ARTICLE

PUBLICIZING CORPORATE SECRETS

CHRISTOPHER J. MORTEN†

INTRODUCTION ........................................................................................................ 1320
I. A DANGEROUS STATUS QUO ............................................................................ 1332
   A. Sweeping Access: Federal Regulators’ Information-Gathering
      Powers .............................................................................................................. 1333
         1. Premarket Approval .............................................................................. 1336
         2. Investigation ....................................................................................... 1338
   B. Locked Vaults: Federal Regulators Keeping Corporate Secrets of
      Public Interest .............................................................................................. 1340
      1. Regulators’ Scattered Proactive Disclosure Programs ..................... 1340
      2. Regulators Tending Toward Secrecy .................................................... 1343
   C. The Public Has No Good Alternatives ...................................................... 1347
      1. FOIA Is Broken ...................................................................................... 1347
      2. The Public Lacks Other Good Tools ..................................................... 1349
II. THE WHY AND HOW OF PUBLICIZING CORPORATE SECRETS .  1352

† Associate Clinical Professor of Law, Columbia Law School. For helpful input, I thank Victoria Baranetsky, Doni Bloomfield, Courtney Cox, Gabrielle Daley, Rochelle Dreyfuss, Megan Graham, Charles Tait Graves, Gautam Hans, Matthew Herder, Camilla Hrdy, Amy Kapeczynski, Amanda Levendowski, David Levine, Clarisa Long, Varoon Mathur, Gabriel Nicholas, Riana Pfefferkorn, David Pozen, Blake Reid, Ira Rubinstein, Sharon Sandeen, Jason Schultz, Nina Srejovic, Kathy Strandburg, Jacob Victor, Salome Viljoen, Michael Weinberg, and commentators at the Works-in-Progress Intellectual Property (WIPIP) Colloquium, Junior Tech Law Scholars Group, NYU Tri-State Region IP Workshop, and Mitchell Hamline School of Law Trade Secret Workshop. I thank Zartosht Ahlers, Xingni (Cindy) Chen, Navya Dasari, Emma Li, Stephanie Lim, Andrew Nassar, Elaina (Ransford) Marx, Kara Smith, and Julia Zhu for invaluable research assistance over the several-year gestation of this article. I also thank the editors of the University of Pennsylvania Law Review, including Alex Geisel, Kristen Marino, Luke McCartney, Phillip Moore, Hugh Murchie and Chayla Sherrod, for their excellent work. Research for this article was made possible in part by The Honorable Bertram Harnett Faculty Research Fund at Columbia Law School.
INTRODUCTION

Let’s begin with two short stories of secrets held by federal regulatory agencies. In each, a regulator obtains and holds secret technical information about a product sold by a company it regulates. The secret information concerns the product’s safety and also contains some kernel of proprietary, commercially valuable knowledge. Each regulator thus faces a dilemma. On the one hand, the regulator wants to protect the regulated entity’s legitimate interest in keeping commercially valuable secrets secret. On the other hand, the regulator wants to inform the American public of a threat to its safety. To disclose the secret risks angering its source, undermining incentives across the broader industry, and, perhaps, triggering legal liability for violating trade secrecy law. To keep the secret risks depriving the world of important
technical information and people possibly being harmed, even killed, by the products in question.

In 1941, inspectors of the Food & Drug Administration (FDA) discovered widespread and deadly contamination in a then-new and best-selling antibiotic drug product: sulfathiazole manufactured by the Winthrop Chemical Company.\(^1\) The contamination arose from a series of ill-conceived features of Winthrop’s manufacturing process—a manufacturing process that fast-growing Winthrop had shielded from its competitors. Winthrop had, among other missteps, placed tableting machines for two different drugs in the same room, adjacent to one another, making it dangerously easy for workers to mix the two drugs up.\(^2\) Winthrop downplayed the problem, telling the FDA (falsely) that contamination was limited to a single lot of tablets and telling its customers (falsely) that the issue was a less serious disintegration problem.\(^3\) Winthrop attempted to keep its manufacturing processes and problems secret, but the FDA elected to publicize them. Through a press release widely covered by the news media, the agency informed the public of Winthrop’s deadly contamination and disclosed specific details of Winthrop’s manufacturing processes that had encouraged the accidental contamination (including the inadvisably placed tableting machines).\(^4\) The resulting scandal prompted Winthrop to reform its manufacturing processes (and to replace many executives).\(^5\) The experience also prompted changes throughout the entire U.S. pharmaceutical industry: the FDA revised its regulations to tighten its oversight of all drug makers’ manufacturing processes and to mandate, for the first time, industry-wide manufacturing controls that reduce the risk of accidental contamination.\(^6\) These quality controls, shaped by knowledge of what went wrong at Winthrop, evolved into the so-called “good manufacturing practices” that are the FDA-enforced norm in the pharmaceutical industry today.\(^7\)

A second short story: In 2018 and 2019, hundreds of people died, tragically, in two separate crashes of Boeing’s 737 MAX passenger jet.\(^8\) After

---

2. Id.
3. Id. at 17, 20.
4. See id. at 20 (“On March 31st the FDA issued a press release that stated when Winthrop first heard about the contamination, that they originally told their clients it was a disintegration problem, the practice that propagated the secondary contaminations, the firm’s failure to notify FDA about the problem, and how many deaths and injuries were linked to the drug up to that time.”).
5. Id. at 22.
6. See id. at 23. (“[T]he agency promptly revised NDA procedures to require disclosure of additional data on manufacturing facilities, control procedures, and processing of the finished product.”)
7. Id.
the first crash but before the second, regulators at the Federal Aviation Administration (FAA) determined that the cause of the crash had been the 737 MAX’s flight control system, the Maneuvering Characteristics Augmentation System (MCAS), a combination of hardware and software designed to correct, automatically, the plane’s trajectory when the plane was at risk of stalling.9 After the first crash, the president of a major commercial pilots’ union stated, “[W]hat we need now is to make sure there is nothing else Boeing has not told the companies or the pilots” about the 737 MAX.10 Yet Boeing and the FAA withheld documentation of the MCAS from pilots’ unions, independent experts, watchdog groups, the public at large, and even Congress—and continue to withhold that documentation as of writing—on the theory that those details contain protected trade secrets (i.e., Boeing’s alleged intellectual property).11 The FAA continues to assert that federal trade secrecy law decisively “prohibits the FAA and its employees from disclosing companies’ proprietary information,” including Boeing’s.12 A 2020 report by the House Committee on Transportation & Infrastructure concluded that Boeing’s and the FAA’s secrecy after the first crash contributed to the second, by preventing pilots and the public from learning

---


of the MCAS’s design problems. The same committee report documented myriad other regulatory failures of the FAA and concluded that the agency had exerted “grossly insufficient oversight” overall—"the pernicious result of regulatory capture.”

In choosing public disclosure over secrecy in 1941, the FDA kept the American public safe, warning the public away from a deadly product. But the FDA did more than just alert the public to the mere existence of an adulterated drug; it explained those problems in detail, sharing with the public and with Winthrop’s drug-making competitors the precise details of Winthrop’s manufacturing process that had invited accidental contamination. In so doing, the FDA effectively transformed valuable, closely held private information about drug manufacturing into public knowledge. Sharing this information with the public produced long-term, concrete public benefits. They include the birth of good manufacturing practices throughout the pharmaceutical industry and safer, higher quality drugs in the decades since.

Eight decades later, the FAA has so far chosen secrecy. It has kept details of Boeing’s flawed flight control system secret on the company’s behalf, despite intense, ongoing pressure from watchdog groups, pilots’ and flight attendants’ unions, and other stakeholders.

In December 2019, an independent airline passengers’ group, Flyers Rights, brought a Freedom of Information Act (FOIA) suit against the FAA, seeking to compel the agency

13 House of Representatives Final Committee Report on the Design, Development, and Certification of the Boeing 737 MAX (Sep. 2020), https://transportation.house.gov/imo/media/doc/2020.09.15%20FINAL%20737%20MAX%20Report%20for%20Public%20Release.pdf [https://perma.cc/Z69T-B52M] (criticizing Boeing and the FAA on the grounds that “[t]he collective responses in this critical time period were woefully inadequate and appeared predisposed to blame the pilots”). See also id. at 32, 99 (providing further criticisms of Boeing’s attempts to hide information from the public); Mark, supra note 10 (indicating that many 737 MAX pilots were unaware of the MCAS’s existence).


15 Swann, supra note 1, at 23 (“The Winthrop experience led FDA to sharpen” its good manufacturing practice controls and ultimately contributed to revised FDA procedures “to require disclosure of additional data on manufacturing facilities, control procedures, and processing of the finished product.”).

16 See supra note 11 (discussing a lawsuit on behalf of FlyersRights.org against the FAA); Alison Sider, Flight Attendants Question Safety of 737 MAX, WALL ST. J. (Oct. 31, 2019), https://www.wsj.com/articles/flight-attendants-question-safety-of-max-737-11572563447 [https://perma.cc/F6EK-EPM7] (“American’s 28,000 flight attendants will ‘refuse to walk onto a plane that may not be safe,’ Ms. Bassani wrote, adding that the union will evaluate information from American airlines, pilots, regulators, and Boeing to determine whether to work on the plane again.”); Leslie Josephs, American Airlines’ pilots union concerned about fixes for Boeing 737 Max after crashes, CNBC (June 18, 2019), https://www.cnbc.com/2019/06/18/american-airlines-pilots-union-concerned-about-boeing-737-max-training.html [https://perma.cc/59C6-YK9Q] (“The union has criticized Boeing for not providing enough information about an automated anti-stall system aboard the 737 Max planes.”).
to disclose technical details of the flight control system.\textsuperscript{17} Flyers Rights alleges that it is “impossible for independent technical experts to evaluate any FAA decision to unground the 737 MAX unless they can obtain access to the technical submissions made by Boeing.”\textsuperscript{18} Flyers Rights lost its case in district court\textsuperscript{19} and, at the time of writing, was litigating an appeal.\textsuperscript{20} Time will tell whether FAA releases this information, and what consequences FAA’s choice to resist disclosure will have for the aerospace industry, passenger safety, and public trust in the industry and agency.

The fight over 737 MAX data is just one fight over corporate secrets, but it is likely an important harbinger of more to come. As carmakers follow airplane manufacturers and design their vehicles to be increasingly autonomous, even “self-driving,” contests over access to information on their software and hardware control systems seem almost certain to recur.\textsuperscript{21}

In turn, autonomous vehicles are but one instance of the broader phenomenon of contestation over regulators’ stores of knowledge on technology- and information-intensive industries. We live in the age of “informational capitalism”\textsuperscript{22} and “infoglut.”\textsuperscript{23} As a greater proportion of industry value is tied up in information itself, a greater proportion of the work of regulators is governance of that information. Today, the federal administrative state holds more information than ever—vast reservoirs of scientific knowledge, economic and sociological data, manufacturing schematics, safety testing data, data on environmental harms, and on and on.\textsuperscript{24} As Rory Van Loo has described, today’s federal regulatory state

\textsuperscript{17} Flyers Rights Education Fund, Inc. v. FAA, No. 1:19-cv-03749 (D.D.C. Dec. 16, 2019).
\textsuperscript{18} Id. at 6.
\textsuperscript{19} Id.
\textsuperscript{20} Flyers Rights Education Fund, Inc. v. FAA, No. 21-5257 (D.C. Cir.).
\textsuperscript{21} See infra subsection I.B.1 (discussing NHTSA’s new program disclosing information concerning autonomous vehicles).
\textsuperscript{22} See JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL (2019) (“I use ‘informational capitalism’ to refer to the alignment of capitalism as a mode of production with informationalism as a mode of development.”); Amy Kapczynski, The Law of Informational Capitalism, 129 YALE L.J. 1460, 1466 (2020) (“Cohen argues that we live not in an age of ‘surveillance’ capitalism, which trains our focus on dynamics of surveillance and behavioral control—but in an age of ‘informational capitalism’—which focuses our attention on informationalism as a broader mode of development in the contemporary political economy.”).
\textsuperscript{23} See generally MARK ANDREJEVIC, INFOLUT: HOW TOO MUCH INFORMATION IS CHANGING THE WAY WE THINK AND KNOW (2013).
\textsuperscript{24} See Rory Van Loo, Regulatory Monitors: Policing Firms in the Compliance Era, 119 COLUMBIA L. REV. 369, 376 (2019) (describing the “greater reliance on regulatory monitors’ real-time data”); Irvin B. Vann, Electronic Data Sharing in Public Sector Agencies, in HANDBOOK OF PUBLIC INFORMATION SYSTEMS 249, 249 (Christopher M. Shear & G. David Garson eds., 3d ed. 2010) (“All levels of government in the United States collect, store, analyze, and disseminate vast amounts of data, whether it is in paper or electronic form.”). See also infra Part I (discussing the ways in which information flows at the federal level).
“emphasize[s] ‘continuous’ information flows,” with regulators receiving and generating “real-time data” on the industries they oversee.25

Some of that torrent of information is supposed to reach the public. A leading treatise puts it this way: federal administrative agencies are supposed to “investigate, enforce, cajole, politicize, spend, hire, fire, contract, collect information, and disseminate information.”26 Regulators collect and share information to educate the public on the industries and technologies that shape our lives—a precondition for the formation of public opinion and of democratic oversight of these industries and technologies, as well as of the regulators that regulate them.27 Public access to information is essential not just to public health and safety but to democracy itself.28 A democratic state cannot govern what it cannot understand.29

Yet despite technological advances that facilitate dissemination of information, little of this immense, growing, and nominally “public” resource reaches the public. If anything, the recent trend seems toward less public understanding of the valuable information that regulators collect from the companies they regulate.30 Regulators today often decline to publicize harmful corporate activity and instead cooperate with wrongdoers to keep their secrets secret.31 Why? This article analyzes one particularly important

25 Van Loo, Regulatory Monitors, supra note 24, at 376.


27 See, e.g., ROBERT C. POST, DEMOCRACY, EXPERTISE, ACADEMIC FREEDOM & FIRST AMENDMENT JURISPRUDENCE FOR THE MODERN STATE 27-35 (2012) (discussing the relationship between expertise and democracy); Contreras, J. (2017), Leviathan in the Commons: Biomedical Data and the State, in K. STRANDBURG, B. FRISCHMANN, & M. MADISON, GOVERNING MEDICAL KNOWLEDGE COMMONS 19-45 (explaining federal agencies’ role as “curators” of scientific and technical knowledge); Amy Kapczynski, Dangerous Times: The FDA’s Role in Information Production, Past and Future, 102 MINN. L. REV. 2357 (2018) (elaborating on the FDA’s role as information producer).


29 See generally JAMES C. SCOTT, SEEING LIKE A STATE: HOW CERTAIN SCHEMES TO IMPROVE THE HUMAN CONDITION HAVE FAILED 6-7 (1998). I thank Salomé Viljoen for this memorable formulation.

30 See infra Part I.

31 See infra Part I.B. See also Charles Tait Graves & Sonia Katyal, From Trade Secrecy to Seclusion, 109 GEORGETOWN L.J. 1337, 1352-68 (2021) (detailing situations where the government declines to publicize company data); Mary L. Lyndon, Trade Secrets and Information Access in Environmental Law, in THE LAW AND THEORY OF TRADE Secrecy 442, 442 (Rochelle C. Dreyfuss & Katherine J. Strandburg, eds., 2011) (looking at the same in the environmental context).
barrier—real or imagined—to federal regulators’ publicizing companies’ secrets: trade secrecy.\textsuperscript{32}

Generally speaking, a trade secret is legally protected, “proprietary” information that has economic value from not being known to competitors and is subject to reasonable efforts to maintain its secrecy.\textsuperscript{33} As Charles Tait Graves and Sonia Katyal have shown, companies claim that an expanding body of information on their activities meets this definition,\textsuperscript{34} and that any sort of public disclosure of that information would constitute a violation of trade secrecy law.\textsuperscript{35}

Invocation and fear of trade secrecy law now seriously hinder federal regulators from disseminating to the public reliable information about the spheres of activity that they regulate, especially those that are technology-intensive.\textsuperscript{36} Meanwhile, claims of trade secrecy now even hinder some regulators from obtaining information from the entities they supposedly regulate in the first place.\textsuperscript{37}

Against that backdrop, this article makes two main contributions. The first is legal—a claim about the powers federal agencies have under existing law. The second contribution is normative—a claim about what federal agencies should do with those powers.

\textsuperscript{32} Of course, more than trade secrecy ails the federal regulatory state today. For deeper analysis detailing modern problems in administrative law, see, for example, Julie E. Cohen, \textit{The Regulatory State in the Information Age}, 17 THEORETICAL INQUIRIES LAW 369, 370-71 (2016); COHEN, BETWEEN TRUTH & POWER, supra note 22, at 170; Rory Van Loo, \textit{The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance}, 72 VAND. L. REV. 1563, 1605 (2019); CARY COGLIANESE, Preface to \textit{REGULATORY BREAKDOWN: THE CRISIS OF CONFIDENCE IN U.S. REGULATION} vii (Cary Coglianese ed., 2012); Gillian E. Metzger, \textit{Foreword: 1930s Redux: The Administrative State Under Siege}, 131 HARV. L. REV. 1, 2-4 (2017).

\textsuperscript{33} Uniform Trade Secrets Act § 1(a); 18 U.S.C. § 1839(3); \textit{Trade Secret}, BLACK’S LAW DICTIONARY (10th ed. 2014).

\textsuperscript{34} Graves & Katyal, supra note 31, at 1352-68.

\textsuperscript{35} \textit{Id. See also} Deepa Varadarajan, \textit{Business Secrecy Expansion and FOIA}, 68 UCLA L. REV. 462, 464 (2021) (“Legal and technological changes have created an environment in which firms invoke trade secrecy to protect all manner of information . . . .”).

\textsuperscript{36} See Graves & Katyal, supra note 31, at 1352 (“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 . . . and other efforts to suppress investigations into governmental or corporate practices in the public interest.”); Sonia K. Katyal, \textit{The Paradox of Source Code Secrecy}, 104 CORNELL L. REV. 1183, 1240-41 (2019) (coining the term “information insulation” to refer to “an increased willingness [by government agencies] to assert trade secret protection in cases where transparency might be justified due to public interest concerns.”). \textit{See also infra} Part I.

The article’s first contribution is to disprove the conventional wisdom that trade secrecy law, or any other existing body of law, creates a general bar against federal agencies publicizing corporate secrets. This insight is simple but important, so it bears repeating: as a general rule, federal regulators generally do have a legal right to disclose (and thereby “break”) even bona fide trade secrets. This authority emerges from the regulators’ enabling statutes and from the fundamental background principle, formalized in statutes and reaffirmed by the Supreme Court, that federal agencies have legal discretion to disclose information within their possession. 38 Even the Roberts Court has acknowledged this authority, giving regulators meaningful room to maneuver. 39 Various constitutional and statutory sources of federal law, including the federal Trade Secrets Act 40 and the Fifth Amendment’s Takings Clause, can complicate disclosure and make it expensive for regulators, but they do not prohibit disclosure.

