long way in defeating such assertions. The concerns expressed by courts in ordinary civil litigation about overbroad claim descriptions are even stronger when a party seeks to claim trade secret rights in nontraditional information that may not—for the reasons set forth above—constitute a type of information appropriate for trade secret coverage in the first place. To parse out such facts and expose such claims, it is important to prevent claimants from overdesignating by asserting entire documents, entire files, and the like as "trade secrets." Forcing specificity may better reveal improper attempts to protect nontraditional information.

Indeed, there is at least some evidence that courts, legislators, and commentators are recognizing the value of pressing for specific identification of trade secrecy. Case law now requires parties to describe, define, and identify, with increased particularity, the trade secrets in question, rather than offer a blanket assertion of confidentiality even before the expert discovery process has commenced.[346] Legislatively, California's version of the UTSA requires trade secret plaintiffs to provide a reasonably particular identification of alleged secrets prior to pursuing discovery and also provides remedies for bad faith trade secret claims.[347] Courts in several states—Delaware, Illinois, Massachusetts, Minnesota, and Florida—have adopted similar requirements, and there is also a similar requirement in the DTSA.[348] Both of us, in prior work, have set forth recommendations that force the plaintiff to be specific in identifying alleged secrets, including directing courts to be wary of highlevel, general lists of trade secrets.[349]

'growing consensus' in favor of 'requiring those plaintiffs bringing claims of trade secret misappropriation to identify, with reasonable particularity, the alleged trade secrets at issue.'").

345. *See* M/A-COM Tech. Sols., Inc. v. Litrinium, Inc., No. SA CV 19-00220-JVS (JDEx), 2019 WL 4284523, at *2 (C.D. Cal. June 11, 2019) (construing the California pre-discovery identification requirement).

346. *See, e.g.*, Synygy, Inc. v. ZS Assocs., Inc., No. 07-3536, 2015 WL 899408, at *6–9 (E.D. Pa. Mar. 3, 2015) (requiring further definition of the scope of a trade secret during discovery); *see also* Michael P. Broadhurst & Ann E. Querns, *Define Trade Secrets Before and During Litigation*, LAW.COM (May 12, 2015, 10:35 AM), https://www.law.com/sites/articles/2015/05/12/define-trade-secrets-before-and-during-litigation ("A series of decisions in *Synygy v. ZS Associates* . . . highlight the critical importance of defining an enterprise's trade secret information . . . ." (citation omitted)).

347. *See* CAL. CIV. CODE § 2019.210 (West 2020) (requiring "reasonable particularity"); Charles Tait Graves & Brian D. Range, *Identification of Trade Secret Claims in Litigation: Solutions for a Ubiquitous Dispute*, 5 NW. J. TECH. & INTELL. PROP. 68, 71, 76, 83 (2006). Massachusetts has also adopted a similar statute. *See* MASS. GEN. LAWS ch. 93, § 42D(b) (West 2020) ("In an action . . . alleging trade secrets misappropriation a party must state with reasonable particularity the circumstances thereof, including the nature of the trade secrets and the basis for their protection.").

348. *See* Graves & Range, *supra* note 347, at 82 (collecting examples).

349. *See, e.g.*, *id.* at 91–96; *see also* Katyal, *supra* note 40, at 1269–70.

5. Challenging "Confidential" Information Claims Under FOIA

As we discussed above, the 2019 *Argus Leader* decision seemingly makes it easier for companies to use the FOIA exemption for "confidential" information to block disclosure of information submitted to government agencies.[350] This raises the question of what flaws exist in such expansive arguments, even under the new *Argus Leader* formulation.[351]

We believe that such overbroad confidentiality claims remain vulnerable even under *Argus Leader*. To begin with, one might ask what constitutes "commercial or financial" information—a precondition for asserting that the information is "confidential" for the FOIA exemption.[352] Is a simple connection to a workplace sufficient?[353] Surely not, or the definition would be almost meaningless—offices, computers, and company-issued phones contain entirely personal information carried in or stored by employees. Any company could block almost any FOIA request for information it has submitted to a government agency, and the exemption thereby would swallow the statutory goals of disclosure. The words "commercial" and "financial" should be read like the terms of the DTSA and UTSA—to focus on information pertinent to marketplace competition, and not merely information about employees or about acts or events of wrongdoing or harm that happen to occur at a worksite, in order to place meaningful boundaries around what can be protected.