It is simply untrue, as a matter of law, that trade secrecy law prevents the sovereign U.S. government from communicating urgent information to its citizens. For an agency to choose to “break” a private trade secret and share it with the public is no more shocking and no less legal than agencies’ well-established powers to exercise eminent domain over real property, or to use privately patented inventions on the public’s behalf. 41

Yet the view that trade secrecy law categorically prohibits disclosure of private trade secrets to the public currently reigns, both inside and outside the U.S. government. FAA and other agencies repeatedly echo the premise that federal law prohibits disclosure of private trade secrets. 42 In 2020, the usually authoritative Government Accountability Office (GAO) stated flatly that “federal laws generally prohibit agencies from disclosing information that concerns or relates to trade secrets, processes, operations, statistical information, and related information.” 43 Most scholars, too, seem to have accepted the same premise, at least implicitly—even leading scholars who support more disclosure as a normative matter and have advanced important

38 See infra Part III.
39 See infra Part III.
42 See, e.g., Airworthiness Directives; The Boeing Company Airlines, 85 Fed. Reg. 74,560, 74,578 (Nov. 20, 2020) (stating that disclosure by the FAA is prohibited).
proposals to unearth information protected as trade secrets. David Levine, for example, has written that “FOIA and the Trade Secrets Act (TSA), a criminal statute, act in tandem to prohibit the government from releasing any information that meets a FOIA trade secret definition.” Hannah Bloch-Wehba has written that agency disclosure of trade secret decision-making algorithms is “legally precluded because these materials are the proper subject of trade secret protections.” With some notable exceptions, including Bernard Bell, Matthew Herder, and David Vogel, the view that trade secrecy law hamstrings the government’s ability to communicate with the public now dominates.

To be clear, regulators’ trade secret-breaking power is far from absolute. Via various enabling statutes, Congress has prohibited some federal regulators from disclosing trade secrets, as I explain below. The most notable regulator so limited is the Federal Trade Commission (FTC); given FTC’s unmatched information-gathering ability, FTC’s bar on disclosure of


48 See Matthew Herder, Reviving the FDA’s Authority to Publicly Explain Why New Drug Applications Are Approved or Rejected, 178 JAMA INTERNAL MED. 1013, 1013 (2018) (“[T]he barrier to greater disclosure is the FDA’s interpretation of its governing laws rather than the laws themselves.”).

49 See David A. Vogel, Government Agencies Can Misuse Your Trade Secret and You Can’t Stop Them, 28 PUB. CONTRACT L. J. 159, 166 (1999) (“The Federal Government can have numerous reasons for releasing a trade secret to a third party or to the general public.”).

50 See infra section III.B.1.

51 See, e.g., A Brief Overview of the Federal Trade Commission’s Investigative, Law Enforcement, and Rulemaking Authority, FED. TRADE COMM’N, https://www.ftc.gov/about-ftc/what-
agency-held trade secrets is momentous. Other agencies’ enabling statutes prohibit them from disclosing certain types of trade secrets, or permit disclosure only when narrow factual circumstances apply. Nonetheless, a majority of major federal regulators, including the Environmental Protection Agency (EPA), FAA, Federal Communications Commission (FCC), FDA, the Department of Health and Human Services (HHS), the National Highway Traffic Safety Administration (NHTSA), and the National Transportation Safety Board (NTSB), retain broad authority to obtain and disclose at least some of the trade secrets (and other secrets) they obtain from the companies they regulate.

The insight that federal regulators can obtain and disclose trade secrets moves the terrain of debate from what is possible as a matter of law to what is desirable as a matter of public policy. It prompts hard normative questions: If an agency can take even bona fide secrets from private companies and publicize them, when and how should it? Which secrets should it share? With whom? On what terms? Real harms surely flow from overbroad disclosure, not just to affected individual companies but to entire industries and to the broader economy.

Accordingly, the article’s second main contribution is a new normative theory of how federal regulators should wield their power to disclose corporate secrets. It proposes selective, controlled “information publicity” of corporate secrets for public good. I choose the phrase “information publicity” rather than simple “disclosure” to emphasize the need to tailor information disclosure to serve some interests in information over others. Transparency is not an end unto itself. Its benefits and costs depend entirely on its context—who is using the information, in what ways, to what ends. As Kapczynski wrote in a recent call to arms, “we cannot achieve the insights that we need into data and AI systems through a simple insistence on passive


52 See infra section III.B.1.
53 See infra section III.B.1.
54 Kapczynski and I chose the corresponding term “data publicity” in our predecessor paper, which proposed controlled disclosure of specific scientific data held by FDA. 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 and Vaccines, 109 CALIF. L. REV. 493, 500 (2021) (“[W]e call what we seek here not data transparency, but data ‘publicity.’”).
55 For two leading analyses of the limits of “transparency” and “privacy” as goals unto themselves, see Daniel J. Solove, Access and Aggregation: Public Records, Privacy and the Constitution, 86 MINN. L. REV. 1137, 1197 (2002), and David Pozen, Transparency’s Ideological Drift, 128 YALE L. J. 100, 108 (2018).
and unmediated ‘transparency.’ If access to data is to serve public ends, it will need to be active, sensitive to underlying structures of power, and in many cases, conditional.”

To that end, the article proposes agency-administered programs of information publicity that do not simply disclose information to all comers, unconditionally, but instead cultivate carefully bounded “gardens” of information. These gardens may exclude some, and they may subject users to substantial legal and technical constraints on information access and use. I argue that agencies can and should discriminate among users and uses, to privilege socially valuable uses and to protect legitimate trade secrets from competitive uses and consequent economic harm. In this way, the competitive value of trade secret information can be protected while socially beneficial noncommercial uses of the information are unlocked. To invoke the garden metaphor: Regulators must be responsible caretakers of the informational “flora” they collect from the companies they regulate. Regulators may permit some representatives of the public to pick informational “fruit,” but only if they do so in ways that don’t harm the plant. Regulators can block competitors and irresponsible would-be users from entering the garden at all.

The bounded garden model of information publicity I propose here builds on recent proposals for “controlled-access” or “bounded” disclosure of trade secrets from Mary Fan, as well as Amy Kapczynski and me. It draws heavily from scholars of privacy and information law, especially Helen Nissenbaum and Daniel Solove. To borrow Nissenbaum’s term, what I propose is, in effect, a kind of “contextual integrity” for trade secrets. My

---


58 See Morten & Kapczynski, supra note 54, at 500-01 (“[T]he future of freedom of information... lies in the development of robust proactive disclosure systems. In part to mark these distinctions, we call what we seek here not data transparency, but data ‘publicity.’ The term as we use it, which draws upon early progressive traditions, marks the need for attention to context, power, and resources if data sharing is to serve the public.”).

59 See infra note 194 and accompanying text.

60 Solove, infra note 193 and accompanying text. This paper is far from the first to recognize doctrinal and conceptual parallels between privacy and trade secrecy. See, e.g., Pamela Samuelson, Privacy as Intellectual Property?, 52 STAN. L. REV. 1125, 1151-52 (2000) (recognizing three important interests that trade secrecy and information privacy have in common); Sharon K. Sandeen, Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law, 2006 MICH. STATE L. REV. 667, 670 (2006) (detailing the parallels in the development of information privacy law and trade secret law).

61 See discussion infra section II.A.
Publicizing Corporate Secrets

model also draws from Sharon Sandeen’s analysis of the doctrine, history, and purposes of trade secrecy law; in trade secret misappropriation cases between private plaintiffs and private defendants, courts and litigants are more likely to recognize that trade secret rights are contingent and limited.62 Finally, my proposal also draws on largely overlooked but vital and contemporary real-world examples of controlled disclosure of valuable information by regulators in contexts where trade secrecy, individual privacy, and other interests militate against unfettered disclosure.63 In other words, I show that successful agency-run information publicity is already happening.

The article proceeds in four parts. Part I describes the troubling status quo: despite unparalleled access to valuable corporate information, federal regulators share little with the public, and the public has no effective recourse. Part II provides a normative case for reviving “information publicity”—controlled, conditioned disclosure of corporate secrets—and prescribes how it should be done. Part III presents a legal roadmap to this sort of information publicity. Part III “shows my work”; it identifies the sources and limits of regulatory agencies’ disclosure authority under existing law. It also presents two simple steps that interested federal regulatory agencies can take to protect information publicity programs from legal challenge, even under scrutiny by a Supreme Court with a pronounced deregulatory bent. I conclude with brief thoughts on how federal agencies’ legal authority to publicize corporate secrets might be exercised more broadly in the data economy and informational age.

A quick note on terminology: Throughout this paper, I use the somewhat unorthodox phrase “corporate secrets.” I intend “corporate secrets” as a convenient umbrella term that encompasses all secret information generated by private commercial entities—not just true corporations but also non-corporate companies, partnerships, and so on. Corporate secrets include all “trade secrets.” But I also use the term corporate secrets to refer to a wider swath of information. This wider swath includes secret information that does not qualify, for one reason or another, for protection as a trade secret but

---

62 See Sandeen, Relative Privacy, supra note 60, at 675-76 (explaining American trade secrecy law’s traditional rejection of a “property basis” and focus instead on the relationship between plaintiff and defendant in trade secret misappropriation cases); see also 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, 498-99 (2010) (“[E]arly courts were unwilling to find an absolute property interest in secret information, [thus] the success of early trade secret cases depended upon the existence of an express or implied agreement of confidentiality or breach of faith.”); Sharon K. Sandeen, Out Of Thin Air: Trade Secrets, Cybersecurity And The Wrongful Acquisition Tort, in RESEARCH HANDBOOK ON INTELLECTUAL PROPERTY AND DIGITAL TECHNOLOGIES (Tanya Aplin ed., 2020) 363, 366, 372 (noting trade secrets may be protected against misappropriation only if, the recipient of the information engaged in wrongful conduct).

63 See infra subsection II.B.2.d.
nonetheless has some commercial or financial value and is accordingly protected by FOIA’s exemption for “commercial or financial information . . . [that is] privileged or confidential” (also known as “confidential commercial information,” or “CCI”). More broadly still, corporate secrets also encompass information that corporations and other businesses manage to keep secret despite the information lacking any genuine commercial or financial character, such as embarrassing evidence of “illegal or unethical payments to government officials or violations of civil rights, environmental or safety laws.”

I choose “corporate secrets” not just because it is a concise and convenient shorthand for all this information but also because it helpfully disregards distinctions between trade secrets, CCI, and other secret information. As I argue below, the precise formal legal category of a piece of information is often irrelevant as a legal matter; under existing federal law, a federal agency can often legally disclose a corporate secret no matter whether it is a trade secret or CCI, assuming the agency takes certain preparatory steps. Moreover, agonizing over the formal legal category of a piece of information is often unhelpful from a policy perspective, as it obscures more pressing, fact-specific questions of the specific harms and benefits likely to flow from publicizing the information in question.

I. A DANGEROUS STATUS QUO

This Part tells a story of how information flows through the federal regulatory state. A torrent of information on regulated entities flows into federal regulatory agencies, yet only a fraction currently trickles out to the public. This Part is primarily descriptive; it maps those information flows. It proceeds in three subparts. Subpart I.A shows that federal regulators have sweeping and durable power to demand and collect information generated and held by the private companies they regulate. Subpart I.B summarizes what federal regulators today do with secrets they collect. It surveys a handful of effective programs of proactive disclosure of corporate secrets to the public. These programs underscore the value of such disclosure, but such programs are scattered, and their numbers may be declining. Subpart I.C then briefly describes the public’s existing set of tools to “self-help”—to get access to corporate secrets of public interest when the relevant regulator does not share them proactively. Subpart I.C shows that this set of tools is small and inadequate. The problem of obsessive corporate secrecy has become deadly

---

66 See infra Part III.
67 See infra Part II.
serious, as journalists, public interest groups, academic researchers, and other representatives of the public find themselves without access to vital information in federal regulators’ hands, even when the information is of intense public interest.

In sum, this descriptive Part will paint a rather dismal picture: the federal regulatory state’s proactive disclosure programs are scattered and limited. FOIA is painful for agencies and public alike, and yet it is the dominant means by which the public obtains information from federal regulators. This picture forms the backdrop for a better solution: proactive information publicity, as proposed in Part II.

A. Sweeping Access: Federal Regulators’ Information-Gathering Powers

U.S. federal regulators hold oceans of information, much of it gathered from the companies they regulate.68 A few examples: FDA houses the largest known repository of clinical data” on prescription drugs and medical devices in the world—almost all of which is generated by industry and then submitted to FDA.69 EPA maintains numerous databases on (inter alia) air and water pollution, environmental radiation, and the chemical and toxicological properties of pesticides.70 The National Transportation Safety Board (NTSB) and FAA each hold vaults of information on commercial aircraft and airline accidents.71

These examples are just the tip of the informational iceberg frozen inside the federal regulatory state. Van Loo72 and Cory Coglianese, Richard

68 See generally Van Loo, Regulatory Monitors, supra note 24, at 376 (“Current governance models [...] emphasize ‘continuous’ information flows. . . . “); see also Irvin B. Vann, Electronic Data Sharing in Public Sector Agencies, in HANDBOOK OF PUBLIC INFORMATION SYSTEMS 249, 249 (Christopher M. Shea & G. David Garson eds., 3d ed. 2010) (“All levels of government in the United States collect, store, analyze, and disseminate vast amounts of data. . . . “); Elizabeth A. Rowe, Striking A Balance: When Should Trade Secret Law Shield Disclosures to the Government?, 96 IOWA L. REV. 791, 803 (2011) (“Agencies, as part of their regulatory function, receive a vast amount of proprietary information from businesses.”).]

69 Morten & Kapczynski, supra note 54, at 503; FDA, DRIVING BIOMEDICAL INNOVATION: INITIATIVES TO IMPROVE PRODUCTS FOR PATIENTS 22 (Oct. 2011), https://www.clinicaltrials.gov/ct2/results?term=otc&show=study
detailonly&cond=adult&drugs=


72 Van Loo, Regulatory Monitors, supra note 24, at 376. Inter alia, Van Loo provides detailed data on various agencies’ resources, including the size of their investigative workforces. See generally, id.
Zeckhauser & Edward Parson\textsuperscript{73} have analyzed in more detail the enormous information flows into the federal regulatory state as a whole. Rather than retrace those authors’ steps, I focus here on how federal regulators come to hold information on the businesses they regulate. I do so for two reasons.

First, the federal administrative state has changed significantly in recent decades and continues to change. Several interrelated trends have converged to sap many regulators’ efficacy, ambition, and independence—among them declining appropriations from Congress, high turnover of agency staff, corporate capture of agency leadership, and executive orders that hamstring agencies’ independence.\textsuperscript{74} Rebuilding the federal regulatory state will require, \textit{inter alia}, restoring agencies’ information-gathering authority. Thus, the question of what precise information the federal regulatory state holds now is arguably less important than the question of what information it could collect, hold, and use in the future.

The second reason I focus on federal regulatory agencies’ information-gathering capacity is to address a concern that reviving regulators’ practice of publicizing corporate secrets will jeopardize other vital elements of the regulators’ work. That concern has been elaborated most thoroughly by Elizabeth Rowe,\textsuperscript{75} but it has been echoed by courts\textsuperscript{76} and by agencies

\textsuperscript{73} See Cary Coglianese et al., \textit{Seeking Truth for Power: Informational Strategy and Regulatory Policymaking}, 89 MINN. L. REV. 277, 305 (2004) (discussing the tactics that regulatory agencies use to elicit information).

\textsuperscript{74} See, e.g., Metzger, supra note 32, at 2 (noting antiregulatory actions, such as decreased funding and repealed regulations, during the Trump administration); Pozen, \textit{Transparency’s Ideological Drift}, supra note 55, at 123 (“[T]ransparency has become increasingly associated with institutional incapacity and with agendas that seek to maximize market freedom and shrink the state.”); Cohen, \textit{The Regulatory State in the Information Age}, supra note 32, at 375 (“[I]nstitutional disruption has provided new points of entry for power. Emerging, nontraditional regulatory models have tended to be both opaque to external observation and highly prone to capture.”); Lisa Heinzerling, \textit{Quality Control: A Reply to Professor Sunstein}, 102 CAL. L. REV. 1457, 1458, 1461-62 (2014) (noting the downsfalls of both cost-benefit analysis and breakeven analysis in justifying regulations); Frank Pasquale, \textit{Cost-Benefit Analysis at a Crossroads: A Symposium on the Future of Quantitative Policy Evaluation}, THE LAW AND POLITICAL ECONOMY PROJECT (Sep. 27, 2021), https://lpeproject.org/blog/cost-benefit-analysis-at-a-crossroads-the-future-of-quantitative-policy-evaluation/ [https://perma.cc/3P9K-4BSG] (noting that during the Reagan administration cost-benefit analysis “was almost always presented as a check on regulation, rather than a way to promote more effective regulation”)

\textsuperscript{75} Rowe, \textit{Striking A Balance}, supra note 68, at 815-18.

themselves.\textsuperscript{77} The concern is that disclosure’s short-term public benefits can easily be outweighed by harmful long-term ripple effects. If a regulator discloses secret information from even a single company, its “collegial” relationships with entire industries may be permanently altered. Thus, regulated entities may refuse to submit sensitive information to the regulator, or hide it from inspectors, or condition submission of information on the agency’s assurance of secrecy.\textsuperscript{78}

That concern is important but manageable, in my view, for two main reasons. First, as this subpart shows, federal regulators have power to get information even if their relationships with industry become less “collegial.” (Of course, one might argue, as Julie Cohen\textsuperscript{79} and others have, that less collegiality between regulators and those they regulate might actually be good for regulation, on balance.) By and large, federal regulators simply do not have to rely on regulated entities’ voluntary submissions to obtain good information. The myriad enabling statutes that create and empower federal regulatory agencies almost always empower those agencies to collect secret information from regulated entities, with or without regulated entities’ consent. In this article, I summarize two varieties of that power—premarket approval and investigative.\textsuperscript{80}

Second, regulators can cultivate carefully bounded “gardens” of corporate secrets that constrain users’ access and use to reduce financial harm to the sources of such secrets and protect regulators’ relationships. These bounded gardens are the focus of Part II.

\textsuperscript{77} See, e.g., Requests for Confidential Treatment of Records Obtained by the Commission, 45 Fed. Reg. 1627, 1628 (Jan. 8, 1980) (“The [Securities & Exchange] Commission believes that the voluntary submission of information will be encouraged if the Commission has procedures which promote the fair evaluation of claims of confidentiality. . . .”); Nanoscale Materials Stewardship Program, 73 Fed. Reg. 4861, 4864 (Jan. 28, 2008) (indicating the EPA’s similar stance); Zachary Brennan, Why FDA Can’t Disclose the First Coronavirus-related Drug Shortage, REGULATORY FOCUS (Feb. 28, 2020), https://www.raps.org/news-and-articles/news-articles/2020/2/why-fda-cant-disclose-the-first-coronavirus-relat (quoting an FDA spokesperson who said that FDA relies on “the cooperation of the drug companies in order to obtain accurate information . . . and companies will be less willing to provide this voluntary information if they cannot trust FDA not to disclose commercial confidential information such as drug names, company names or exact location of facilities.”).

\textsuperscript{78} See Rowe, Striking A Balance, supra note 68, at 794 (“sometimes [companies] are either unwilling to provide trade-secret information at all, or may be willing to provide the information if and only if the integrity and safety of the information will be fully protected against direct or indirect disclosure to competitors.”).

\textsuperscript{79} See Cohen, The Regulatory State in the Information Age, supra note 32, at 413 (“In the informational era, thinking about the proper relationship between government and management requires a more measured and constructively critical approach.”).

\textsuperscript{80} Any harms to the company whose secrets are disclosed, and any chilling effects felt industry-wide, can be minimized through use of bounded information publicity, discussed in detail in Part II.
1. Premarket Approval

A minority of federal regulators possess a particularly potent tool to collect information from regulated entities: “premarket approval” power. When an agency possesses this power, a private entity seeking to sell a new good or service on the U.S. market must first apply for and receive the regulator’s approval before it can legally do so.81 Among the federal regulators that wield premarket approval power are FDA (with respect to essentially all prescription drugs82 and vaccines83 and some medical devices84), EPA (pesticides85), Department of Defense (military equipment and other defense contracting86), and FAA (design and manufacture of commercial airplanes, operation of commercial airlines87).

Under premarket approval review regimes, regulators require applicants to make certified submissions of large quantities of information on their products and services, which are then reviewed by the regulator to decide whether to approve or deny the application. FDA, for example, has for decades demanded that drug companies generate and submit reams of data as a condition of letting those companies’ new drugs onto the U.S. market.88 Regulated entities that decline to submit the required information are barred from the market.89

82 See 21 U.S.C. § 355(e) (“The Secretary shall undertake enhanced and joint enforcement activities with other Federal and State agencies, and establish regional capacities for the validation of prescription drugs. . .”).
83 See 42 U.S.C. § 262 (“The Secretary shall establish, by regulation, requirements for the approval, suspension, and revocation of biologics licenses.”).
84 See 21 U.S.C. § 360(e) (“The Secretary may by regulation prescribe a uniform system for the identification of devices intended for human use and may require that persons who are required to list. . . shall list such devices in accordance with such system.”).
85 See 7 U.S.C. § 136a(c)(1)(D) (stating that a person cannot sell pesticide unless she turns over a “complete formula of the pesticide” to the Environmental Protection Agency).
86 See 48 C.F.R. § 227.7102-1(a) (requiring defense contractors to submit certain “technical data,” defined by rule, to DOD as a condition of DOD’s purchase).
87 See 49 U.S.C. §§ 40113, 44701, 44704, 44709, 44711, and 44713 (establishing FAA’s certification process and mandating that aircraft cannot fly in U.S. airspace without FAA certification). FAA’s premarket approval rules are set out at 14 CFR Subchapter C §§ 413.1, 413.3, 413.5, 413.7.
88 See Morten & Kapczynski, supra note 54, at 592 (describing some of the types of data required by FDA for review and approval of new products).
89 See Ruckelshaus, 467 U.S. at 1007 (observing that pesticide manufacturers had to choose between submitting (allegedly) trade secret information to the government and foregoing “the ability to market pesticides in this country”). Of course, faced with the prospect of unwanted disclosure of their secrets, regulated entities could refuse altogether to sell their goods and services in the U.S. marketplace, refusing all U.S. sales revenues to protect their secret information. See
Regulated entities have argued in the past\textsuperscript{90} and may argue again that a regulator’s decision to make submission of trade secret information a precondition of approval constitutes an unconstitutional condition, under a takings\textsuperscript{91} or other constitutional theory. But the Supreme Court has foreclosed this argument: in \textit{Ruckelshaus v. Monsanto}, it held that a regulator (EPA) may legally require a regulated company (a pesticide manufacturer) to submit information on a product (a pesticide) that the regulator and regulated company agreed was a trade secret (the pesticide’s health and safety properties) as a condition of permission to sell the product to the U.S. market.\textsuperscript{92} \textit{Ruckelshaus} declared (quoting Justice Brandeis) that such restrictions on manufacturers “are the burdens we all must bear in exchange for the advantage of living and doing business in a civilized community.”\textsuperscript{93}

\textit{Ruckelshaus}’s holding that regulators may condition regulatory approval on mandatory submission and disclosure of information remains the law. To be sure, it has been criticized.\textsuperscript{94} A 2002 en banc decision of the First Circuit attempted to cabin \textit{Ruckelshaus} into near-oblivion, suggesting that it had effectively been overruled \textit{sub silentio} by subsequent Supreme Court decisions.\textsuperscript{95} In that case, the tobacco giant Philip Morris managed to defeat a

---

\textsuperscript{90} See Philip Morris, Inc. v. Reilly, 312 F.3d 24, 27-29 (1st Cir. 2002) (en banc) (discussing the arguments made by Philip Morris and other tobacco companies challenging statutes requiring public disclosure of ingredients lists).

\textsuperscript{91} For more thorough discussion of the Takings Clause and its interaction with federal agencies’ disclosure authority, see infra Section III.B.3.

\textsuperscript{92} See \textit{Ruckelshaus}, 467 U.S. at 1007 (“[A] voluntary submission of data by an applicant in exchange for the economic advantages of a registration can hardly be called a taking.”).

\textsuperscript{93} \textit{Id.} (internal quotation marks and citations omitted). See also Corn Prods. Refining Co. v. Eddy, 249 U.S. 427, 431 (1919) (holding that “a manufacturer or vendor has no constitutional right to sell goods without giving to the purchaser fair information of what it is that is being sold”); Kapczynski, \textit{The Public History}, supra note 89, at 1435 (describing legal logic of the early 20\textsuperscript{th} century, which suggested that because states create the markets, businesses transacting in those markets must necessarily be subject to public regulation).

\textsuperscript{94} See Janka, supra note 44, at 367-68 (arguing that the decision should be construed today to provide broad protection for trade secrets); Richard A. Epstein, \textit{The Constitutional Protection of Trade Secrets and Patents Under the Biologics Price Competition and Innovation Act of 2009}, 66 FOOD \& DRUG L.J. 285, 304-13 (2011) (arguing extensively that this element of \textit{Ruckelshaus}’s holding exists in some tension with later Supreme Court decisions on the unconstitutional conditions doctrine and the reach of the Takings Clause). Yet even Richard Epstein acknowledges that the Court “tiptoed…around” \textit{Ruckelshaus} rather than overrule it. \textit{Id.} at 308.

\textsuperscript{95} Philip Morris, Inc. v. Reilly, 312 F.3d 24, 47 & n.21 (1st Cir. 2002) (en banc) (concluding that a Massachusetts disclosure law imposed an unconstitutional condition, declining to adhere to the holding of \textit{Ruckelshaus}, and electing instead to apply the reasoning of a later Supreme Court decision, \textit{Nollan v. Cal. Coastal Comm’n}, 483 U.S. 825, 833 n. 2 (1987)).
Massachusetts state law that would have required it to disclose to regulators and the public a complete list of the ingredients in its cigarettes. But, unlike the First Circuit, the Supreme Court has consistently reaffirmed Ruckelshaus—and this specific holding—as good law, as recently as 2019. If the Court has cabinéd this aspect of Ruckelshaus at all, it is only in the modest respect that, to avoid imposing an unconstitutional condition, the regulator must confirm that the goods and services properly subjected to mandatory information submission and disclosure schemes pose some legitimate risk to the public—e.g., to environmental health or workers’ safety.

2. Investigation

Most federal regulators—even those that lack premarket approval authority—possess a second, similarly potent tool to collect data from regulated entities: investigation. Agencies with investigative power can, through subpoenas and the like, demand that regulated entities submit confidential information, or can send auditors and inspectors to gather that information, with penalties for noncompliance. As Van Loo has written,

96 Id.
97 Ruckelshaus was cited as good law in the Court’s conservative-led 2015 and 2019 takings decisions in Horne and Knick. See Horne v. Dep’t of Agric., 576 U.S. 351, 365–66 (2015) (characterizing the regulations in the case as creating a voluntary exchange of benefits); Knick v. Township of Scott, Pa., 139 S. Ct. 2162, 2173 (2019) (upholding language in Ruckelshaus, which states that no takings occur unless administrative remedies have been exhausted).
98 See Horne, 576 U.S. at 366 (characterizing Ruckelshaus as “[a] case about conditioning the sale of hazardous substances on disclosure of health, safety, and environmental information related to those hazards” and describing government-granted permission to engage in commerce as a “valuable Government benefit”). This portion of Horne is entirely consistent with Ruckelshaus itself, which held that conditioning permission to sell a product on public disclosure about the product is particularly appropriate “in an area, such as pesticide sale and use, that has long been the source of public concern and the subject of government regulation.” Ruckelshaus, 467 U.S. at 1007. Cf. Cedar Point Nursery v. Hassid, 141 S. Ct. 2063, 2079 (2021) (“[T]he government may require property owners to cede a right of access as a condition of receiving certain benefits, without causing a taking. . . . When the government conditions the grant of a benefit such as a permit, license, or registration on allowing access for reasonable health and safety inspections, both the nexus and rough proportionality requirements of the constitutional conditions framework should not be difficult to satisfy.”).
99 In this paper, I use the term “investigation” broadly, to refer to all information-gathering activities that do not involve premarket approval or rely on voluntary submissions of information by regulated entities. As such, the term “investigation” covers not just formal investigations—e.g., those made pursuant to a specific consumer complaint—but also less formal information-gathering.
900 See Coglianese, Zeckhauser & Parson, Seeking Truth for Power, supra note 73, at 307 (“Regulators can mandate that firms release information or submit to government audits or inspections, with the threat of penalties if firms do not comply.”); KRISTIN E. HICKMAN & RICHARD J. PIERCE, JR., ADMINISTRATIVE LAW TREATISE 940 (6th ed. 2019) (“Most agencies
“[i]n many agencies, regulatory monitors combine prosecutors’ enforcement and adjudication authority with the patrol function of police officers and investigatory function of detectives.”\textsuperscript{101} The only real limit is that the information gathering must serve the regulator’s statutorily-defined regulatory function.\textsuperscript{102}

Among the many federal regulators with strong investigative authority resources are the U.S. Department of Agriculture (USDA) (which, \textit{inter alia}, sends investigators into slaughterhouses and meat processing plants\textsuperscript{103}), Centers for Medicare & Medicaid Services (CMS) (which investigates, \textit{inter alia}, medical testing laboratories\textsuperscript{104}), EPA (which investigates, \textit{inter alia}, water pollution,\textsuperscript{105} oil tankers,\textsuperscript{106} and makers and distributors of pesticides\textsuperscript{107}), FAA (which investigates, \textit{inter alia}, aircraft manufacturers and commercial airlines\textsuperscript{108}), FDA (which investigates, \textit{inter alia}, drug manufacturing facilities\textsuperscript{109} and clinical trials\textsuperscript{110}), FTC (which has wide-ranging authority to investigate most any corporate activity that affects competition and consumer welfare\textsuperscript{111}), the Department of Health and Human Services’ (HHS) Office have broad powers to compel reports.”); \textit{id.} at 950 (the prevailing “legal framework renders it difficult for any private party to prevail in a subpoena enforcement dispute”); Van Loo, \textit{Regulatory Monitors, supra} note 24, at 395 (observing that “[a]cross diverse industries and under both Democratic and Republican party leadership, Congress has since the mid-1800s steadily expanded federal agencies’ ability to monitor private firms”); Diego A. Zambrano, \textit{Discovery as Regulation}, 119 MICH. L. REV. 71, 102-03 (2020) (summarizing federal administrative agencies’ strong and broad subpoena power).

\textsuperscript{101} Van Loo, \textit{Regulatory Monitors, supra} note 24, at 374.

\textsuperscript{102} KRISTIN E. HICKMAN & RICHARD J. PIERCE, JR., \textit{ADMINISTRATIVE LAW TREATISE} 941, 946, 950, 983 (6th ed. 2019).


\textsuperscript{105} 33 U.S.C. § 1318.

\textsuperscript{106} 33 U.S.C. § 1321.

\textsuperscript{107} 7 U.S.C. § 126g.

\textsuperscript{108} 49 U.S.C. § 44709(a).


\textsuperscript{111} See 15 U.S.C. §§ 43, 46(a) (granting the FTC authority to investigate any person or organization in the United States with business activities impacting commerce, with the exception of banks). For analysis of FTC’s potent investigative powers, see Van Loo, \textit{The Missing Regulatory State, supra} note 32, at 1617 (describing FTC’s powers). See also Andrea Vittorio, \textit{FTC’s Demand for Tech Company Data Shows ‘Underutilized’ Power}, BLOOMBERG LAW (Dec. 16, 2020, 5:01AM),
for Civil Rights (OCR) (which investigates healthcare providers’ compliance with medical data privacy rules and federal civil rights laws\textsuperscript{112}), and NTSB (which investigates the causes of aviation and other transportation accidents\textsuperscript{113}). In each case, agency inspectors have legal authority to collect confidential information from regulated entities and authority to retain and use what they collect.

B. Locked Vaults: Federal Regulators Keeping Corporate Secrets of Public Interest

The previous subpart described how federal regulators gather secret information from industries they regulate. This subpart turns to how regulators share those secrets with the public—and whether they share at all.

Today, federal regulators tend to keep corporate secrets secret. True, some federal regulators maintain programs of broad proactive disclosure of corporate secrets of public interest, and these programs underscore the social value of such disclosure. However, these proactive programs are scattered, and anecdotal evidence suggests they have dwindled in recent years.

1. Regulators’ Scattered Proactive Disclosure Programs

A few federal regulators maintain effective programs of proactive disclosure of corporate secrets. Like FDA’s disclosure of manufacturing problems at Winthrop Chemical,\textsuperscript{114} these programs inform the public of corporate malfeasance and keep regulators themselves publicly accountable.

Here are three examples:

1. For years, FDA has consistently publicized reports prepared by FDA inspectors that document deviations from Current Good Manufacturing Practices in pharmaceutical manufacturing facilities around the world.\textsuperscript{115} For example, between 2016 and 2020 FDA published a series of these reports documenting ongoing mold contamination at an ostensibly sterile drug

\textsuperscript{112} Infra § III.B.

\textsuperscript{113} See The Investigative Process, NTSB, \url{https://www.ntsb.gov/investigations/process/Pages/default.aspx} (describing the NTSB’s investigative process).

\textsuperscript{114} See Swann, supra notes 1–7 and accompanying text.

manufacturing plant in Kansas operated by Pfizer. Although the Pfizer plant still suffered from problems in early 2020, media coverage (plus FDA's chastisement) led Pfizer to make “significant management changes” between their 2018 and 2020 inspections, which helped lead to an improved rating at the 2020 inspection at the Kansas plant—just in time to begin packaging and shipping the Pfizer-BioNTech COVID-19 vaccine. Moreover, after the January 2020 report, a Pfizer spokesperson announced that “‘significant investments have been made’ in resources, equipment and the facility.”

2. The Centers of Medicare & Medicaid Services (CMS), which regulates most medical laboratory testing in the U.S., similarly publicizes its laboratory inspection reports as a matter of standard practice. In CMS’s words, the agency makes such reports—so-called “CMS Form 2567” —”publicly available through a variety of settings as part of the Department’s commitment to transparency, and to providing all health care consumers and the general public with access to quality and safety information.” In 2016, CMS disclosed an inspection report cataloguing rampant problems in the central lab of the then-high-flying, now-infamous Silicon Valley biotech startup Theranos, which created “immediate jeopardy to patient health and safety.”

The report disclosed technical flaws in the Edison, a proprietary, secret, and supposedly highly innovative blood testing device developed by Theranos.

---

116 See Sarah Jane Tribble, Pfizer’s Newest Vaccine Plant Has Persistent Mold Issues, History of Recalls, KAISER HEALTH NEWS (Mar. 10, 2021), https://khn.org/news/article/pfizer-new-vaccine-plant-persistent-mold-issues-history-of-recalls/ (“Pfizer’s management knew last year there was ‘a mold issue’ at the Kansas facility now slated to produce the drugmaker’s urgently needed covid-19 vaccine, according to a Food and Drug Administration inspection report.”).


118 Tribble, supra note 116.

119 See JOHN CARREYROU, BAD BLOOD 284 (2018) (“CMS usually made such documents public a few weeks after sending them to the offending laboratory, but Theranos was invoking trade secrets to demand that it be kept confidential.”).


Once released, CMS’s report was dissected by independent experts, who declared the Edison “not reliable enough to form the backbone of a lab service.” Shortly thereafter, Theranos publicly voided or revised tens of thousands of test results obtained on the Edison in 2014 and 2015—unreliable results that had shaped doctors’ care and harmed patients’ health. CMS’s disclosure thus helped to drive a dangerous device out of use, and Theranos itself went out of business two years later.

3. In June 2021, the National Highway Traffic Safety Administration (NHTSA) issued a new order requiring automakers, tech companies, and other entities that design and operate vehicles equipped with advanced driver-assistance and fully automated driving systems—so-called “self-driving cars”—to submit crash data promptly after any crash. NHTSA’s order was explicit that the goal of this effort is not just to gather information but to disseminate it: except for a few categories of information defined by the agency (not industry) as protected “confidential business information,” NHTSA has vowed it “will not keep this information confidential” and “intends to make it publicly available.” NHTSA’s acting administrator stated that “gathering data will help instill public confidence that the federal

redacted in the latest version [of the report], show that the devices often failed to meet Theranos’s own accuracy requirements for a range of tests. . . ."

123 See Scott Gottlieb, Theranos Woes Offer Lesson In How Labs Should Be Regulated, FORBES (Apr. 28, 2016), https://www.forbes.com/sites/scottgottlieb/2016/04/28/theranos-woes-offer-lesson-in-how-labs-should-be-regulated/?sh=72618ea348d9 [https://perma.cc/3988-C4TG] (discussing how the problems at Theranos were both the machine itself and how the lab was run).


government is closely overseeing the safety of automated vehicles” and that “[a]ccess to [driverless vehicle] data may show whether there are common patterns in driverless vehicle crashes or systematic problems in operation.”

As of November 2022, the NHTSA has disclosed data from 18 fatal accidents it said involved advanced driver-assistance. (Almost all of these accidents involved a Tesla.

2. Regulators Tending Toward Secrecy

The above examples of proactive information publicity programs at federal regulatory agencies are isolated. In recent years, many federal regulators—even some of the same regulators that once promoted proactive information publicity programs—have resisted calls to share secret information on the businesses they regulate. The story of FAA’s ongoing refusal to disclose data on Boeing’s 737 MAX is no outlier.

Take fracking. Consumer groups, environmentalists, and scientists have fought, for years, to get information on the potentially toxic chemicals used in fracking fluid, which can poison soil and water. Despite these efforts, the federal regulators that hold this information—EPA and Bureau of Land Management (BLM)—have refused to disclose it.

A representative of the environmental group Environmental Integrity Project (EIP) said it had “long pressed the EPA to have the oil and gas industry report fracking fluid ingredients under an EPA program called the Toxic Release Inventory, a


132 See supra notes 8-14 and accompanying text.

133 See Graves & Katyal, supra note 31, at 1358 (“According to one report from the Government Accountability Office, ninety-five percent of new notifications (and almost 18,000 chemicals) are . . . withheld from the public.”). See also Lyndon, Trade Secrets and Information Access in Environmental Law, supra note 31, at 444 (“With respect to trade secrets, the [Toxic Substances Control Act] seems to require disclosure of health and safety studies relating to any chemical in commercial distribution, whether they are claimed as proprietary or not. However, the EPA has not consistently implemented this part of its mandate; indeed, secrecy is pervasive in chemicals regulation.”); Lyndon & Levine, BLM Trade Secrets Comment, supra note 37, at 1 (“[T]he [BLM] Regulations would allow entities engaged in hydraulic fracturing to withhold purported chemical information trade secrets from the BLM, and by extension, the public.”).
public database of hazardous chemicals and wastes the regulator compiles.”  

“The regulator, not the company, determines if chemicals can be kept from public view as a trade secret”—and the EPA chose secrecy.  

BLM too: In 2015, BLM promulgated a rule that promised to begin public disclosures of the chemicals in fracking fluids, but the rule was challenged by fossil fuel industry groups and then rescinded under President Trump before the agency disclosed any secret formulas. President Biden has not reinstated the rule.