Second, we question whether companies have an ownership stake in nontraditional categories of information such as attributes of employees or events of wrongdoing. The *Argus Leader* formulation refers to a concept of ownership: "[a]t least where commercial or financial information is both customarily and actually treated as private by its owner."[354] As with the discussion of standing

350. *See* Food Mktg. Inst. v. Argus Leader Media, 139 S. Ct. 2356, 2366 (2019).

351. As Varadarajan has noted, *Argus Leader* was based on facts that pre-dated the FOIA Improvement Act of 2016 with its foreseeable harm requirement, and its reach therefore may prove to be limited. *See* Varadarajan, *supra* note 11, at 5. Varadarajan also proposes several potential constraints on overbroad FOIA confidentiality assertions in the wake of *Argus Leader*, including inserting better pro-disclosure terms into government contracts and enacting statutory safe harbors, such as for whistleblowers. *See id.* at 44.

352. *See* 5 U.S.C. § 552(b)(4) (2018).

353. Some FOIA cases provide for broad definitions of "commercial and financial." *See, e.g.*, Flightsafety Servs. Corp. v. U.S. Dep't of Labor, 326 F.3d 607, 611 (5th Cir. 2003) (affirming finding in FOIA dispute that wage information submitted to the Bureau of Labor Statistics on promise of confidentiality was "commercial" and "confidential," albeit without analysis as to the former); Am. Airlines v. Nat'l Mediation Bd., 588 F.2d 863, 870 (2d Cir. 1978) (finding "commercial" to have broad meaning, but in somewhat question-begging language: "'Commercial' surely means pertaining or relating to or dealing with commerce. Labor unions, and their representation of employees, quite obviously pertain to or are related to commerce and deal with the commercial life of the country"). That said, employee-related information does not always fit within that term. *See* Getman v. NLRB, 450 F.2d 670, 673 (D.C. Cir. 1971) (finding that information was not "commercial" where law professors sought names and contact information of employees to survey them about campaign methods during union elections). Notably, none of the litigants in such cases appears to have presented in-depth arguments about the degree to which information simply present in a workplace, but not tied to market competition, qualifies.

354. *Argus Leader Media*, 139 S. Ct. at 2366.

above, at least some types of nontraditional information claimed as trade secrets do not comprise a company's property or information that can be owned or licensed in the marketplace sense.

Finally, something akin to the reasonable security measures requirement of civil trade secret law can also be deployed in the FOIA context. That is, at least some of the information that a company seeks to exempt from disclosure is not "customarily treated as confidential or private." This question seems open to a reasonable security measures analysis, as under the DTSA and UTSA. If the company itself has not been consistent in its practices, or if the nature of the information is such that employees can openly disclose it because it relates to facts about their own attributes, establishing customary treatment would seem questionable. And when statutes or regulations allow employees to disclose the information at issue, such "custom" would seem even weaker. An example might be recent state statutes, discussed above, allowing employees to disclose and discuss their salaries.

C. LIMITING TRADE SECRECY

The points discussed above underscore that not every claim to trade secrecy should be taken as such; many types of nontraditional information fall outside the scope of trade secret law altogether. That said, some of the information we discuss does in fact fall within traditional categories of trade secret protection: software code (for example, as used in technologies used by the prosecution in a criminal case, or as used by local governments), chemical formulae (as may be reflected in environmentally polluting industrial wastes), or software and hardware product designs (where companies try to prevent a "right to repair" by consumers). But even where nontraditional trade secret claims concern types of information that comprise typical candidates for trade secret protection, this should not be the end of the analysis.

Trade secret protection should not be viewed as a monolith where the skimpiest satisfaction of the elements of trade secrecy means that regulatory or other disclosure in the public interest is impossible. There are contexts where the public interest in disclosure is strong, and the case for competitive harm is weak. The challenge is to articulate simple and flexible tests courts can employ to protect trade secrets where harms are real but also to separate instances where disclosure is appropriate. We begin with doctrinal limits to trade secret overreach, and we then explore potential legislative solutions.