Relatedly, under the Trump administration, multiple federal regulators that had historically cultivated important proactive disclosure programs ended them. As of writing, most of these disclosure programs have not been revived under President Biden.

For example, for decades, the USDA disclosed inspection reports compiled by the Animal and Plant Health Inspection Service (APHIS). These reports documented mistreatment and death of animals in research laboratories, zoos, equestrian centers, and other businesses that rely on animals. In 2017, the USDA removed all such reports from its website, reportedly under pressure from businesses that had been criticized and lost business after disclosures of abuse. In 2020, after animal welfare groups “filed several lawsuits aimed at forcing the agency to restore the records” and successfully lobbied Congress to bring back a public database of the reports, USDA restored these reports to its website and added updated records.

Similarly, for decades the FDA maintained a program in which, upon approval of a new drug or vaccine, it disclosed detailed “reviews” prepared by its expert scientists that summarized the product’s therapeutic, chemical, and


135 Id.


138 Id.

other properties for the public. In July 2019, the FDA announced that it will cease posting complete reviews and instead make public only a single condensed “integrated review.” The FDA’s shift to less information-rich, more “integrated” reviews was welcomed by many in the industry but criticized by dozens of academics (including me), who observed that it would “deprive researchers . . . of valuable information and data” otherwise inaccessible to the public.

Around the same time, the FDA retreated from other nascent agency efforts at proactive disclosure of information of public interest. It abandoned one initiative to share agency-generated analyses, so-called Complete Response Letters, that illuminate the safety and efficacy data on not-yet-approved drugs and abandoned a second initiative to publicize near-complete Clinical Study Reports (CSR) that would have provided a detailed look at important clinical trials on FDA-approved drugs. Medical researchers and consumer watchdog groups such as Public Citizen had advocated these disclosure programs for years and lamented the FDA’s retreats. But the pharmaceutical industry cheered. One of the two leading

140 See Matthew Herder, Christopher J. Morten & Peter Doshi, Integrated Drug Reviews at the US Food and Drug Administration—Legal Concerns and Knowledge Lost, 180 JAMA INTERNAL MED. 629, 629 (2020) (describing the benefits of the antecedent review process).

141 See id. (“The disciplines will collectively generate an integrated review—a ‘collaborative document with input from clinical, clinical pharmacology, biostatistics, toxicology reviewers, and other disciplines based upon the issues raised by the application.’” (internal citations omitted)).


144 See Nick Paul Taylor, FDA Chief Gottlieb Backs Away from Plan to Publish CRLs, FIERCEPHARMA (Jan. 17, 2018), https://www.fiercebiotech.com/biotech/fda-chief-gottlieb-backs-away-from-plan-to-publish-crls [https://perma.cc/DG4X-GMAT] (“Researchers, investors and other interested parties rely on the honesty and transparency of the companies that receive CRLs to learn why a drug was rejected by the FDA”).


pharma industry trade organizations had expressed “serious concerns” with the FDA’s rescinded plan to publicize CSRs, alleging (unsubstantiated) incompatibility “with global disclosure and data protection policies.”147 The other leading trade organization similarly contended that the same rescinded plan had threatened “commercially confidential information” necessary “to protect a Sponsors’ intellectual property rights and further commercial development.”148

Graves and Katyal document additional vivid examples of federal regulators withholding information despite public outcry, such as the EPA’s refusal to share data on Teflon.149 In short, regulators’ current programs for proactive disclosure of corporate secrets of public interest within their possession are important but scattered.

The apparent trend away from proactive public disclosure of corporate secrets has occurred even as the U.S. government has committed itself to increasing levels of “open government” and “open data.”150 Over the past two decades, major federal initiatives along these lines, such as the Obama Administration’s Open Government Initiative151 and 2019’s OPEN Government Data Act,152 have expanded public access to some forms of data held by the U.S. government. Much of this data is not just generated by the government but is about its very operation, providing information on the U.S. government’s own spending and performance in areas such as health, education, and climate policy. Through such various open government initiatives, the U.S. government has arguably made itself more open to public

FDA must join the EMA and Health Canada in allowing the public to know when a drug is deemed unsafe or ineffective for a certain use.”).

147 PhRMA Comment, supra note 142, at 4.
148 BIO Comment, supra note 142, at 7.
149 Graves & Katyal, supra note 31, at 1355 n.57.
152 OPEN Government Data Act, Pub. L. No. 115-435, 132 Stat. 5529, 5534-44 (“[Agencies must provide] a point of contact within the agency to assist the public and to respond to quality issues, usability issues, recommendations for improvements, and complaints about adherence to open data requirements”).
Publicizing Corporate Secrets

C. The Public Has No Good Alternatives

The preceding subpart showed that today’s federal regulators do not maintain consistent or effective proactive disclosure programs to share secret information on corporate activity, even when it is of major public interest. As a result, the public often turns to “self-help.” That is, journalists, consumer organizations, activists, academics, and other interested citizens try to obtain pertinent information on corporate conduct with other tools.

But those tools are inadequate. The most prominent such tool—FOIA—suffers from deep structural problems and is today very difficult to use to obtain information on corporate conduct. Other tools, including disclosure by state-level regulators, disclosures in litigation, and reliance on individual whistleblowers “on the inside,” are likewise inadequate. These inadequacies underscore the need for substantially expanded proactive disclosure by federal regulators—the “information publicity” that this paper proposes in detail in Part II.

1. FOIA Is Broken

On its face, FOIA seems the perfect tool for members of the public to obtain information from federal regulators. FOIA ostensibly requires any federal agency subject to FOIA to make information—“records”—within its possession “promptly available” to “any person” who requests it.154 FOIA makes disclosure the default rule, though it carves out nine seemingly narrow categories of information as exempt from the presumption of disclosure.

Yet, in reality, FOIA has four key flaws.155 First, FOIA requests are reactive and require the requester to know precisely what information she needs before she asks.156 Second, FOIA requests are slow, sometimes taking years to produce the documents the requester seeks.157 Third, FOIA requests are resource-intensive for requesters, often requiring sophisticated and expensive legal help.158 Fourth, FOIA requests are highly deferential to

---

153 See generally Pozen, supra note 55; see also Kapczynski, supra note 27. As Pozen, Kapczynski, and others have argued, it’s no surprise to see these two trends occur together; transparency has been weaponized as a tool against the state.
155 Kapczynski and I described these at greater length in a recent paper. Morten & Kapczynski, supra note 54, at 520.
156 Id.
157 Id. at 521.
158 Id.
industry; agencies can and do legally withhold information that regulated entities ask the agencies to keep secret.\footnote{Id. at 522.}

Today, FOIA offices throughout the federal administrative state are overwhelmed with requests. Kwoka has calculated that in just 2013 and 2014, federal agencies received over 700,000 FOIA requests.\footnote{Margaret B. Kwoka, FOIA, Inc., 65 DUKE L.J. 1361, 1364 (2016).} The average FOIA request takes months to fulfill, and complex requests often linger for years.\footnote{Id. at 1374-75 ("The average processing time across the entire federal government for complex FOIA requests is a staggering 118 days . . . . At the end of FY 2014, the oldest pending requests across the federal government dated back to 1993."); see also Morton & Kapczynski, supra note 54, at 521 (detailing long processing time).}

One vivid example: in response to a 2021 FOIA request for copious data on Pfizer’s COVID-19 vaccine, FDA’s lawyers asked a court to allow fifty-five years to fulfill it.\footnote{Jenna Greene, Wait What? FDA Wants 55 Years to Process FOIA Request over Vaccine Data, REUTERS (Nov. 18, 2021, 4:31 PM), https://www.reuters.com/legal/government/wait-what-fda-wants-55-years-process-foia-request-over-vaccine-data-2021-11-18 [https://perma.cc/T4R9-DMHR].} The never-ending flood of requests to federal regulators comes mostly from commercial users—often public corporations—using FOIA to gather “[c]ompetitive [i]ntelligence” on the regulator’s plans as well as their direct competitors.\footnote{See Kwoka, supra note 160, at 1393-94 (noting the high number of commercial FOIA requests by companies such as Thomson Reuters). See also Margaret B. Kwoka, Inside FOIA, Inc., 126 YALE L.J.F. 265, 266 (2016) ("[T]he majority of requests at some agencies are made by commercial requesters. These agencies include large regulatory agencies . . . ."); Pozen, supra note 55, at 125 (describing capture of FOIA and other transparency programs by commercial users).}

Each FOIA request requires a bespoke response, even if numerous requesters seek the same types of information repeatedly. The result is enormous burden on federal agencies. As Kwoka has described, “agencies spend millions—and sometimes tens of millions—of dollars processing FOIA requests, and recoup very little of the costs through fees paid by requesters, even commercial requesters.”\footnote{Kwoka, supra note 164, at 267.} The FDA alone spent over $300 million responding to FOIA requests between 2008 and 2017.\footnote{Alexander C. Egilman, Joshua D. Wallach, Christopher J. Morten, Peter Lurie & Joseph S. Ross, Systematic Overview of Freedom of Information Act Requests to the Department of Health and Human Services from 2008 to 2017, 4 R Sch. INTEGRITY & PEER REV. 26, 4 (2019).}

Given the backlog and burden of responding to FOIA requests, agencies have understandable incentives to offload some of the work. When a FOIA request seeks information submitted by a third party, agencies have a perfect excuse to offload—in fact, a legal obligation to do so. Pursuant to a Reagan-era executive order, No. 12,600,\footnote{Exec. Order No. 12,600, 52 Fed. Reg. 23,781 (Jun. 25, 1987).} that has since been encoded into ubiquitous
regulations, federal regulators must notify a regulated entity before disclosing, to a FOIA requester, information designated confidential by that entity. The effect is that regulated entities typically get a first cut at proposing what to disclose and what to withhold. Regulated entities have exploited this procedure to claim massive swaths of information as withholdable under FOIA. One of FOIA’s statutory exemptions, Exemption 4, permits an agency to withhold not just trade secrets but the broader category of confidential commercial information (CCI) from FOIA requesters. The category of CCI has always been broad, and thus problematic for FOIA requesters. But in 2019, the Supreme Court made a bad situation even worse. As Deepa Varadarajan has described, the Court’s Food Marketing Institute v. Argus Leader Media decision dramatically “expand[ed] the private sector’s ability to shield information provided to the government from disclosure.” “Upending four decades of circuit court precedent, the Court held that information can be withheld from FOIA disclosure as ‘confidential’ so long as the submitter . . . treats it as private”—without requiring anything more. The early evidence we have on the effects of Food Marketing Institute indicate that federal agencies are using the decision to defer more than ever to industry—and thus keeping more corporate secrets than ever from FOIA requesters.

2. The Public Lacks Other Good Tools

If FOIA is broken, does the public have other tools to obtain corporate secrets of vital public interest? In short, no. Here I will briefly describe three alternatives to FOIA and explain why they too are inadequate.

State governments regulate the same industries that the U.S. government does. That begs the question of whether requests made under state public records laws could fill the gap left by FOIA. That is undoubtedly true in some cases. But Christina Koningisor has shown that state public records requests

167 See, e.g., 21 C.F.R. § 20.61(e)(1) (2021) (requiring the FDA to make reasonable efforts to notify the submitter of any FOIA requests for secret information that may contain trade secrets or CCI and giving the submitter an opportunity to submit objections to disclosure).
169 See Deepa Varadarajan, Business Secrecy Expansion and FOIA, 68 UCLA L. REV. 462, 466 (2021) (discussing how the broad right of access provided by FOIA is subject to certain constraints to balance the public’s right to know with other governmental and private interests).
170 Id. at 500.
171 Id. at 516.
172 See id. at 499–500 (describing cases in which district courts have described plaintiffs’ burden as harder to meet and noted changes in agency withholding behavior after Food Marketing Institute).
tend to be even more difficult than federal FOIA requests, and state agencies even more secretive.\textsuperscript{173}

As another alternative, civil and criminal litigation can provide invaluable, otherwise secret information on corporate activity that threatens public health and other interests.\textsuperscript{174} For example, tort litigation has for decades unearthed otherwise secret information on the safety and efficacy of medical products.\textsuperscript{175} However, information via litigation is no systemic solution. Litigation is rare and slow. Information on troubling corporate conduct may not emerge for years or even decades.\textsuperscript{176} And overprotection of trade secrets is a problem for courts just as it is for agencies. For example, Rebecca Wexler has documented how overbroad exercise of the trade secret privilege in criminal cases has stymied disclosure of information on technologies used by law enforcement, including DNA-matching and facial recognition software.\textsuperscript{177} A team of investigative journalists at Reuters has shown that judges’ negligent sealing of information alleged to be trade secrets (but often not actually trade secrets) hid, for decades, everything from the extent of opioid abuse

\textsuperscript{173} See Christina Koningisor, \textit{Transparency Deserts}, 114 NW. L. REV. 1461, 1534 (2020) (concluding that a review of state public records laws suggests that local governments have fewer resources, and that barriers to disclosure are steeper for the public); see also Christina Koningisor, \textit{Secrecy Creep}, 169 U. PA. L. REV. 1751, 1758 (2021) (“State and local governments are not monitored by the same internal and external systems of checks and balances, and these secrecy tools allow state and local officials to aggregate power while shielded from public view.”).


\textsuperscript{175} See Christopher J. Morten, Aaron S. Kesselheim & Joseph S. Ross, \textit{The Supreme Court’s Latest Ruling on Drug Liability and Its Implications for Future Failure-to-Warn Litigation}, 47 J.L. MED. & ETHICS 783, 783, 785 (2019) (“For decades, the litigation discovery process, in which plaintiffs commonly receive access to millions of pages of internal drug company documents, has revealed important new information on the benefits and risks of many drug products.”).

\textsuperscript{176} See, e.g., Egilman et al., \textit{Confidentiality Orders and Public Interest in Drug and Medical Device Litigation}, supra note 174, at 292 (“STAT and other news organizations convinced courts to allow the public to see documents that shed light on the improper marketing of opioids that were given to state and private attorneys several years earlier but that had been held secret under court order.”).

knowingly fueled by prescription drug manufacturers\textsuperscript{178} to the deadly rollover risk of General Motors’ SUVs.\textsuperscript{179}

Like litigation, individual whistleblowers also provide a vital stream of information on illegal corporate activity. Think, for example, of the Theranos employees, Erika Cheung and Tyler Shultz, who bravely informed CMS and the media of improprieties in Theranos’s blood testing laboratories.\textsuperscript{180} However, reliance on individual employees to blow the whistle on dangerous corporate activity is no structural solution. In addition, existing whistleblower laws in the United States provide employees with insufficient incentives and protections.\textsuperscript{181} Those same Theranos employees, Cheung and Shultz, faced intense legal threat from Theranos’s lawyers and incurred substantial financial losses and stress as a result of their decision to divulge Theranos’s secrets in this way.\textsuperscript{182} As Katyal and Graves have explained, “[d]espite recent legal protections for whistleblowers, secrecy can still remain paramount, harming the public interest in exposing wrongdoing.”\textsuperscript{183}

That leaves federal regulators’ information publicity abilities as our best hope.


\textsuperscript{181} See Graves & Katyal, supra note 31, at 1167 (“[D]espite the DTSA, employers have continued to bring state law trade secret misappropriation claims against whistleblower employees, again with mixed success.”); see also Lauren Rogal, \textit{Secrets, Lies, and Lessons from the Theranos Scandal}, 72 \textit{HASTINGS L.J.} 1663, 1695-96 (2021) (arguing that the inaccessibility and uncertainty of whistleblowing protections for workers tilts the balance of incentives against whistleblowing); Deepa Varadarajan, \textit{The Uses of IP Misuse}, 68 \textit{EMORY L.J.} 739, 781-83 (2019) (detailing weaknesses of protections for whistleblowing speech in the Defend Trade Secrets Act); Evan J. Ballan, \textit{Note, Protecting Whistleblowing (and Not Just Whistleblowers)}, 116 \textit{MICH. L. REV.} 475, 495-97 (2017) (arguing that the federal False Claims Act provides insufficient protections to whistleblowers who challenge potential fraud); Aaron S. Kesselheim, David M. Studdert & Michelle M. Mello, \textit{Whistle-Blowers’ Experiences in Fraud Litigation Against Pharmaceutical Companies}, 362 \textit{NEW ENG. J. MED.} 1832, 1836 (2010) (summarizing the experiences of “insider” whistleblowers who reported fraud committed by their pharmaceutical company employers, including job loss and financial ruin for some).

\textsuperscript{182} See CARREYROU, \textit{BAD BLOOD}, supra note 119, at 247, 255 (describing how private investigators surveilled both Shultz and Cheung, and how Theranos’s counsel threatened to bankrupt Shultz’s entire family and sent Cheung a cease-and-desist letter threatening legal action).

\textsuperscript{183} Graves & Katyal, supra note 31, at 1365.
II. THE WHY AND HOW OF PUBLICIZING CORPORATE SECRETS

Part I described the unsatisfactory, even dangerous, status quo we live under. Despite holding some of the world's largest reservoirs of information concerning public health and safety, environmental safety, and other matters of vital public interest, U.S. federal regulatory agencies disclose little. Regulators disclose little even though sharing some of these secrets may be more vital than ever to protect public health and safety, the environment, consumer welfare, labor rights, and democracy itself. Where do we, as a country, go from here?

In this Part, I propose a solution, or at least a step toward one. That step is “information publicity,” to inform, enrich, and protect the public. This proposal is this article’s main normative contribution: a new theory of how administrative agencies should govern information and disseminate it to the public. I argue in this Part that the federal regulatory state can and should undertake a comprehensive, intentional program of information publicity—controlled, bounded disclosure of corporate secrets to the public, including secrets that merit the legal protections of trade secrecy.

I build this theory in three subparts. First, in subpart II.A, I show that when agencies elect to disclose information proactively, they are free to control who gets access to the information and on what terms. This feature of proactive information disclosure distinguishes it from reactive disclosures to FOIA requesters, which, by statute, must be made unconditionally, to all requesters.

Given this feature, I then argue in subpart II.B that federal regulators should cultivate bounded “gardens” of secret corporate information, accessible to only to trustworthy users and then only on the regulators’ terms. That is, federal regulators can and should provide moderated access to corporate secrets subject to both legal and technical limits, which dictate which users get access and constrict the uses those users make of that information. This is “information publicity,” distinct from blunt, unfettered information disclosure. By bounding information gardens carefully, federal regulators can foster uses that maximize public benefit and prevent, or at least discourage, those uses of commercially valuable secret information that would most harm the sources of this information. In fact, successful proof-of-concept models for these agency-moderated bounded gardens of information already exist. A handful of federal agencies in the U.S. and Canada have quietly pioneered programs of what are—in substance if not in name—information publicity: they constrain access and use of valuable agency-held information through contract law, technical limits on information access, and other bounds.
Subpart II.C proposes a procedural framework for agencies to set those boundaries. Balancing the potential benefits of (controlled) disclosure against its harms can be difficult, but there are procedures an agency can employ to gather relevant information and make wise choices.

Part II focuses on what I believe agencies should do with corporate secrets of public interest. The next part, Part III, “shows my work.” That is, Part III explains why the proposals of Part II are legal under existing law—even when the corporate secrets to be publicized are bona fide trade secrets.

A. Escaping the Secrecy/Disclosure Dichotomy

A simple but important legal insight forms the basis of this article’s information publicity proposal: when federal agencies disclose information proactively, they set the rules of that disclosure—when, to whom, and on what terms.