1. Overarching Defenses and Limits on Trade Secrecy Assertions

In addition to context-specific proposals, scholars have recently advanced new theories of more general application to restrain overreaching trade secrecy assertions. We believe that these proposals offer promising theories for a broad, overarching limiting doctrine to trade secret law because they are not situationally specific, are broad enough to capture many different concepts, and have recognized antecedents in other, more developed categories of intellectual property law.

Before reaching these proposals, however, some might ask if the trade secret statutes already provide an express solution—and one that is broad and thus flexible for different contexts. That potential solution is the statutory penalty for asserting trade secret claims in "bad faith" in the DTSA and in most state UTSA enactments—the case where plaintiffs improperly claim trade secret rights, or make trade secret assertions, for ulterior purposes such as preventing a former employee from competing.[355] Does the existence of a penalty for bringing an improper lawsuit suffice to provide a generalizable hook to deter and block improper trade secrecy assertions over nontraditional subject matter?

Although it is possible that the "bad faith" penalty could be effective in some instances where nontraditional claims are asserted—after all, courts *do* examine the plaintiff's subjective motive in wrongfully filing or maintaining a trade secret lawsuit[356]—the answer is likely "no." Bad faith applies in civil lawsuits brought by a plaintiff and may not be extensible to other contexts. In addition, bad faith is akin to a remedy, not a defense. A defendant in a civil misappropriation lawsuit can obtain recovery only upon or after prevailing on the merits—that is the nature of statutory attorneys' fees awards.[357] Because the likelihood of any given trade secret case reaching that endpoint is low and because the defendant must marshal evidence of the plaintiff's objective and subjective wrongful litigation conduct, such awards are relatively rare. They are not a firm deterrent. Thus, although bad faith is not out of the question where a defendant has prevailed and the plaintiff improperly claimed trade secret rights in nontraditional information, trade secret law needs more specific tools to challenge such assertions earlier in disputes, and in disputes that do not involve misappropriation lawsuits.

One such possibility—and the subject of a proposal by Deepa Varadarajan—is to develop a theory of trade secret fair use.[358] Varadarajan has noted that "[u]nlike copyright and patent laws, trade secret law lacks limiting doctrines sufficiently

355. *See, e.g.*, 18 U.S.C. § 1836(b)(3)(D) (2018) (providing for attorneys' fees "if a claim of . . . misappropriation is made in bad faith"); CAL. CIV. CODE § 3426.4 (West 2020) (same).

356. Many courts apply a two-step objective and subjective approach to assess bad faith. For cases examining the plaintiff's improper motives and finding bad faith under the California UTSA, see Cypress Semiconductor Corp. v. Maxim Integrated Prods., Inc., 236 Cal. App. 4th 243, 268–71, 186 Cal. Rptr. 3d 486, 507–10 (2015) (finding bad faith where former employer acted to stop rival from hiring its employees); SASCO v. Rosendin Elec., Inc., 207 Cal. App. 4th 837, 846–48, 143 Cal. Rptr. 3d 828, 835–36 (2012) (same); and FLIR Sys., Inc. v. Parrish, 174 Cal. App. 4th 1270, 1282–85, 95 Cal. Rptr. 3d 307, 318–21 (2009) (finding bad faith where former employer acted to stop rival from hiring its employee and demanded illegal terms to settle the lawsuit, including prohibitions on hiring the plaintiff's employees and on contesting the validity of its patent applications).

357. A jury can decide the fact question of bad faith, but the calculation of any fees award is reserved for the court. *See* GSI Tech., Inc. v. United Memories, Inc., No. 5:13-cv-01081-PSG, 2015 U.S. Dist. LEXIS 140085, *4, *6–8, *21 (N.D. Cal. Oct. 14, 2015) (denying pretrial motions to block presentation of various fact issues on claim of bad faith by defendants, but granting motion to block evidence of attorneys' fees issues before the jury).