This insight may seem trivial or self-evident to some readers. The insight is stated plainly in some basic treatises on administrative and information law. As James O’Reilly’s Federal Information Disclosure puts it,

[E]xcept where Congress actually mandated withholding . . . , [an] agency has very broad discretionary choices [about disclosure] . . . . Agencies can publish, place on their websites or otherwise disseminate any document that is not required to be withheld under another statutory requirement.184

But others will be surprised to learn that federal agencies make their own rules when they disclose information proactively. The same O’Reilly treatise characterizes this key insight as “a crucial fact, often overlooked.”185 How did it come to be overlooked? Perhaps because of the dismal history told in Part I. Part I showed that the federal regulatory state’s proactive disclosure programs are scattered and limited, and that FOIA, flawed as it is, is today the dominant means by which the public obtains information from federal regulators. FOIA’s dominance may have fueled a mistaken perception among scholars, information users, and even agencies themselves that all information disclosure by federal agencies must proceed via FOIA request, or must follow the procedures of FOIA.186

185 Id.
Under FOIA, disclosure is reactive, unfettered, decontextualized, and blunt. Under FOIA’s standard process for disclosure, an agency waits for a FOIA request to come in and then conducts a responsive search, gathers relevant records, and determines whether it has a legal basis to redact or withhold them. By FOIA’s express statutory text, any information for which the agency lacks a legal basis to redact or withhold must be disclosed without restriction or condition. That is, if no exemption or exclusion applies to a piece of information, the agency must disclose it to any and all who request it, regardless of who the requester is or how they plan to use it.187 FOIA treats all requesters equally, with minor exceptions.188 That means FOIA treats public interest groups that intend no commercial use of information they obtain as if they were direct competitors of the source of a corporate secret.189 As the DOJ put it in 2009, “Neither the willingness of the requester to restrict circulation of the information nor a claim by the requester that it is not a competitor of the submitter should logically” bear on the question of whether to disclose or withhold.190 “The question is whether ‘public disclosure’ would cause harm; there is no ‘middle ground between disclosure and nondisclosure.’”191 Faced with FOIA’s all-or-nothing, dichotomistic choice between total secrecy and total disclosure, courts and agencies alike have

187 5 U.S.C. § 552(a)(3)(A); see also David E. Pozen, Freedom of Info. Beyond the Freedom of Info. Act, 165 U. Pa. L. Rev. 1097, 1100-04 (2017) (discussing FOIA’s decontextualized quality); Kwoka, FOIA, Inc., supra note 160, at 1372-78 (summarizing the FOIA request process and challenges journalists face with FOIA requests); Morten & Kapczynski, supra note 54, at 520 (“FOIA generally requires a federal agency to make information—‘records’—within its possession ‘promptly available’ to ‘any person’ who requests that information.”); cf. Schiffer v. FBI, 78 F.3d 1405, 1411 (9th Cir. 1996) (holding that a federal agency cannot use a protective order to constrain a FOIA requester’s use of information received pursuant to a FOIA request).

188 By statute, agencies subject to FOIA must offer fee waivers and expedited processing to some requesters. See 5 U.S.C. § 552(a)(4)(A), (a)(6)(E). In practice, noncommercial, public-spirited FOIA requesters regularly get fee waivers, but expedited processing is granted in fewer cases. See, e.g., Mark. H. Grunewald, E-FOIA and the "Mother of All Complaints:" Information Delivery and Delay Reduction, 50 ADMIN. L. REV. 345, 364 (1997) (noting that the “vast majority” of FOIA cases “do not meet the standard” for expedited processing). Neither fee waivers nor expedited processing affect the ultimate level of access the FOIA requester receives.

189 See, e.g., Pub. Citizen Health Rsch. Grp. v. FDA, 185 F.3d 898, 904 (D.C. Cir. 1999) (explaining the Supreme Court has been clear that the identity of the requester does not bear on whether disclosure of a document is warranted). But see id. at 908-10 (Garland, J., concurring) (reasoning that FOIA does authorize agencies and courts to weigh whether a FOIA requester’s use of information will benefit the public in their determination of whether the FOIA exemption protecting trade secrets and CCI applies); GC Micro Corp. v. Def. Logistics Agency, 33 F.3d 1109, 1115 (9th Cir. 1994) (same).

190 DEPT’ OF JUST., DEPT’ OF JUST. GUIDE TO THE FREEDOM OF INFO. ACT: EXEMPTION 4 (2004).

reason to err on the side of caution and keep secret any secret information that has even an iota of potential commercial value to competitors.

Proactive disclosure of information by federal agencies is appealing in significant part because it offers a way to escape FOIA’s blunt choice between total disclosure and total secrecy. When disclosing information proactively, agencies have “very broad discretionary choices” about when, how, and to whom to disclose. Unlike with FOIA requests, when making proactive disclosures, agencies are free to ask who will use the information, and how, and to limit disclosure accordingly. Agencies can, for example, selectively publicize information—permitting and encouraging certain uses of information by certain members of the public, in ways that simultaneously protect the information’s integrity and serve the public interest—rather than bluntly disclosing the information unconditionally.

Privacy scholars have mounted similar descriptions and critiques of once-dominant, blunt and dichotomistic views of personal privacy and the purposes of privacy law. Solove, Nissenbaum, and Woodrow Hartzog are among the prominent scholars here. They have shown that, in privacy law, absolutist thinking about information as either entirely “public” or entirely “private” occluded, for decades, deeper questions about just how broadly individuals’ personal information is and should be shared, with whom, in what contexts, and with what restrictions. For example, two decades ago, Solove convincingly critiqued the blunt and “outmoded” way that privacy “law often treats information in this black-and-white manner; either it is

192 O’Reilly, supra note 184, at § 9:11. See Part III for more.
195 See Woodrow Hartzog, The Public Information Fallacy, 99 B.U. L. REV. 459, 518-20 (2019) (“[T]he question of what is public is often just the threshold line that is drawn somewhere on the spectrum of things that range from completely obscure to totally obvious or known . . . . [H]e privacy law, it seems, is often content to treat disclosures to anyone outside of narrowly prescribed, formalized confidential relationships as ‘public.’”).
wholly private or wholly public.” The way forward for privacy law, argued Solove, was to “abandon the secrecy paradigm” and create gradated, context-specific “control over and limitations on certain uses of information, even if the information is not concealed” entirely. In parallel, Nissenbaum developed the concept of “contextual integrity” and a related framework for understanding and protecting the privacy of personal information. Under Nissenbaum’s framework, “private” information need not be kept purely secret; it remains private—its integrity remains intact—so long as context-relative informational norms are respected. To quote Nissenbaum, “[u]sually, when we mind that information about us is shared, we mind not simply that it is being shared but that it is shared in the wrong ways and with inappropriate others.”

My critique of FOIA’s dominant model of disclosure and its grip on our imaginations is inspired by these critiques of privacy law. In my view, the administrative law of corporate secrets is overdue for precisely the sort of shake-up that privacy scholars accomplished. The next Subpart details my proposal for “information publicity” for corporate secrets—proactive, controlled sharing of corporate secrets by federal agencies with the public in a way that escapes the secrecy/disclosure dichotomy.

B. Cultivating Bounded “Gardens” of Public Information

How should federal regulators exercise their power to disclose corporate secrets? In my view, they should take advantage of the flexibility of discretionary proactive information disclosure to cultivate protected, bounded “gardens” of corporate secrets. Within these gardens, information becomes accessible to select members of the public only on the regulators’ terms. That is, federal regulators can and should provide moderated access to corporate secrets subject to both legal and technical limits that constrict what information users get access to and what uses those users make of that

196 Solove, Access and Aggregation, supra note 55, at 1177.
197 Id. at 1178.
198 See Nissenbaum, Privacy as Contextual Integrity, supra note 194, at 124-25 (introducing the “contextual integrity” analysis).
199 See Nissenbaum, PRIVACY IN CONTEXT, supra note 194, at 140 (explaining informational norms, context-relative informational norms, and contextual integrity).
200 Id. at 142.
201 Again, this paper is not the first to observe conceptual links between trade secrecy and privacy law. See, e.g., Samuelson, Privacy as Intellectual Property?, supra note 60, at 1151-52 (explaining three commonalities between trade secrecy and information privacy laws); Sandeen, Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law, supra note 60, at 673-692 (showing that the two fields share common doctrinal roots). Sandeen has also analyzed the distinct concepts of “disclosure” in trade secret, patent, and copyright law. Sharon K. Sandeen, A Typology of Disclosure, 54 AKRON L. REV. 657, 667 (2021).
information. This is “information publicity,” distinct from blunt, unfettered information disclosure. This Section argues that by bounding these public gardens carefully, federal regulators can foster uses that maximize public benefit and simultaneously prevent, or at least discourage, uses of commercially valuable secret information that would most harm the sources of this information.

Later in this Section, I show that we already have working proof-of-concept models for agency-cultivated bounded gardens of information. Under the radar of most scholars, numerous federal agencies have quietly pioneered programs of what are, in effect, information publicity, with access and use of valuable agency-held information effectively constrained through contract and technical controls.

1. The Theory of Bounded Gardens of Corporate Secrets

Why information publicity through “bounded gardens” of information? In short, the goal of bounded gardens is to minimize harm inflicted on the source of the relevant corporate secret while simultaneously maximizing socially beneficial uses. Agencies can achieve both goals at once because there is a beneficial mismatch between the uses of corporate secrets most harmful to their sources and uses that most public interest groups, researchers, and other members of the public wish to make of the information. In other words, there are many socially valuable ways the public can use a corporate secret that do not destroy the economic value of the secret. The economic value of the trade secret endures even though the secret is no longer entirely secret.

What are the socially beneficial, noncommercial uses I propose be made of corporate secrets? Blowing the whistle on unsafe products and services to protect public health and safety or the environment? Exposing discriminatory or exploitative treatment of workers? Conducting novel secondary scientific research on industry-generated data sets? Informing the public about new developments in science and technology? Simply expanding public knowledge of (and thus democratic oversight of) regulated industries? Rebalancing, even in a limited way, some of the growing imbalance of information between private companies and the broader American public? Opening regulators themselves to greater public scrutiny, perhaps as a gesture to rebuild public trust?

The answer to all these questions is “yes.” My goal in this paper is not to advance a single vision of the “public good” or an omniscient theory of when private secrets should be publicized. (I have neither.) Instead, my goal is to reopen a political debate over when and how federal agencies should wield their largely dormant but powerful authority over information. In my view,
federal regulators themselves have not just power but unique competence to determine how information should be publicized.

Though overlooked today, dissemination of information has been a central part of federal regulators’ mission and expertise since the dawn of the federal regulatory state in the Progressive Era. Regulators then emphasized the very same concept of “publicity” that this paper proposes—context-sensitive information disclosure by public agencies, intended to privilege noncommercial uses over commercial ones. As David Pozen has described, “[f]or American progressives at the turn of the twentieth century, the call for new laws mandating [regulatory] ‘publicity’ was tied to a reform agenda that aimed to limit the influence of big business and to produce more efficient, scientific, and democratically accountable regulation.”202 From that origin, regulatory “publicity” has always been distinct from mere disclosure. Publicity has always emphasized selective, contextual disclosure to particular audiences to serve particular goals and values within the agency’s ambit.203 In the 20th Century, regulators collected secret information from industry and then disseminated and contextualized it, at turns warning, outraging, teaching, and “improving” the public, and helping, over time, to form democratic competence and will.204 Empowering the public to use information effectively was an essential function of the federal regulatory state, especially in fields of industry and activity where information is complex, new, or fast-changing, as was (and is) the case with technology industries.205 (Recall the Winthrop Chemical example told in the Introduction, wherein the FDA not only warned the public away from a

202 Pozen, Transparency’s Ideological Drift, supra note 53, at 108.
203 See id. at 113-14 (“Exposing the inner workings of institutions was not an end in itself, but rather a precondition for new modes of responsive regulation and democratic action. As attested by the introduction of the secret ballot and by Brandeis’s own efforts to establish a right to privacy, progressives were willing to trade certain forms of openness for opacity where the risks to principled decision making or other values seemed too severe.”).
204 Id.; see also Matthew Herder, Denaturalizing Transparency in Drug Regulation, 8 MCGILL J. L. & HEALTH 57, S61 (2015) (explaining the progressive tradition of “publicity” in Canadian consumer protection law in the late 19th and early 20th Centuries).
205 See Pozen, Transparency’s Ideological Drift, supra note 55, at 102, 113-14 (describing how Progressives used publicity to promote economic fairness during the advances of the Gilded Age); Herder, Denaturalizing Transparency, supra note 205, at S61 (explaining the importance of publicity for Canadian federal regulation of food and drug technologies). For more examples of effective “publicity” in action, see generally Kapczynski, Dangerous Times, supra note 27, at 2359; Bradley C. Karkkainen, Bottlenecks and Baselines: Tackling Information Deficits in Environmental Regulation, 86 TEX. L. REV. 1409, 1411 (2008) (explaining that environmental regulation typically “place[s] the burden of acquiring or producing information, and then managing, analyzing, and evaluating that information, on the government—more particularly, on the responsible regulatory or resource-management agencies”); Mary L. Lyndon, Information Economics and Chemical Toxicity: Designing Laws to Produce and Use Data, 87 MICH. L. REV. 1795, 1810 (1989) (explaining the challenges of publicity for chemical toxicity data).
specific unsafe product but educated a then-nascent industry about safe manufacturing.) Effective information publicity spurred and ensured effective legislation, substantive regulation, and democratic oversight of industry and government alike.206 As Brandeis wrote, a century ago, regulators’ “publicity” can be “a remedy for social and industrial diseases.”207

The question of how, exactly, today’s agencies should revive their authority to publicize corporate secrets is a complex factual and legal question, and certainly not an easy one. But in innumerable other contexts, these same regulators routinely generate, gather, and analyze factually complex evidence, solicit feedback from fractious stakeholders, and then make difficult choices. Such questions are exactly the sort that our political and legal system traditionally delegates to administrative agencies because of their unique expertise and structure208—and, indeed, a close look at many regulators’ enabling statutes shows that Congress expressly empowered these agencies to ask and answer questions about whether and how to disseminate secret information.209 The question of how agencies should wield their information publicity power is also a quintessential political question, suitable for contestation by our country’s democratic process, messy and fragile as it is. Regulators are at least somewhat democratically accountable; presidents whose regulators err too far on the side of secrecy or disclosure may lose

206 See Pozen, Transparency’s Ideological Drift, supra note 55, at 108-14 (highlighting the effects of effective publicity information).


208 See, e.g., Pharm. Mfrs. Ass’n v. Weinberger, 401 F. Supp. 444, 446 (D.D.C. 1975) (acknowledging that FDA has “special expertise and administrative experience” in interpreting its own enabling statutes and determining the proper contours of its own disclosure authority).

209 See, e.g., 7 U.S.C. § 136h(d)(2) (provision of FIFRA specifying that EPA may collect information on pesticides, including information “entitled to confidential treatment,” and then, at its discretion, disclose it publicly “in connection with a public proceeding to determine whether a pesticide, or any ingredient of a pesticide, causes unreasonable adverse effects on health or the environment, if the [EPA] Administrator determines that such disclosure is necessary in the public interest.”); 12 U.S.C. § 5512 (authorizing the Consumer Financial Protection Bureau to obtain secret information from the consumer finance industry and then “make public such information obtained by the Bureau under this section as is in the public interest,” pursuant to the agency’s own rules on confidentiality); 42 U.S.C. § 282(j)(3)(D) (provision of the Food and Drug Administration Amendments Act (FDAAA) of 2007 granting broad authority to the National Institutes of Health (NIH) to define an “expanded” set of information on clinical trials, mandate its submission to NIH by companies, universities, and other entities that run clinical trials, and then disseminate that information to the public, “[t]o provide more complete results information and to enhance patient access to and understanding of the results of clinical trials”); 49 U.S.C. § 40123 (provision of the Federal Aviation Reauthorization Act of 1996 specifying that FAA should withhold “safety or security related information” only if “withholding such information from disclosure would be consistent with the Administrator’s safety and security responsibilities”). For more examples, see infra subsection III.B.1.
popular support. (Consider that in the wake of the George W. Bush administration—widely perceived as secretive210—Obama won the presidency on a platform that promised, among much else, “increasing public access to information,” including a specific proposal to “conduct regulatory agency business in public.”211) In short, the question of what precise goals publicity of corporate secrets should serve is a question I think best left to the agencies.

Having said something about the intended benefits of publicity of corporate secrets, what about its harms? Compared to publicity’s benefits, publicity’s potential harms are simpler to define: in short, the legally and normatively relevant harm is use by competitors. The dominant theoretical justifications for legal protection of trade secrets212 are that protection incentivizes the creation of socially valuable inventions, discourage overprotection of these inventions through actual secrecy, and promote “ethical competition.”213 All these justifications for trade secrecy law focus on mediation of relationships among existing and potential commercial competitors, and more specifically on protecting the rightful holder of commercially valuable information from misappropriation.214 Thus, the core harm that trade secrecy law seeks to avert is competitive use of the information by a competitor of the holder of the trade secret. When

---

210 See Clint Hendler, What We Didn’t Know Has Hurt Us, COLUM. JOURNALISM REV. (Feb. 2009), https://archives.cjr.org/feature/what_we_didnt_know_has_hurt_us.php ("The [George W.] Bush administration was pathological about secrecy.").


212 And related categories of information, such as CCI.

213 See Mark A. Lemley, The Surprising Virtues of Treating Trade Secrets as IP Rights, 61 STAN. L. REV. 311, 313 (2008) (arguing that trade secrets are intellectual property that must be protected to encourage invention); Michael Risch, Why Do We Have Trade Secrets?, 11 MARQ. INTELL. PROP. L. REV. 1, 4 (2007) (describing four theories to justify trade secret laws); Michael Risch, Trade Secret Law and Information Development Incentives (analyzing the effect of trade secret law on incentives to innovate), in THE LAW AND THEORY OF TRADE SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH 154 (Rochelle C. Dreyfuss & Katherine J. Strandburg, eds., 2009); Kapczynski, The Public History of Trade Secrets, supra note 89, at 1390-91 (providing a historical account of the justifications for trade secret law); Robert G. Bone, The (Still) Shaky Foundations of Trade Secret Law, 92 TEX. L. REV. 1803, 1806 (2014) (describing how trade secret laws are justified based on claims they promote incentives to create and prevent wasteful precautions).

214 See Sandeen, Relative Privacy, supra note 60, at 698 (explaining the importance of relationships in trade secrecy law); Sandeen, Out of Thin Air, supra note 62, at 366, 371-72 (similar) ("If information meets the legal definition of a trade secret, then it might be protected against ‘misappropriation’, but trade secret protection ends when the information becomes generally known or readily ascertainable"); Kapczynski, The Public History of Trade Secrets, supra note 89, at 1380, 1395 (explaining trade secret law prevents using commercial information in violation of a duty of confidence or gained through improper means).
publicizing corporate secrets, regulators can and should seek to avert this core harm.

Happily, the primary uses of corporate secrets that members and representatives of the public—consumer watchdogs, environmental and labor groups, academic researchers, patient activists, and so on—make are usually noncommercial and almost always noncompetitive. These people and groups typically have no interest in competing with the company that is the source of a given corporate secret. Instead, they typically seek to investigate and inform the public about features of the company’s products and services, and often focus on harms—poisoned water, toxic drugs, erratic autonomous vehicles, racial discrimination against employees or customers, and so on.