358. *See* Deepa Varadarajan, *Trade Secret Fair Use*, 83 FORDHAM L. REV. 1401, 1401 (2014) ("[C]ompanies increasingly use trade secret law to block a wide swath of information from the scrutinizing eyes of consumers, public watchdog groups, and potential improvers.").

attuned to a defendant's follow-on improvements . . . ."[359] Pointing to hypotheticals—such as a whistleblower who discloses "secret formula" for a toxic chemical "that can leak into the water supply and significantly affect public health"; a company that "aggregates and discloses prices paid by hospitals for medical devices, information that is deemed proprietary by the device manufacturer but has implications for national health care costs"; or a former employee "who makes significant improvements to trade secret-protected information gleaned from her previous workplace"—she considers doctrines that limit other areas of intellectual property law, such as the reverse doctrine of equivalents and the experimental use defense for academics in patent law, and the fair use defense in copyright law.[360] Varadarajan then proposes a five-factor analysis for "trade secret fair use," which would examine: (1) the purpose of the infringing use; (2) the nature of the trade secret; (3) the substantiality of the trade secret relative to the defendant's improvements to it; (4) the effect of use on the trade secret owner; and (5) appropriateness of a reasonable royalty.[361] This concept may fit best with disputes over the "right to repair" and other situations where a company tries to control downstream maintenance and other aspects of its products.[362]

Separately, and as noted above in our rubric of anticompetitive concerns, Varadarajan has also proposed a defense of trade secret misuse—one more akin to copyright misuse than patent misuse.[363] In addition to protecting against overbroad licensing terms, it would combat "abusive overclaiming of trade secret scope."[364] Thus, the defense could be raised where overbroad assertions of trade secrecy are raised against a departing employee, and penalties could include "the unenforceability of the IP right for a period of time, and a lesser penalty, such as not enforcing a particular contract provision."[365] This concept is promising, but may overlap substantially with the existing "bad faith" penalty, at least in the civil misappropriation context.

A broad and generalizable principle to limit the reach of trade secret law is a flexible concept of thin trade secrecy (or thin "confidentiality"). Again borrowing from copyright law, this would be a concept that courts or regulatory bodies in all manner of disputes could apply.[366] Under this approach, courts could recognize that some trade secrecy assertions are weaker than others and that in some cases

359. *Id*. at 1404.

360. *Id*. at 1404, 1423–25, 1427–30.

361. *See id*. at 1447–52.

362. *See* Adrian Potoroaca, *Apple Will Expand Access to Genuine iPhone Parts for Independent Repair Shops in the US*, TECHSPOT (Aug. 29, 2019 1:10 PM), https://www.techspot.com/news/81668-apple-expand-access-genuine-iphone-parts-independent-repair.html [https://perma.cc/MJ2E-FUEL] (noting Apple's resistance to allowing independent shops to repair Apple products and to right-to-repair legislation).

363. *See* Deepa Varadarajan, *The Uses of IP Misuse*, 68 EMORY L.J. 739, 744 (2019) (setting up the proposal by noting that "trade secret boundaries are highly uncertain, making it easier for trade secret owners to misrepresent the scope of their rights, particularly to legally unsophisticated audiences").

364. *Id*. at 787–89.

365. *Id*. at 797–98.

366. *See* Feldman & Graves, *supra* note 50, at 116 ("The logic of thin copyright reflects the concern that copyright [law] might be used to reach beyond its boundaries—extending its grasp to subject matter

there are strong public policy interests in disclosure even if borderline trade secrecy has been established.[367] This concept also has the advantage of emphasizing those trade secret claims that are weak, and thus operates at the symbolic level against any assumption that establishing trade secrecy provides an insurmountable bulwark.[368]

2. Situationally Specific Solutions

Some potential means to limit attempts at corporate seclusion are context-specific. Indeed, in some highly specific cases, situational fixes may solve the problem—as in criminal law, where ending a privilege for the prosecution to withhold evidence from the defense on trade secret grounds, and thereby following the routine exchange of evidence which is ubiquitous in civil misappropriation lawsuits under protective orders, would be a seemingly complete solution to that particular issue.[369] In the case of diversity data, Jamillah Bowman Williams proposes policies ranging from encouraging companies to voluntarily disclose such data to mandatory disclosure akin to a United Kingdom regulatory enactment from 2017, which "require[s] all employers with 250 or more employees to publish aggregate pay data by sex on their websites and to make these data publicly available for at least three years."[370] And in the case of pharmaceutical clinical trial data submitted to the FDA and treated as secret, a recent proposal calls for "proactive disclosure of safety and efficacy data" by the FDA in a change of current administrative practices.[371]