Of course, if researchers use a corporate secret to establish and publicize a product’s harm, the product’s maker may lose business. Yet any diminution in profits that follows the revelation that a company’s products or services are unsafe, or that its business practices are unsavory, is not the “competitive” harm that trade secrecy law intends to prevent, nor is it the sort of harm that any part of our law seeks to prevent. As the Supreme Court announced in *Ruckelshaus*

> [T]he value of a trade secret lies in the competitive advantage it gives its owner over competitors . . . . If . . . a public disclosure of [trade secret] data reveals, for example, the harmful side effects of the [trade secret] submitter’s product and causes the submitter to suffer a decline in the potential profits from sales of the product, that decline in profits stems from a decrease in the value of the pesticide to consumers, rather than from the destruction of an edge the submitter had over its competitors, and cannot constitute the taking of a trade secret.215

The D.C. Circuit has similarly stated that

“[c]ompetitive harm [to the holder of proprietary information] should not be taken to mean simply any injury to competitive position, as might flow from customer or employee disgruntlement or from the embarrassing publicity attendant upon public revelations concerning, for example, illegal or unethical payments to government officials or violations of civil rights, environmental or safety laws.”216

---

215 *Ruckelshaus*, 467 U.S. at 1011-12 n.15 (emphasis added).

Indeed, as Sandeen and Kapczynski have shown, trade secrecy law writ large was never intended to restrict noncompetitors’ use of trade secrets in the same way it restricts competitors’.

To quote Sandeen,

The rhetoric of “theft” that pervades trade secret law and accusations of cyberhacking suggests that many assume that all acts leading to the unauthorised acquisition of information should be deemed “wrongful” but . . . a commitment to free enterprise and a competitive market environment requires a more nuanced view—one that recognises the value of information flows, particularly for information that is not protected by an existing body of law. This is particularly true if the subject information was acquired for a salutary purpose, such as to reveal criminal behaviour, share unprotected information or enhance competition.

The obvious solution, then, is information publicity—selective disclosure of corporate secrets to members of the public in ways that prohibit competitive uses. By cultivating bounded gardens of information publicity, agencies can unlock the benefits of disclosure without inflicting the harms to regulated entities that unfettered disclosure would. As Fan put it,
“[b]ounded disclosure thus optimizes the utility of disclosure so that the benefits are enhanced while the costs are reduced.”

To elaborate on the garden metaphor: Imagine (entirely hypothetically) that the NHTSA wanted to expand its nascent data-sharing program on self-driving cars to include not just crash data but also certain data collected from everyday driving. Researchers might reasonably argue that sharing this data would permit them to better understand the software and critique the claims made by car companies. Those companies might reasonably argue that sharing this data would make it dangerously easy for competitors to reverse-engineer their proprietary and innovative software. To accommodate both arguments, NHTSA could create and maintain a “bounded garden” of information. In this garden, regulated companies’ data sets, collected by NHTSA, become the precious “plants.” NHTSA bounds the garden carefully and blocks competitors and frivolous users from even seeing the plants. NHTSA permits established safety researchers and other credible, noncommercial users into the garden, to scrutinize, query, and even download some data, but subject to strict conditions—no commercial use, no retransmission of data, and so on. (I say more on such conditions in the next section.) In effect, a few representatives of the public are allowed into the garden, to study and sample the informational plants’ flowers and fruit under the watchful eye of the regulator, so long as these visitors are careful not to harm the plants in the process.

Here, again, are instructive parallels with privacy law. To talk, as Fan and I do, about enhancing the utility of disclosure of certain information while reducing or eliminating the costs of disclosure is, in effect, to talk about protecting the integrity of that information when sharing and using it in a new context, very much as Nissenbaum has theorized vis-à-vis governance of “private” personal information. Privacy law and trade secrecy law alike are

within the world of administrative law, under EPA’s FIFRA-based regime for sharing trade secret pesticide data, controlled sharing of a source company’s data with a competitor does not destroy the data’s status as a trade secret vis-à-vis future competitors. Future competitors must continue to compensate the source company for access to the data. See Pesticide Registration Manual: Chapter 10 - Data Compensation Requirements, ENV’T PROT. AGENCY, https://www.epa.gov/pesticide-registration/pesticide-registration-manual-chapter-10-data-compensation-requirements (describing the pesticide registration information an applicant must submit to comply with FIFRA).

Fan, Private Data, Public Safety, supra note 57, at 169; see also id. at 198-203 (arguing for bounded access to privately held data of public concern and the merits of this model over regimes of unconditioned disclosure).

Supra subsection I.B.1.

See Nissenbaum, Privacy as Contextual Integrity, supra note 194, at 138-40 (discussing contextual integrity when norms of appropriateness and distribution are upheld); Nissenbaum, A Contextual Approach to Privacy Online, supra note 194, at 33 (“Generally, when the flow of information adheres to entrenched norms, all is well; violations of these norms, however, often result in protest
designed not to thwart all flows of information but to govern them toward normatively desirable ends. In a recent piece, Madelyn Sanfilippo, Brett Frischmann, and Katherine Strandburg made explicit the many lessons that the fields of privacy law, on one hand, and innovation and intellectual property law, on the other, hold for one another. They observed that “private” personal information is just “one type of knowledge resource, which can produce value when it is shared and managed appropriately,” and that many of “[the] communities within which privacy is a hotly contested issue are also dealing with corresponding questions about” creation and governance of valuable knowledge—traditionally the core concern of intellectual property law and related fields. Sanfilippo, Frischmann, and Strandburg map intriguing similarities between Nissenbaum’s theory of contextual integrity for governance of private information and Ostrom’s theory of knowledge commons for governance of innovative information, and they encourage further “exploration of intersections of privacy with commons arrangements focused on knowledge production and sharing.”

The next subsection explores some of those intersections and proposes that, through “bounded garden” information publicity, the integrity of corporate secrets can be protected even as their secrecy is “violated” to create new knowledge.

2. The Gardens’ Bounds: Useful Legal and Technical Constraints on Access and Use

Let’s get practical. How, exactly, can agencies publicize corporate secrets for public good while prohibiting competitive uses and protecting their integrity as trade secrets?

Both legal and technical constraints on these gardens of information are possible and effective. I sketch three exemplary constraints below: (1) information use applications, (2) information use agreements, and (3) technical limits on access to information. These legal and technical constraints find meaningful real-world precedents in important but little-noticed data-sharing programs already undertaken by federal agencies in contexts where similar pro-secrecy and pro-disclosure interests clash. For example, a combination of legal and technical constraints successfully

---

and complaint.”); Nissenbaum, PRIVACY IN CONTEXT, supra note 194, at 148-50 (“If [a] new practice generates changes in actors, attributes, or transmission principles, the practice is flagged as violating entrenched informational norms and constitutes a prima facie violation of contextual integrity.”).

223 Madelyn Rose Sanfilippo, Brett M. Frischmann, & Katherine J. Strandburg, Privacy and Knowledge Commons, in GOVERNING PRIVACY IN KNOWLEDGE COMMONS 5, 8, 9 (Madelyn Rose Sanfilippo, Brett M. Frischmann, & Katherine J. Strandburg, eds., 2021).

224 Id. at 44.
mediates clashing interests in the context of medical data, where scientists clamor for broad access to data but patients and privacy advocates urge privacy-preserving restrictions on access and use of individuals’ sensitive medical data. In sketching here the legal and technical constraints on information access and use that agencies may impose in their information publicity programs, I draw less from the trade secrecy context than from the better-developed literatures around privacy law and the open science movement.

To be clear, I do not propose that all the constraints enumerated below be imposed in every instance of information publicity. Instead, agencies can and should pick and choose among these constraints—and devise others. My main goal here is simply to illustrate that it is indeed possible, even practical, to publicize corporate secrets without destroying their commercial value.

---

225 To my knowledge, the only prior proposals in the legal literature for controlled disclosure by federal agencies of privately held trade secrets are Fan’s bounded access model, see Fan, Private Data, supra note 55, at 198–99, and the “data publicity” for clinical trial data held by FDA, proposed by Kapczynski and me, see Morten & Kapczynski, supra note 52, at 540–49.

226 See Solove, Access and Aggregation, supra note 55, at 1195 (“When government discloses information, it can limit how it discloses that information by preventing it from being amassed by companies for commercial purposes, to be sold to others, or to be combined with other information and sold back to the government.”); see also Nissenbaum, Privacy as Contextual Integrity, supra note 194, at 119–20 (“This Article seeks to shed light on the problem of public surveillance first by explaining why it is fundamentally irreconcilable within the predominant framework that shapes contemporary privacy policy, and second by positing a new concept—contextual integrity—to explain the normative roots of uneasiness over public surveillance.”); Nissenbaum, A Contextual Approach to Privacy Online, supra note 194, at 32–33 (“This article explores present-day concerns about online privacy. . . . Finally, the essay lays out an alternative approach to addressing the problem of privacy online based on the theory of privacy as contextual integrity.”); Nissenbaum, PRIVACY IN CONTEXT, supra note 194, at 91–98 (discussing the various ways in which the “private/public dichotomy” has guided the normative scope of privacy); Sanfilippo, Frischmann & Strandburg, supra note 222, at 6–8 (discussing and supplementing Nissenbaum’s theories of information governance).

a. Information Use Applications

When sharing corporate secrets proactively, federal agencies can discriminate. That is, they can elect to publicize secret information to certain users, while sharing less information, or nothing at all, with others.

Information use applications that detail a prospective user’s credentials, intended uses, and security practices can help agencies decide with whom to share corporate secrets, and on what terms. In her proposal for agency-administered bounded public access to private secrets, Fan puts it this way: Only those applicants that document their “ability to design and adhere to a data protection plan to ensure use . . . for the purpose of addressing important public health and safety issues would be allowed to access the database.” Agencies could also demand that prospective users submit detailed information use plans, spelling out exactly how they intend to use the secret information in socially beneficial ways. As I describe below, three existing information publicity programs administered by the National Institutes of Health (NIH), CMS, and Canada’s national drug regulator require exactly this. Agencies may refuse access to their informational gardens for any number of reasons—e.g., to prospective users who appear unable to make effective use of the publicized information (especially if technically complex), unable to disseminate their findings to the broader public, or likely to use the information in a way that competes with its source.

b. Information Use Agreements

An information use agreement (or data use agreement) is simply a contract that governs transfer, maintenance, and use of protected information. These agreements are legal devices to constrain information users, and the constraints imposed can be positive as well as negative—they can discourage or prohibit information users from doing certain things and can equally well encourage or require information users to do other things.
These agreements can be paired with the information use applications described above; a prospective information user that clears the application is typically required to sign an information use agreement before it receives access to the agency’s information.

Contract law is highly flexible, and the regulatory agencies that administer information publicity programs can devise and impose any number of different provisions on information users. For example, information use agreements can prohibit the user from making commercial uses of the information; prohibit the user from sharing the protected information with others; require the user to report, promptly, to the regulator any findings that implicate public health and safety; give the regulator a right to review any publications before publication; require the user to disseminate new knowledge to the public at large—e.g., through the medical or scientific literature, or through the news media; and require the user to destroy the information once analysis is complete.

Agencies can levy penalties for breach of any of these provisions, including a ban on future participation in the information publicity program and financial penalties. (Think here of literal gardens: Visitors who ignore instructions to stay on paths and end up trampling a flower will be banned from future visits.)

c. Technical Limits on Access to Information

The two prior bounds on information access and use, information use applications and information use agreements, are administrative and legal in nature. They regulate information flows and protect information’s integrity.

But, as Lawrence Lessig\footnote{Lawrence Lessig, \textit{Code: Version 2.0} 125 (2006) (“The code or software or architecture or protocols set [inclusive or exclusive] features, which are selected by code writers. They constrain some behavior by making other behavior possible or impossible. The code embeds certain values or makes certain values impossible. In this sense, it too is regulation . . . .”).} and others\footnote{See, e.g., William J. Mitchell, \textit{City of Bits: Space, Place, and the Infobahn} 111-12 (1996) (concluding that “control of code is power” because interactions with software are totally delimited by formally-stated rules).} have observed, technical architecture, too, can regulate flows of information. Agencies that undertake information publicity can contrive the architecture of information sharing in ways that shape access and use.

These technical limits may prove even more effective than legal ones. For example, regulators can build information publicity portals that permit information users to view and/or query proprietary information but not to download or copy in full.\footnote{For an example in the pharma and biotech context, see Inst. of Med. of the Nat’l Acads., \textit{Sharing Clinical Trial Data}, supra note 226, at 147 (“Several data sharing}
noncommercial uses of secret information while discouraging or preventing the directly competitive uses most harmful to the secret's source. (More garden analogy: These technical limits would work something like a fence ringing the trunk of a beloved fruit tree in a public park. The fence prevents people from climbing the tree and damaging its branches but allows people to enjoy its blossoms and pick its lowest-hanging fruit.)

For example, an academic or environmental advocacy group seeking to determine whether the fluid used in a particular location for hydrocarbon fracking contains a particularly hazardous chemical could query the EPA for the answer; the EPA could then publicize the presence or absence of the chemical, and its concentration, without revealing the entire chemical makeup of the fluid. Similarly, the FAA could conceivably provide groups seeking to scrutinize Boeing’s 737 MAX MCAS software with access to portions of Boeing’s code and other secret information (but not all)—enough to scrutinize and validate Boeing’s claims but not enough build a competing product.

d. *Agency-Cultivated “Bounded Gardens” of Information Already in Existence*

Why focus on these three constraints on information access and use—information use applications, information use agreements, and technical limits? In part because each is already working in proactive information disclosure programs run by administrative agencies. That is, these three constraints already govern access to bounded gardens of otherwise-secret information currently cultivated by parts of the U.S. government (and, in one example, the Canadian government). These constraints determine which users access information; they dictate the range of uses users make of information; and they shape the flow of information from users back to the agency and to the public at large. These existing proactive information disclosure programs are—as best I can tell—little noticed and little theorized in the legal academic literature. But they are, in effect, proofs-of-concept for the information publicity I propose in this paper.

---

programs . . . grant[,] some access to clinical trial data to secondary users but [do] not allow[,] them to download the data to their own computers. . . . This approach helps protect sponsors from secondary users’ carrying out analyses beyond those proposed in the data request . . . .); *Discussion Framework for Clinical Trial Data Sharing, supra* note 226, at 30 (“In some [data sharing models], the actual data are not provided to the requestor. Instead, data holders might run specific data analyses for approved requestors . . . . In another model, recipients . . . access and run queries on the data, but are not able to download or obtain copies of the data.”).
i. NIH’s BioLINCC: Information Use Applications & Information Use Agreements

Since the 2000s, NIH has maintained the Biologic Specimen and Data Repositories Information Coordinating Center (BioLINCC), a center that shares sensitive and scientifically valuable biomedical data with select requesters.235 NIH created and administers the center, but much of the information contained in BioLINCC’s databases is contributed not by NIH itself, but by nongovernmental entities. (Many of these entities are required to submit information to BioLINCC as a condition of taking grant money from NIH’s National Heart, Lung, and Blood Institute (NHLBI).) BioLINCC’s information-sharing program has proven popular and influential, as hundreds of requesters have sought and received access to thousands of data sets, leading to dozens of high-profile scientific and medical publications in cardiology, infectious disease, and other fields of research.236


BioLINCC data does not typically implicate trade secrecy, but it does implicate individual patients’ privacy. As such NIH avoids unconditioned disclosure of BioLINCC data and instead constrains access to and use of the data—making BioLINCC a bounded “garden” of information. BioLINCC requires information use applications, which must disclose would-be users’ intended uses (their “Research Plan”) and their data security practices and commitments. NIH discriminates among users: Commercial users can access only a subset of BioLINCC’s data, and would-be data users that cannot muster a credible Research Plan are provided no access at all. Before getting access to any BioLINCC data, information users must execute, with NIH, an information use agreement termed a “Research Materials Distribution Agreement” (RMDA). The RMDA imposes various prohibitions and obligations on users. For example, the RMDA prohibits the transfer of BioLINCC data, or the use of data to identify specific medical study subjects. It also obligates users to destroy all downloaded data after research is complete, and to provide NIH with yearly updates on use of the data. NIH warns that any information users who breach the RMDA may be denied further access to BioLINCC data. No misuse of BioLINCC data has been reported in the many years of the center’s existence.

ii. CMS’s Medicare Data for Performance Measurement: Information Use Applications, Information Use Agreements & Technical Limits on Access to Information

CMS is the single largest payer for healthcare in the United States and important federal regulator. In 2011, under the Affordable Care Act, CMS

238 See The BioLINCC Handbook, supra note 234, at 8 (“[F]or studies with commercial use data restrictions, investigators requesting data for commercial use would be eligible to receive only the subset of the overall dataset that was provided by subjects who consented to commercial research.”).

239 See id. at 12 (“Approved requests require an executed Research Materials Distribution Agreement (RMDA) before data can be transferred.”).


241 The BioLINCC Handbook, supra note 234, at 20 (“[F]ailure to adhere to the terms of the RMDA will be taken into consideration with respect to any future requests for data and/or biospecimens from the NHLBI repositories.”).

began publicizing certain information on the quality and costs of healthcare services and supplies that it pays for through Medicare—data for so-called “performance measurement.” CMS also shares other Medicare claims data with researchers on a more ad hoc basis, fielding requests through a dedicated Research Data Assistance Center (ResDAC). Public sharing of Medicare claims data has since served a wide variety of useful ends: “[T]o describe patterns of morbidity and mortality and burden of disease, compare the effectiveness of pharmacologic therapies, examine the cost of care, evaluate the effects of provider practices on the delivery of care, and explore the effects of important policy changes on physician practices and patient outcomes.”

For example, the nonprofit Health Care Cost Institute uses CMS’s performance measurement data and other data to generate annual reports on regional, state, and national trends in healthcare spending for the general public; it recently used this data to show that Medicare generally pays less for healthcare services than commercial health insurers.

---


244 See Katherine E. Mues, Alexander Liede, Jiannong Liu, James B. Wetmore, Rebecca Zaha, Brian D. Bradbury, Allan J. Collins & David T. Gilbertson, Use of the Medicare Database in Epidemiologic and Health Services Research: A Valuable Source of Real-World Evidence on the Older and Disabled Populations in the US, 9 CLINICAL EPIDEMIOLOGY 267, 268-69 (2017) (“Requests for [Medicare claims] data access are submitted to CMS via the . . . [ResDAC], which reviews the request for scientific merit and technical feasibility. If sound, the request is then sent to CMS for approval. If approved, CMS enters into a Data Use Agreement (DUA) with the researcher.”).