As to government entities claiming trade secret rights to block information disclosure requests, David Levine has proposed disallowing trade secret protection or FOIA exemptions as well as requiring these entities to show that they act as market competitors in the private sector.[372] In the narrower case of algorithms used by government actors in decisionmaking, Robert Brauneis and Ellen P. Goodman describe their efforts in seeking such information through records

that should not be restricted to the public and blocking activity outside of the creative appropriation that copyright was intended to prevent.").

367. *See id.* at 119–23 ("Thin trade secret would exist when the independent economic value or creation aspect of the secret is scant, such that the item of information qualifies for protection, but only just so. . . . [The] information would exist near the margins of trade secret protection. . . . In that case, the tug of a countervailing public policy interest would have particular force.").

368. As Sharon Sandeen observed during the July 2020 Trade Secrets Scholars Workshop, in civil trade secret lawsuit where courts consider a plaintiff's request for injunctive relief, courts theoretically should consider the public interest. *See, e.g.*, Winter v. Nat. Res. Def. Council, 555 U.S. 7, 20 (2008) ("A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest."). This could provide a ready means for courts to consider the issues discussed here at least where equitable relief is sought.

369. *See* Wexler, *supra* note 8, at 1429 ("This Article has made the case against recognizing a trade secret privilege in criminal cases.").

370. Williams, *supra* note 8, at 1728 (footnote omitted); *see id.* at 1723 (favoring "treating diversity data and strategies as public resources rather than safeguarding them as trade secrets").

371. *See* Morten & Kapczynski, *supra* note 46, at 6, 19–22 (discussing EU and Canadian approaches to "a proactive disclosure policy").

372. *See* Levine, *supra* note 42, at 107, 110–14.

requests and trade secrecy assertions.[373] In a nuanced proposal for disclosure, they explain that obtaining information necessary to understand such decision-making may not require disclosure of actual algorithms—which itself may not result in "understand[ing] the results of an algorithmic process."[374] Their model focuses first on contracts between private contractors and governments that use their technology, and would place a greater burden on the contractor to designate portions of documents as trade secrets to avoid blanket trade secrecy assertions. It would also call upon government agencies to push for ownership or disclosure-promoting license terms.[375] They then focus on the types of documentation that governments might create and disclose in an eight-point model including articulation of goals of using a predictive algorithm, data used or excluded, predictive criteria, and audits and validation studies.[376]

When it comes to FOIA requests more generally, commentators differ about the most appropriate way to provide a limiting principle that courts can apply. *Argus Leader*, of course, makes this prospect more difficult. One commentator has called for a case-by-case application of a "precautionary principle" to evaluate such assertions against public health and safety concerns.[377] This proposal envisions a general balancing test broad enough to cover a wide variety of contexts, but perhaps insufficiently specific to provide meaningful guidance. By contrast, another commentator rejects a "case-by-case balancing approach" to environmental and health risk information because of the "asymmetries between the organizational, financial, and information resources of the two sides" in disputes over access to regulatory disclosures.[378] This proposal favors a narrow and

373. *See* Brauneis & Goodman, *supra* note 195, at 133–52, 153–59 (describing, at length, attempts to obtain information in the face of "aggressive trade secre[cy] and confidentiality claims" (capitalization omitted)).

374. *See id.* at 131. Others have made similar observations. *See, e.g.*, Katyal, *supra* note 40, at 1250–51 ("Many systems have also not been designed with oversight and accountability in mind and, thus, can be opaque to [an] outside investigator. . . . Further, even if source code disclosure reveals some elements of a decision reached through automated processing, it cannot be fully evaluated without an accompanying investigation of the training data. . . ." (footnotes omitted)); Levine, *supra* note 148, at 40–41 ("Public access to an algorithm's source code does not guarantee that the public will have the resources and knowledge needed in order to understand it, scrutinize it, or even care. . . . Therefore, it has been suggested that transparency is required at multiple dimensions of algorithmic decision-making." (footnotes omitted)).