245 Id. at 268.


247 See Bill Johnson, Kevin Kennedy, Daniel Kurowski, Aaron Bloschichak, Elianna Clayton, Jean Fuglesten Biniek & Katie Martin, Comparing Commercial and Medicare Professional Service Prices, HEALTH CARE COST INSTITUTE (Aug. 13, 2020), https://healthcostinstitute.org/hcci-research/comparing-commercial-and-medicare-professional-service-prices?highlight=WyJiZWdpYyJdFyZSiSm1iZGlyYXJjZ3MiXQ== [https://perma.cc/Z3U8-XJ7G] (“Nationally, we found that the commercial prices paid for the average professional service were 122% of what would have been paid under the Medicare Physician-Fee-Schedule (PFS).”).
Like BioLINCC data, CMS’s Medicare data for performance measurement does not typically implicate trade secrecy, but it does implicate individual patients’ privacy. As such, CMS, like NIH, avoids unconstrained disclosure of this data and instead constrains access and use—making this another bounded “garden” of information. To access any of this data, prospective information users must complete an elaborate, multi-phase application process administered by CMS. Among other things, CMS demands that applicants prove “expertise and sustained [multi-year] experience” in health data analysis as well as “[e]xpertise in establishing, documenting and implementing rigorous data privacy and security policies including enforcement mechanisms.” As of September 2022, about 40 institutions—a mix of commercial, nonprofit, and academic—had met CMS’s criteria and become so-called “qualified entities.” Once qualified, entities that seek CMS data must first execute data use agreements with CMS that require them to, *inter alia*, maintain privacy and security protocols and destroy all downloaded data once research is complete. Qualified entities that use CMS data must provide annual updates to the agency and if a qualified entity breaches its data use agreement, CMS can impose penalties, including fines for any instances of individuals’ private medical information kept insecurely. CMS now gives qualified entities the option of visiting and querying data through a “virtual research environment” called the Virtual Research Data Center (VRDC); within the VRDC, users are prohibited (by the data architecture itself) from accessing personally identifiable information on individual patients. This technical limit both protects the

---


252 See 42 C.F.R. § 401.719 (2021) (requiring qualified entities to send annual reports to CMS for monitoring purposes).

253 See id. (detailing penalty fees for violations of CMS data use agreements).

Publicizing Corporate Secrets


Since 2019, Canada’s central regulator of drugs, vaccines, and medical devices—Health Canada—has shared rich datasets from clinical trials of products it has approved, under the “Public Release of Clinical Information” (PRCI) program. The data shared through PRCI is generated and compiled not by Health Canada, but by the drug and device companies who submit it when seeking product approval. As of February 2023, data on over 340 distinct products, gathered from dozens of companies, have been posted to PRCI. Academic researchers have used data shared via PRCI to analyze and communicate the safety and efficacy of important medical products, constituting an important check on and complement to the work of Health Canada, FDA, and other national regulators. For example, one academic group recently used PRCI data to show that extended-release oxycodone hydrochloride (better known under its brand name OxyContin) was approved by Health Canada, the FDA, and other national regulators without evaluation of the risks of misuse and addiction, even though opioids were widely known at the time to be addictive.


interests, Health Canada asks regulated entities to redact what it deems “confidential business information” (CBI)—essentially, trade secrets—as well as information identifying individual trial participants before making the data accessible to routine users of PRCI. Users who wish to access and use these redacted data sets may do so with few restrictions.

Yet Health Canada shares even more information—including unredacted trade secrets. According to Paragraph 21.1(3)(c) of the Canadian Food and Drugs Act, Health Canada will share trade secrets (CBI) with certain users, on certain conditions. First, users must submit a data use application that proves their use is noncommercial and relates to “protection or promotion of human health or the safety of the public.” The application must also explain “[h]ow the results of the proposed project will be disseminated to the Canadian public.” Any users granted access must then sign data use agreements insisting “the specified CBI can be used only for the purposes of the proposed project and must be kept confidential using appropriate safeguards.” In the event that a data user detects a safety, efficacy, or quality problem, Health Canada requests that the user notify Health Canada as well as the public at large.

In 2018 a medical researcher, Peter Doshi, successfully used Paragraph 21.1(3)(c) to obtain detailed and previously secret data on the safety and efficacy of several medical products, including oseltamivir (Tamiflu) and

259 Health Canada’s definition of CBI is nearly identical to the UTSA’s definition of a trade secret. Health Canada defines CBI as “business information[] that is not publicly available . . . in respect of which the person has taken measures that are reasonable in the circumstances to ensure that it remains not publicly available, and . . . that has actual or potential economic value to the person or their competitors because it is not publicly available and its disclosure would result in a material financial loss to the person or a material financial gain to their competitors.” Gov’t Can., Guidance Document - Disclosure of Confidential Business Information Under Paragraph 21.1(3)(c) of the Food and Drugs Act, CANADA.CA (Mar. 12, 2019), https://www.canada.ca/en/health-canada/services/drug-health-product-review-approval/request-disclosure-confidential-business-information/disclosure-confidential-business-information/guidance.html#a1.2 [https://perma.cc/26X2-X785].


261 See Gov’t Can., supra note 258 (noting that the government has discretion to share non-redacted data under certain conditions).

262 Id.

263 Id.

264 Id.

265 See id. (“Recipients of disclosed information are expected to make the findings of their project with the disclosed information publicly available when the findings provide additional knowledge about the therapeutic product under study. If the recipient of disclosed information has made a determination that the safety, efficacy or quality of a product(s) may change as a result of the evaluation of the CBI then the results should be submitted to Health Canada.”).
vaccines for human papillomavirus (HPV), without signing a confidentiality agreement. The researcher’s access to this CBI—and his legal authority to disseminate analysis of it—was upheld by the Canadian Federal Court.

C. Getting the Balance Right: A Procedural Framework

How should an agency decide whether to publicize a particular corporate secret? And if the agency does elect to publicize it, which bounds should it impose on access and use? The answers to these questions rely on a deeper set of factual concerns. For example, will a particular prospective user’s use of the information cause competitive harm to the source? If so, how, and how bad? Will that user’s proposed use meaningfully benefit the public? What information can reasonably be disclosed without condition to all comers? What information should never be publicized at all? In short, how should the overall balance of secrecy and disclosure be struck to unlock information’s socially valuable uses while protecting its integrity?

In my view, the process of publicizing corporate secrets should start with the regulator gathering information from both the secret’s prospective users and its source (or sources). To gather information from a secret’s prospective users, the regulator can require information use applications, as described above.

To gather information from the secret’s source(s), the regulator can adapt the process that already exists for FOIA requests. As noted above, regulators already routinely ask regulated entities to designate information those entities believe should be kept confidential—whether because it contains trade secrets or some other protected category of information—and notify those entities before contemplating disclosure.

But to build effective information publicity programs, regulators should do more than simply ask regulated entities to identify secret information. Regulators should also ask those entities to articulate the competitive value of the information and the corresponding harm that would flow from


268 See supra Part II.B.2.a (discussing governmental use of these applications).

269 See supra Part I.C.1.
disclosure to competitors. This, too, is entirely consistent with longstanding FOIA practice; until 2019 (when the Supreme Court upended the legal standard for withholding CCI under FOIA exemption 4), federal agencies in FOIA disputes routinely asked the submitters of purported CCI to describe and document whether unconstrained disclosure would “cause substantial harm to [their] competitive position.” There are good efficiency reasons to ask regulated entities to submit this analysis to regulators, rather than forcing agencies to speculate; regulators face huge information asymmetries, and regulated entities are better positioned to identify and quantify the harms that would flow from unconstrained disclosure.

Of course, regulators contemplating beginning information publicity programs can and should solicit and gather input from a broader group of stakeholders whenever time and resources permit. Particularly if contemplating an ongoing, long-term information publicity program rather than an urgent, one-time release of information, regulators may choose to use notice-and-comment rulemaking to gather detailed feedback. (As I explain below, notice-and-comment rulemaking may be not just desirable but legally necessary, both to undo existing rules that constrain agencies’ disclosure of information and to supply the necessary legal “authorization” to make sharing of any bona fide trade secrets permissible under the federal TSA). NHTSA’s newly announced program of sharing data on accidents involving self-driving cars and CMS’s long-running program of publicizing inspection reports from diagnostic blood-testing laboratories are two examples of long-term information publicity programs for which rulemaking would be beneficial, to formalize the scope and process of publicity.

All this comes with some costs for the agency. Each step—gathering information, organizing and analyzing information, deciding whether to publicize information, implementing an information publicity program, and maintaining the program—imposes burdens. Rulemaking is itself difficult and takes years. Yet burdens are already borne by the same agencies, as they respond to FOIA requests. Indeed, the burdens of responding to FOIA requests may be uniquely high, as current practice involves painstaking page-

---

270 For further discussion, see Varadarajan, supra note 169, at 466-67.
271 Nat’l Parks & Conservation Ass’n v. Morton, 498 F.2d 765, 770 (D.C. Cir. 1974). Notifying sources in this way of the possibility of information disclosure—controlled or otherwise—will not only comport with Executive Order 12,600 and unearth information useful to the regulator, but it will also help the agency preempt any challenges made under the Due Process Clause.
272 See Cohen, The Regulatory State in the Information Age, supra note 32, at 384 (“Information abundance also enables new types of power asymmetries that revolve around differential access to data and to the ability to capture, store, and process it on a massive scale.”).
273 See infra Part III.B.2.
274 For a more detailed discussion of these issues, see supra notes 119–32 and accompanying text.
by-page, line-by-line redaction of each document to excise information exempted from disclosure. Proactive information publicity can, in general, be cheaper and quicker than fulfilling FOIA requests, as technical and legal limits on information access and use can obviate the need for line-by-line redaction. Agencies can quickly and cheaply publicize information to certain users in toto, subject to appropriate constraints. In addition, effective information publicity will moot at least a subset of FOIA requests, permitting agencies to divert resources currently consumed by these requests. For example, as Kapczynski and I described in an earlier paper, the FDA could publicize complete or near-complete data sets from the clinical trials of prescription drugs and medical devices without undertaking the difficult redaction that regularly demands months, and sometimes years, of FOIA officers’ time to fulfill even a single significant FOIA request.

One final recommendation: A corporate secret’s formal legal category should not dictate either the process for publicizing a corporate secret or the substantive limits imposed on users’ access and use. In other words, agencies’ analysis should not begin or end with preoccupation over whether the information constitutes a trade secret (under the Uniform Trade Secrets Act (UTSA) definition). As I show below, as a legal matter, agencies generally have legal authority to disclose even bona fide trade secrets (though they may need to take preparatory steps to do so, including rule changes). Equally important, from a normative perspective, agencies should be thinking less about formal legal categories and more about the actual, material consequences that could flow from use of the secret—both the benefits that would flow from sharing with independent analysts and the broader public and the harms that would flow from sharing with competitors.

---

275 See 5 U.S.C. § 552(b) (“Any reasonably segregable portion of a record [subject to mandatory disclosure under FOIA] shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection.”).

276 For example, see the information use agreements and technical limits described in Part II.B.2.b.

277 See Morten & Kapczynski, supra note 54, at 521, 555 (detailing the arduous process of redaction for FDA data and the benefits of using a data publicity approach).


279 See infra Part III.

280 In this regard, I align with Sanfilippo, Frischmann, and Strandburg, who have argued that both Nissenbaum’s contextual integrity and Ostrom’s governing knowledge commons frameworks focus on context, not whether information is “innately ‘private’ or ‘sensitive.’” Sanfilippo, Frischmann & Strandburg, supra note 222, at 6-7, 13.
whether to undertake information publicity, agencies should consider not just the formal boundaries of trade secrecy but other values and interests that militate toward close control of information, including individual privacy and the agency’s own deliberative processes.

III. A LEGAL ROADMAP TO PUBLICIZING CORPORATE SECRETS

The preceding Part II was largely normative. It argued that agencies should proactively publicize corporate secrets. Part II endorsed bounded “gardens” of information that unlock socially useful uses of corporate secrets while protecting their integrity vis-à-vis competitors, and it sketched a procedural framework for agencies to determine how and how much to publicize.

This Part is largely doctrinal. It shifts focus to the important question of how federal regulators can undertake proactive information publicity programs within the confines of existing law—and survive the scrutiny of a Supreme Court skeptical of administrative action. This Part provides detailed support for the article’s central claim that federal regulators generally do have a legal right to disclose trade secrets. (Or, better yet, to publicize them carefully, subject to the legal and technical limits described in Part II.) In other words, this Part challenges and disproves the conventional wisdom, first articulated in the Introduction, that agencies have some deep-seated legal obligation under federal statute or the U.S. Constitution to keep trade secrets and other corporate secrets secret. As this Part explains, the default rule is the reverse: disclosure is permitted unless something in the agency’s enabling statute prohibits it.

Subpart III.A identifies the legal sources of federal regulators’ wide-ranging authority to disclose information in their possession, on their own terms. Subpart III.B identifies the three major legal limits on agencies’ authority to disclose trade secrets and related categories of commercially valuable confidential information: (1) agencies’ respective enabling statutes, (2) the federal Trade Secrets Act (TSA), and (3) state trade secrecy law, made enforceable against the U.S. government through the Takings Clause of the U.S. Constitution and the Federal Tort Claims Act (FTCA). It then explains how most regulators can navigate these limits to achieve meaningful information publicity. Subpart III.C identifies the procedural steps that agencies contemplating information publicity programs should undertake before they begin disclosure. Finally, Subpart III.D briefly considers judicial review of federal regulators’ information publicity programs and concludes that review will likely favor the regulators over aggrieved companies.
A. Locating Regulators’ Sweeping Power to Disclose Information

The legal rule is simple: Federal agencies have wide-ranging background legal authority to disclose information within their possession. As one treatise puts it, “except where Congress actually mandated withholding . . . [an] agency has very broad discretionary choices.”

From where does federal agencies’ general background authority to disclose information within their possession arise? Federal statute, for one: “The head of an Executive department or military department may prescribe regulations for . . . the custody, use, and preservation of its records, papers, and property.” This statute—5 U.S.C. § 301, sometimes called the federal “housekeeping statute”—began in an act of the very first Congress of 1789, which delegated to federal agencies broad authority to control their own records.

But federal agencies’ general legal authority to disclose information within their possession can also be understood simply as the absence of any prohibition on disclosure—that is, as a background presumption of authority to disclose. This background presumption has been affirmed by the Supreme Court on at least three occasions in the last 50 years, including in Food Marketing Institute, a 2019 decision authored by Justice Gorsuch. The same...
background authority was recognized by President Obama\textsuperscript{286} and by the Department of Justice in both his administration and President Trump’s.\textsuperscript{287}

Federal agencies’ wide-ranging authority to disclose corporate secrets within their possession is subject only to three modest limits: (1) agencies’ own enabling statutes, (2) the federal TSA, and (3) state trade secrecy law, made enforceable against the U.S. government to a limited extent by the Takings Clause of the U.S. Constitution and the FTCA. I deem these limits modest because they do not, as a blanket rule, prohibit federal agencies from disclosing even genuine trade secrets, so long as the agencies take appropriate steps to “authorize” disclosure.

First, a word on two sources of law that do not limit federal agencies’ disclosure or use of trade secrets: FOIA and the federal Defend Trade Secrets Act (DTSA).

Despite frequent misconceptions, FOIA does not restrict federal agencies’ power to disclose confidential information within their possession. As the Supreme Court has announced, “the FOIA is exclusively a disclosure statute.”\textsuperscript{288} “Congress did not design the FOIA exemptions to be mandatory bars to disclosure.”\textsuperscript{289} FOIA’s Exemption 4 specifically permits but does not require agencies to withhold information that qualifies as a trade secret or as CCI.\textsuperscript{290} Indeed, in 1977, Congress considered and rejected a statutory amendment to FOIA that would have made agency withholding of CCI and trade secrets mandatory rather than discretionary.\textsuperscript{291}

\textsuperscript{286} Freedom of Information Act: Memorandum from Barack Obama, President of the United States, for the Heads of Executive Departments and Agencies, 74 Fed. Reg. 4683 (Jan. 21, 2009) (“The presumption of disclosure . . . means that agencies should take affirmative steps to make information public.”).

\textsuperscript{287} Memorandum from the Attorney General for Heads of Executive Departments and Agencies Concerning the Freedom of Information Act (FOIA), 74 Fed. Reg. 51879 (Oct. 8, 2009) (“I strongly encourage agencies to make discretionary disclosures of information. An agency should not withhold records merely because it can demonstrate, as a technical matter, that the records fall within the scope of a FOIA exemption.”); Brief for the United States as Amicus Curiae Supporting Petitioner at 32, Food Mktg. Inst., 139 S. Ct. 2356 (2019) (No. 18-481) (Because “[FOIA] does not limit an agency’s discretion to disclose information,” “even if a district court’s order requiring disclosure under FOIA is stayed pending appeal, the government could simply release the records itself, rendering any appeal moot,” and “nothing in an appeal by a nongovernment person could prevent the agency’s disclosure of its own records.”) (quoting Chrysler, 441 U.S. at 294).

\textsuperscript{288} Chrysler, 441 U.S. at 292.

\textsuperscript{289} Id. at 293.

\textsuperscript{290} Id. at 291. See also Food Mktg. Inst., 139 S. Ct. at 2362 (observing that FOIA's Exemption 4 provided the USDA with "discretion to withhold the requested data" and that USDA might "might just as easily choose to provide the data anyway," even if the exemption applies) (emphasis in original).

With 2016’s DTSA, Congress created a right of action for injured trade secret holders to sue private parties in federal district court for misappropriation of trade secrets.\(^292\) However, the DTSA does not constrain federal agencies; Congress declined to waive the U.S. government’s immunity from trade secret misappropriation suits brought under that act,\(^293\) and the DTSA’s definition of a trade secret does not apply outside the act.

Now, let’s turn to the three sources of law that do limit agencies’ disclosure of corporate secrets. Again, they are (1) agencies’ own enabling statutes, (2) the federal TSA, and (3) state trade secrecy law, made enforceable against the U.S. government via the Takings Clause of the Fifth Amendment and the Federal Tort Claims Act.\(^294\)

\(^{292}\) The DTSA creates a right of action for injured trade secret holders to sue private parties in federal district court for misappropriation of trade secrets. 18 U.S.C.§ 1836(b)(1).

\(^{293}\) 18 U.S.C. § 1833(a)(1) (stating that there is no right of action against “otherwise lawful activity” by U.S. government); see also David S. Bloch, Can the Government Be Sued Under the Defend Trade Secrets Act?, 45 AIPLA Q.J. 407, 411 (2017) (“While the Government has created mechanisms to enforce patents, copyrights, and trademarks against the Government, it has not created a uniform remedy for trade secret misappropriation by the government.”) (emphasis in original).

\(^{294}\) Vogel suggests a possible fourth limit, the Economic Espionage Act (EEA), 18 U.S.C. §§ 1831-39. See Vogel, supra note 45, at 166. Vogel acknowledges, however, that the EEA was mainly passed to regulate private conduct, and whether the TSA applies to the government is a question for the courts; no court has concluded that the EEA applies against the U.S. government or its employees. Id. at 168. Separately, the First Amendment could conceivably constrain how federal agencies disseminate information. In 2002, Solove argued convincingly that when federal administrative agencies exercise their discretion to disclose information proactively, they do not trouble the First Amendment. See Solove, Access and Aggregation, supra note 55, at 1200-1201. In Solove’s view, this is true even when agencies discriminate among information users and uses. Id. at 1209. To my knowledge, no proactive information disclosure program administered by a federal agency has ever been challenged on First Amendment grounds, including the active programs maintained by NIH and CMS described in Part II. However, the Supreme Court’s First Amendment jurisprudence has changed significantly since 2002, and it is possible that industry or other critics of information publicity could mount First Amendment challenges. For example, regulated entities might characterize regulatory regimes that require them to submit information to an agency for later dissemination to the public as impermissible “compelled speech.” See Sarah Haan, The Post-Truth First Amendment, 94 INDIANA L.J. 1351, 1366, 1375 (2019) (summarizing recent “compelled speech” cases); Caroline Mala Corbin, Compelled Disclosures, 65 ALA. L. REV. 1277, 1282 (2014) (same); and see generally Salome Viljoen, Privacy and the Legal Constitution of Social Data (Nov. 2, 2022) (forthcoming) (analyzing the weaponization of compelled speech doctrine against regulatory and public oversight). This will be an area to watch. Finally, the international Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) requires, inter alia, that signatory members protect confidential pharmaceutical and chemical data submitted to national regulators “against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use.” Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), art. 39.3, Apr. 15, 1994. The information publicity proposed in this paper comports with TRIPS, as publicity is contemplated “to protect the public,” and the data use agreements and other bounds on users’ uses of information protect “against unfair commercial use.” In 2020, the Court of Justice of the European Union concluded that an information publicity program of the European Medicines Agency—publicizing otherwise secret clinical trial data—does
B. Navigating Three Legal Limits

1. Agencies’ Enabling Statutes

Agencies’ enabling statutes are the most important, so I turn to them first. “Enabling statutes” are the statutes through which Congress establishes the powers and responsibilities of an administrative agency.295 Through these statutes, Congress decides how much authority to delegate to each agency. (Congress itself has essentially unlimited power to demand trade secrets from private parties and then disclose them,296 though in practice its investigations tend to be narrow, and it exercises this power sparingly.)