375. *See* Brauneis & Goodman, *supra* note 195 at 164–65.

376. *See id.* at 168–75.

377. *See* Zink, *supra* note 78, at 1177 ("This determination can and should involve third-party analysis, so as to avoid corrupted science.").

378. *See* Lyndon, *supra* note 7, at 482, 523; *see also* Mary L. Lyndon, *Secrecy and Innovation in Tort Law and Regulation*, 23 N.M. L. REV. 1, 51–52 (1993) (focusing on environmental issues, including chemical "exposure" incidents where approaches could include "dispens[ing] with any secrecy protection in the exposure context," requiring "an arbitration on value and terms of use" among firms "[w]hen there is a request for disclosure of exposure or health and safety information," or a "mini-patent or registration system," like the registration system described in the Lydon article cited *supra*); Lyndon, *supra* note 53, at 464 ("A clear disclosure imperative would present firms with a choice among (1) avoiding exposures, (2) patenting or other appropriability strategies and (3) investing in research to prove safety or compliance with a regulatory standard.").

time-limited "registration system" for "[t]ime-limited entitlements" where registrants can seek a "period of automatic exclusive use" but be subject to rivals' challenges.[379] Another proposal favors a different form of substantive change, in recognizing a new property right held by the public in certain forms of regulatory disclosures.[380]

These proposals lead to the question of whether legislative solutions may be ideal, because enactments can target specific problems and avoid the uncertainties and costs of the litigation approaches discussed above.

IV. PROPOSALS FOR LEGISLATIVE SOLUTIONS

There are tradeoffs when proposing legislative solutions to nontraditional trade secret claims. On one hand, legislative enactments are stronger than court-created doctrines. In whatever jurisdiction they are enacted, they are usually the final word. Perhaps most important, statutes create norms for conduct, and thus can deter behavior before lawsuits or other disputes arise. To take an example from the law of employee mobility—an area adjacent to trade secret law with claims over both frequently brought in lawsuits against departing employees—California prohibits noncompetition covenants in employment agreements.[381] This means employees do not have to worry about merely seeking work with a competitor (or forming a new business themselves) because there is no threat of litigation over that issue. It is likely that countless attorneys in California have had to explain to angry executives that there is no ugly letter to be sent, and no lawsuit to be filed, just because a rival offered a talented employee a better salary. Massachusetts may see similar results with its new limitations on such covenants, which in most instances now require the former employer to pay the employee in order to enforce it.[382]

On the other hand, there are drawbacks to efforts at legislative reform. Sometimes diluted legislation ends up legitimizing practices that were supposed to be reformed. To stick with our example of restraints on employee mobility, Utah purported to modify its noncompetition covenant rules in 2016, only to enact a statute that permits such covenants for one year, and that allows nonsolicitation covenants to last longer.[383] Rather than reform, this effort essentially ratified the common one-year noncompetition covenant—probably the most common time period companies use in such restrictions—thus accomplishing next to nothing in improving worker mobility in that state. As another example from the recent wave of noncompete legislation, the Oregon legislature can point

379. *See* Lyndon, *supra* note 7, at 523–24.

380. *See* D. Victoria Baranetsky, *The New New Property: Corporate Secrecy and Access to Public Records* (forthcoming) (on file with author) (with respect to FOIA actions, proposing recognition of a property right to government records based on "a reasonable expectation to [the] receipt" of such records).

381. *See* CAL. BUS. & PROF. CODE § 16600 (West 2020).

382. *See* MASS. GEN. LAWS ch. 149, § 24L(b)(vii), (c) (West 2020).

383. *See* Post-Employment Restriction Act, 2016 Utah Laws ch. 153, § 3 (codified as amended at UTAH CODE ANN. § 34-51-201 (West 2020)).

to a partial achievement in restricting noncompetition covenants for low-salary employees except where the employer pays the employee a partial salary during the noncompete period, but this enactment, again, implicitly ratifies the use of noncompetition covenants against others.[384]

To take another example where legislation may not operate as anticipated, our discussion of the whistleblower protection clause in the DTSA noted how some litigants in state court bring claims under contract or tort law—but not trade secret law—in an apparent effort to plead around the DTSA's immunity for "trade secret" claims.[385] This demonstrates how parties will examine statutory language closely and come up with creative ways to try to evade it.

In addition, some proposed legislation simply stalls. For example, so-called "right to repair" bills—statutes that would permit consumers to engage in self-repair of products such as farm tractors without facing potential trade secret, contract, or copyright claims brought by manufacturers—have thus far failed in Congress and in several states.[386] Only one state, Massachusetts, has succeeded in enacting such a statute. That 2013 statute requires certain types of manufacturers to provide the same diagnostic information to independent repair shops and owners, for a reasonable price,[387] and was recently expanded by referendum just this year.[388] Part of the problem is that manufacturers deem information enabling repair to constitute a trade secret, and this creates difficulties in enacting consumer-friendly right-to-repair statutes. In short, attempts at reform can prove suboptimal, especially where there is significant opposition and corporate lobbying while a bill is being drafted.

Finally, and perhaps most significantly, any legislative enactment only affects its jurisdiction. Because the federal DTSA does not preempt state trade secret law[389] and because the states also have their own versions of open-records laws, employee mobility laws, and the like, any victory is a local triumph.

---

384. *See* OR. REV. STAT. ANN. § 653.295(1)–(2) (West 2020) (limiting noncompetition agreements to eighteen months).

385. *See supra* notes 135–38 and accompanying text.

386. *See* H.R. 1449, 112th Cong. (2011) ("To protect the rights of consumers to diagnose, service, maintain, and repair their motor vehicles . . . ."); H.B. 3030, 100th Gen. Assemb., Reg. Sess. (Ill. 2017); H.B. 556, 87th Gen. Assemb., Reg. Sess. (Iowa 2017); L.B. 67, 106th Leg., Reg. Sess. (Neb. 2017); S.B. S618C, 202d Sess. (N.Y. 2017); S.B. 888 § 5, 110th Gen. Assemb., Reg. Sess. (Tenn. 2017); H.B. 2279, 65th Leg., Reg. Sess. (Wash. 2017); H.B. 0199, 65th Leg., Reg. Sess. (Wyo. 2017). For a thorough study of the problem, see Leah Chan Grinvald & Ofer Tur-Sinai, *Intellectual Property Law and the Right to Repair*, 88 FORDHAM L. REV. 63, 66–67 (2019) (proposing right to repair theory congruent with justifications for intellectual property law).

387. *See* MASS. GEN. LAW. ANN. ch. 93K, § 2(a) (West 2020) ("All content in any such manufacturer's repair information system shall be made available to owners and to independent repair facilities in the same form and manner and to the same extent as is made available to dealers utilizing such diagnostic and repair information system. Each manufacturer shall provide access to such manufacturer's diagnostic and repair information system for purchase by owners and independent repair facilities on a daily, monthly and yearly subscription basis and upon fair and reasonable terms.").

388. *See* Adi Robertson, *Massachusetts Passes 'Right to Repair' Law to Open up Car Data*, VERGE (Nov. 4, 2020, 12:44 PM), https://www.theverge.com/2020/11/4/21549129/massachusetts-right-to-repair-question-1-wireless-car-data-passes [https://perma.cc/WSY3-2HUS].

389. *See* 18 U.S.C. § 1838 (2018).

Still, legislative enactments are possible even recognizing these limitations. As noted above, many states acted to change corporate nondisclosure practices regarding sexual harassment following the #MeToo movement.[390] The DTSA's whistleblower protection clause—something not seen in prior state trade secret enactments—was inspired by an academic proposal, and represents a real achievement even as companies try to find ways around it.[391] Another example we discussed above is the recent wave of state statutes that now protect employees' rights to discuss and to inquire about salary information.[392]

A. A BROAD, MULTIPURPOSE ENACTMENT

We can imagine two paths for statutory reform. One would recognize a broader limiting concept for trade secrecy (or confidentiality) assertions in federal or state trade secret and open-records laws. Like the concepts of trade secret fair use and thin trade secrecy discussed above, a simple clause could direct courts to weigh public-interest concerns when a claim of trade secrecy is weaker, and the risk of competitive harm is slight. One solution is to have a simple balancing test: that if the court determines that access to the trade secret is relevant and necessary, then an appropriate safeguard can be a protective order or release of the information to the public.[393] To be sure, balancing tests are risky: powerful interests can push for their desired outcomes without precise rules. But at present, trade secret law does not generally call for an examination of public interests, and thus, providing courts with that option grants permission to do so.

For any version of a trade secret statute or an open-records statute, a legislature could enact such a balancing test. Courts might be directed to consider: (1) the nature of the information at issue and the proximity of its use to marketplace competition; (2) the strength of the assertion of trade secrecy (or confidentiality) versus proximity to ready ascertainability or time-limited value for marketplace competition; (3) the nature and degree of the disclosure sought; (4) the public interest at stake, such as whether a regulatory goal is involved; and (5) tailoring and means of disclosure—for example, redaction or aggregation, or a protective order versus full disclosure. The whistleblower provision of the DTSA, discussed above, may offer a model means of restricted disclosure to, for example, a party's attorneys or government investigators in some cases. In other cases, aggregated or redacted disclosures may best balance competing interests where information comprises a valid trade secret.

To be sure, there are important drawbacks to proposing such legislation. We expect fierce lobbying might dilute or eliminate a bill during its time in committees, and the final product could be substantially weakened. At the same time,

390. *See supra* notes 301–05 and accompanying text.

391. *See* Menell, *supra* note 8, at 2 ("Based on an earlier draft of this Article, Congress adopted a whistleblower immunity provision as part of the Defend Trade Secrets Act of 2016.").

392. *See supra* note 263 and accompanying text.

393. *See, e.g.*, M-I LLC v. Stelly, 733 F. Supp. 2d 759, 802 (S.D. Tex. 2010) (applying balancing test).

however, a general clause of this type is broad enough to be useful for a multiplicity of problems including those that are still unknown today but will almost certainly arise in the years to come. And unlike issue-specific legislation, this type of clause would directly amend trade secret or open-records statutes, leaving no potential gaps between them.

B. NARROWER, ISSUE-SPECIFIC ENACTMENTS

In the alternative, we can also envision state-level and regulatory changes to address one-off but important exceptions to potential trade secret coverage. The strongest would either mandate disclosure of certain data—where disclosure might incentivize better workplace conditions or stronger diversity efforts—or explicitly permit the sharing and disclosure of such data. The effect would be to prevent trade secrecy claims to block such disclosure, whether through civil litigation or open-records litigation. Indeed, such context-specific enactments may benefit from a sense of urgency as issues hit the news and when momentum for change is strong.

We have discussed several examples—both successful and unsuccessful. These include the new laws that some thirteen states have enacted to provide greater workplace transparency over sexual harassment disputes, state statutes that permit employees to share salary information, and the uncertain future of proposed statutes to address right-to-repair concerns.

We can envision other, similar transparency statutes aimed at discrete problems, such as workplace injury data, workplace diversity data, technologies used by the prosecution in criminal cases, and transparency in technologies used in government decisionmaking. Each may differ as to precisely what information is to be disclosed, to whom, and in what form. And there is no reason to expect that disclosure only means a one-way disclosure to the public, especially considering that a broad range of protective orders can be obtained to protect the trade secret's confidentiality and yet still enable investigators to pursue their work. Although state statutes provide only local coverage, they may prove easier to enact than federal legislation, and a pattern of similar enactments could together cover large portions of the population.

CONCLUSION

We have identified several areas of law where would-be trade secret owners are pushing the boundaries of laws designed to protect certain commercial, marketplace information, not to protect business reputations or forestall investigations of wrongdoing. Because claimants can assert trade secrecy in misappropriation lawsuits and confidentiality in open-records disputes with ease, we anticipate that the problems we discuss here may worsen in the years to come. Those working in disparate areas of legal scholarship and practice need solutions that are generalizable to new situations as they arise, in order to speak with a common voice about problems that share common elements. We offer practical paths toward reform in the service of a more balanced approach to trade secret law that takes better account of the many public interests at stake.