In the enabling statutes of several federal regulators, Congress chose to limit the corporate secrets those regulators are permitted to disclose. A handful of important federal regulators are statutorily prohibited from disclosing any and all “trade secrets”297 obtained from regulated entities, unless those entities consent.298 Most notably, the Federal Trade Commission Act prohibits FTC from disclosing to the public “any trade secret or any commercial or financial information which is obtained from any person and which is privileged or confidential.”299 The Federal Trade Commission Act’s statutory prohibition on disclosure has major consequences, as FTC has more oversight and information-gathering resources than any other federal regulator. (FTC can and does publicize much other non-trade-secret information.) Similarly, the Consumer Product Safety Act prohibits the Consumer Product Safety Commission from disclosing trade secrets as defined by either the federal TSA300 or FOIA.301 Some agencies’ enabling

---

296 See Rowe, Striking a Balance, supra note 68, at 803 (“[A]ny disclosures by a member of Congress may not constitute an unconstitutional taking for private use.”); TODD GARVEY, MARK J. OLESZEK, BEN WILHELM, CONG. R.SCH. SERV. IF10015, CONGRESSIONAL OVERSIGHT AND INVESTIGATIONS (2014), https://crsreports.congress.gov/product/pdf/IF/IF10015 [https://perma.cc/B4X-MV3V]) (last visited Dec. 13, 2022) (“Congress’s power to obtain information, including classified and/or confidential information, is extremely broad.”); 3 ROGER M. MILGRIM & ERIC E. BENSEN, MILGRIM ON TRADE SECRETS § 12.02 n.69 (2011) (trade secret information obtained by Congress via FTC subpoena “is subject to investigatory review—and possible dissemination—by Congress itself.”).
297 Some statutes do not define “trade secret,” and as such the scope of prohibition is not entirely clear.
298 For a non-exhaustive list of such enabling statutes, see 3 MILGRIM & BENSEN, MILGRIM ON TRADE SECRETS, supra note 294, § 12.04.
statutes do not prohibit disclosure of all trade secrets but do prohibit
disclosure of certain trade secrets. The Food, Drug, and Cosmetic Act, for
example, includes one provision that prohibits FDA from disclosing trade
secret manufacturing processes\(^\text{302}\) and another that generally prohibits the
agency from disclosing trade secrets submitted by medical device
manufacturers.\(^\text{303}\) The Patent Act prevents the Patent & Trademark Office
from disclosing information submitted in patent applications until 18 months
from filing, unless special circumstances apply.\(^\text{304}\)

However, many federal regulators do not face such agency-specific
statutory restrictions on their power to gather and disclose corporate secrets.
Among the major regulators whose enabling statutes do not categorically
prohibit them from disclosing trade secrets are EPA,\(^\text{305}\) FAA,\(^\text{306}\) FCC,\(^\text{307}\)
FDA,\(^\text{308}\) HHS (at least vis-à-vis its administration of Medicare\(^\text{309}\) and
HIPAA\(^\text{310}\)), NHTSA,\(^\text{311}\) and NTSB.\(^\text{312}\)

The subset of federal regulators whose enabling statutes expressly limit
disclosure of certain or all trade secrets must therefore tread carefully.
Disclosure of trade secrets may subject them to litigation.\(^\text{313}\) This is, of course,
perfectly consistent with foundational theories of administrative law; federal agencies must stay within statutory bounds in every action that they take.

2. The Federal Trade Secrets Act

The second legal limit on federal agencies’ legal authority to disclose corporate secrets is the federal TSA. Despite widespread misperception that the TSA constitutes an outright prohibition on federal agencies’ disclosure of private trade secrets, the statute’s constraints are as much procedural as substantive and can be overcome by any federal agency whose enabling statute permits the disclosure of trade secrets.

The TSA is a criminal statute that prohibits federal employees from disclosing certain confidential information (including “trade secrets”) when not “authorized by law”:

> Whoever, being an officer or employee of the United States or of any department or agency thereof, . . . publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof, which information concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association; . . . shall be fined under this title, or imprisoned not more than one year, or both; and shall be removed from office or employment.

The most severe criminal penalties contemplated by the TSA—imprisonment and termination of employment—have apparently never been applied in the TSA’s many decades of existence.

---


317 See 3 Roger M. Milgrim & Eric E. Benson, Milgrim on Trade Secrets § 12.02 n.9 ("[18 U.S.C. § 1905] has not yet been applied in the criminal context."). This statement is not true, but it underscores the rarity of prosecutions. See, e.g., United States v. Wallington, 889 F.2d 573, 575, 580 (5th Cir. 1989) (Fifth Circuit affirming conviction under § 1905 of a United States
By the statute’s plain text, the TSA appears to encompass not just “trade secrets” but also confidential information relating to “operations,” “style of work,” and certain financial information. Yet, despite that broad text, the TSA has historically been construed narrowly by the Supreme Court—more narrowly than state trade secrecy laws. Many corporate secrets held by regulators fall outside the TSA and can consequently be disclosed without implicating it at all. Of course, it is not clear that the current Supreme Court, with a self-proclaimed “textualist” wing now ascendant, will continue to construe the TSA narrowly.

But the precise scope of information subject to protection as a “trade secret” under the TSA turns out to be of rather modest importance, as the plain text of the TSA prohibits only disclosures made “in any manner or to any extent not authorized by law.” Any disclosure of trade secrets properly “authorized by law” is expressly permitted by the TSA. “Authorization by law” is the key constraint on the TSA; the TSA’s text contemplates legally authorized agency disclosure of even the most precious trade secrets.

When is an agency’s disclosure “authorized by law,” so as to bypass the anti-disclosure restrictions of the TSA? The answer is again regulators’ enabling statutes. In some enabling statutes, Congress has legislated to define certain information as disclosable that would otherwise be protected by

 Customs Service employee who had disclosed to a friend, without authorization, information from a confidential law enforcement database; the employee was ordered to pay a $250 fine and placed on probation for two years.


319 In Ruckelshaus, certain pesticide “health, safety, and environmental data” was deemed by the Court to be a trade secret under Missouri state law, but not covered by the TSA’s prohibition on unauthorized disclosure. Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1001-02. In 2019, the Supreme Court reaffirmed a narrow construction of the TSA in Food Marketing Institute, albeit only implicitly. In Food Marketing Institute, Justices Roberts, Thomas, Alito, Kagan, and Kavanaugh joined Gorsuch’s majority opinion. The Court held, by implication, that the scope of the TSA must be narrower than FOIA exemption 4, which provides agencies discretion to withhold trade secrets and CCI. Food Marketing Institute v. Argus Leader Media, 139 S. Ct. 2356, 2362 (2019). For further analysis of the TSA’s narrow construction, see Morten & Kapczynski, supra note 54, at 537-38.

320 See, e.g., Morten & Kapczynski, supra note 54, at 534-37 (arguing that certain safety and efficacy data on prescription drugs and vaccines is not protected by the TSA).


323 See Memorandum from William B. Schultz to Allan Coukell, Director, Pew Prescription Project 4 (Aug. 5, 2009), https://www.regulations.gov/document?D=FDA-2009-N-0247-0097 [https://perma.cc/E6QS-DLMF] (“[I]t is not necessary to address [the question of whether clinical data is protected by the TSA] because the Trade Secret bar does not apply where disclosure is authorized by law.” (internal citations omitted)).
§ 1905. In most cases, however, Congress has more broadly delegated authority to define a set of information, including trade secret information, that regulators may disclose in service of their regulatory functions. Agencies can then formalize their disclosure authority through regulations that have “force and effect of law.”

As the D.C. Circuit has explained:

[T]he [TSA] seems to embody a congressional judgment that private commercial and financial information should not be revealed by agencies that gather it, absent a conscious choice in favor of disclosure by someone with power to impart the force of law to that decision. The Act attempts to forestall casual or thoughtless divulgence—disclosure made without first going through a deliberative process—with an opportunity for input from concerned parties.

With an appropriate rule in place, disclosure of trade secrets is authorized and therefore entirely legal under the TSA.

The Supreme Court has explained that “force and effect of law” inures when a regulation is a “substantive” or “legislative-type” rule “affecting individual rights and obligations” and is properly promulgated pursuant to an appropriate delegation by Congress of authority to disclose. Assuming it is promulgated with proper process (e.g., notice and comment), a regulation effectively authorizes disclosure so long as it meets the “nexus test” articulated in the Court’s landmark Chrysler decision: there must be “a nexus between the regulation[] and some delegation of the requisite legislative authority by Congress.” The question of whether Congress delegated the requisite authority is precisely the same enabling statute question addressed in the preceding subpart: if an agency’s enabling statute permits the agency to obtain and disclose a specific secret, the agency has the requisite “legislative authority.” The nexus standard is relaxed and permissive; as the Supreme Court has held, “[t]he pertinent inquiry is whether under any of the arguable

325 See Chrysler Corp. v. Brown, 441 U.S. 281, 301 (1979) (“In order for a regulation to have the ‘force and effect of law,’ it must have certain substantive characteristics and be the product of certain procedural requisites.”).
327 Chrysler, 441 U.S. at 301-03.
328 Id. at 304.
329 See id. at 310, 312 (reviewing the statute at issue and concluding that its legislative intent did not authorize regulations permitting disclosure of trade secrets). Thus, an agency seeking to promulgate a rule authorizing disclosure of trade secrets must do so under authority conferred by its enabling statute(s), not the housekeeping statute.
Statutory grants of authority the . . . disclosure regulations . . . are reasonably within the contemplation of that grant of authority. The D.C. Circuit has elaborated that Congress need not expressly mention “trade secrets” in its delegation of information-gathering and disclosing authority for an agency’s regulation authorizing disclosure to pass muster under § 1905.

What kinds of authorizing regulations legalize agencies’ disclosure of trade secrets, bypassing the restrictions of the TSA? Here are four examples. All four are little-noticed in the legal academic literature on trade secrecy and intellectual property more broadly. Yet three of the four are good law, “on the books” today. These examples prove that federal regulators can and do formalize their legal authority to “break” trade secrets.

a. EPA

The Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA) requires that pesticide manufacturers submit detailed, otherwise confidential information about the formulas and properties of their pesticides to the EPA. FIFRA also delegates to EPA authority to determine whether and when this secret information can be disclosed outside the agency. Pursuant to this delegation, EPA promulgated a rule authorizing disclosure to certain parties outside the agency: EPA gives itself “authority to disclose any information to which this section applies to physicians, pharmacists, and other qualified persons needing such information for the performance of their duties, notwithstanding the fact that the information might otherwise be

---

330 Id. at 306; see also id. at 308 (“What is important is that the reviewing court reasonably be able to conclude that the grant of authority contemplates the regulations issued.”); Qwest Comm’ns Int’l Inc. v. F.C.C., 229 F.3d 1172, 1177 (D.C. Cir. 2000) (“[T]he [Chrysler] Court stated that ‘what is important’ is whether [a] reviewing court could reasonably conclude that the statutory grant of authority contemplated the regulations providing for release of information.”) (citing Chrysler, 441 U.S. at 308); Parkridge Hospital, Inc. v. Califano, 625 F.2d 719, 724 (6th Cir. 1980) (holding that a statute that provided, generally, that “no disclosure . . . shall be made except as the Secretary may by regulations prescribe” satisfied the Chrysler nexus standard); United States v. Nova Scotia Food Products Corp., 568 F.2d 240, 246 (2d Cir. 1977) (“When agency rulemaking serves the purposes of the statute, courts should refuse to adopt a narrow construction of the enabling legislation which would undercut the agency’s authority to promulgate such rules.”). But see an instance of a court finding a disclosure-authorizing regulation from NASA to fail the nexus test: J.H. Lawrence Co. v. Smith, 545 F. Supp. 421, 426 (D. Md. 1982).

331 See Qwest, 229 F.3d at 1178 (“Under Chrysler, § 1905 is satisfied without a provision of law that expressly refers to trade secrets.”).


333 See 7 U.S.C. § 136(a)(2)(D) (making it unlawful for any person to reveal any confidential information, except, for instance, when done in accordance with directions the Administrator may prescribe).
entitled to confidential treatment under this subpart.”  The rule also permits disclosure of pesticides’ formulas to the public: “[i]nformation to which this section applies, and which relates to formulas of products, may be disclosed at any public hearing or in findings of fact issued by the Administrator, to the extent and in the manner authorized by the Administrator or his designee.”

A different section of the same rule explicitly references the TSA and specifies the agency can disclose trade secrets. This rule has been on the books since 1978 and has seemingly never been challenged in court—likely because EPA has never actually exercised its authority under the rule to disclose pesticide data directly to the public.

b. FDA

In 2001, FDA proposed a rule that would have authorized the agency to begin disclosing secret data submitted by regulated entities on the safety and efficacy of gene therapies. The statutory basis of the proposed rule was 21 U.S.C. § 371, the provision of FDA’s enabling statute (the FDCA) that grants the agency general-purpose rulemaking authority: “authority to issue regulations for the efficient enforcement of” the FDCA as a whole. According to FDA, disclosure of secret data would be properly authorized “even if the information to be disclosed could be considered . . . within the scope of protection of the Trade Secrets Act (18 U.S.C. 1905).”

336 See 40 C.F.R. § 2.201(e) (2021) (outlining reasons of business confidentiality and federal agency obligations to trade secrets). 40 C.F.R. § 2.201(e) recognizes trade secrets and business confidentiality; 40 C.F.R. § 2.307 permits their disclosure by the agency in certain circumstances.
338 A Westlaw search turned up no instances of EPA exercising its disclosure authority formalized under 40 C.F.R. § 2.307(h)(1). EPA has faced sustained criticism from independent researchers and civil society groups for not disclosing details of pesticides to the public, apparently in deference to pesticide manufacturers’ claims of trade secrecy. See, e.g., Sharon Lerner, New Evidence About the Dangers of Monsanto’s Roundup, INTERCEPT (May 17, 2016), https://theintercept.com/2016/05/17/new-evidence-about-the-dangers-of-monsantos-roundup/ (discussing new evidence about mysterious ingredients in pesticides being brought to the courts); Ctr. for Env’t. Health v. McCarthy, 192 F. Supp. 3d 1076, 1042 (N.D. Cal. 2016) (holding that while EPA is permitted to require the listing of hazardous inert ingredients in pesticides, it is not mandated to).

340 Id. at 4694 (citing section 701(a) of the FDCA, codified at 21 U.S.C. § 371(a)).
341 Id. at 4694. This broad interpretation of FDA’s power to regulate under § 371 has been endorsed by courts, though the precise question of whether § 371 empowers FDA to create rules that authorize disclosure of trade secrets has not been litigated. See Nat’l Ass’n of Pharmaceutical Mfrs. v. FDA, 637 F.3d 877, 889 (2d Cir. 1981) (holding that 21 U.S.C. § 371(a) confers power to make
ultimately withdrew the proposed rule for undisclosed reasons, but it never repudiated its interpretation of § 371 as sufficient to support regulations authorizing disclosure of trade secrets.\footnote{\textit{Pharmaceutical Mfrs. v. Food & Drug Admin.}, 484 F. Supp. 1179, 1183 (D. Del. 1980) (finding that the FDA can make rules and regulations as necessary to carry out the provisions of the Act). In past work, Kapczynski and I argued that § 371 empowers FDA to promulgate regulations authorizing disclosure of a wide range of data on drugs and vaccines. See Morten & Kapczynski, supra note 54, at 538.}

c. HHS \& NIH

Pursuant to the Food and Drug Administration Amendments Act of 2007 (FDAAA), NIH operates the ClinicalTrials.gov website, the world’s largest public database of clinical trial data.\footnote{Guodong Liu, Gang Chen, Lawrence I. Sinoway, Arthur Berg, \textit{Assessing the Impact of the NIH CTSA Program on Institutionally Sponsored Clinical Trials}, 6 CLINICAL \& TRANSLATIONAL SCI. 196, 196 (2013).} NIH operates the website and manages submission and publication of data from hundreds of thousands of clinical trials.\footnote{ClinicalTrials.gov Background, NIH (May 2021), https://clinicaltrials.gov/ct2/about-site/background.} In 2014, NIH and its parent department, HHS, jointly proposed a rule that interprets FDAAA to require the sponsors of clinical trials of unapproved drugs, vaccines, and medical devices to report results of their trials to ClinicalTrials.gov.\footnote{Clinical Trials Registration and Results Submission, 79 Fed. Reg. 69,566, 69,566 (2014).} During the notice-and-comment period, industry commenters challenged the proposed rule on the basis that requiring submission and publication of results of trials of products not yet approved by FDA would violate the TSA. HHS and NIH responded that Congress had, through FDAAA, delegated to these agencies legal authority to gather trade secrets and subsequently to disclose them to the public through ClinicalTrials.gov:

\[
\text{[T]o the extent that clinical trial information, including but not limited to results information from applicable clinical trials of unapproved, unlicensed, or uncleared drugs and devices, described in [the relevant provisions of the FDAAA] and this final rule may contain trade secret and/or confidential commercial information, the requirement that such information be posted on ClinicalTrials.gov is authorized by law for the purposes of the U.S. TSA.}\footnote{Id. (emphasis added). The relevant portions of the FDAAA are codified at 42 U.S.C. § 282(j)(3)(D).}
\]

Since the FDAAA Final Rule took effect in 2017, trial sponsors have been legally required to submit protocols and results of trials of unapproved drugs, vaccines, and medical devices to ClinicalTrials.gov.
products to ClinicalTrials.gov, and NIH has promptly published them. Much of this information would otherwise remain unpublished and hidden from the public. Despite industry’s objections during the notice-and-comment period, no company has actually challenged the FDAAA Final Rule in court.

d. NTSB

In 2017, NTSB promulgated a rule that permits it to disclose certain trade secrets. According to the rule, NTSB understands itself to be:

authorized by 49 U.S.C. 1114(b) to disclose, under certain circumstances, confidential commercial information that would otherwise be subject to penalties for disclosure under the Trade Secrets Act, or excepted from disclosure under FOIA. The NTSB may exercise this authority when disclosure is necessary to support a key finding, a safety recommendation, or the NTSB’s statement of probable cause of an accident.

NTSB’s rule explicitly “applies to information the NTSB receives from any source that may be subject to the Trade Secrets Act (18 U.S.C. 1905) or the Freedom of Information Act (FOIA, 5 U.S.C. 552).” Congress expressly delegated to NTSB the authority it needed to create this rule: 49 U.S.C. § 1114(b)(1) specifies that “[t]he Board may disclose information related to a trade secret referred to in section 1905 of title 18” under certain circumstances enumerated in the statute. The rule has been criticized by industry—Boeing complained that it could “lead to the disclosure of ‘a broad range of Boeing trade secrets to the public’” but has not been challenged in court.

---

348 42 C.F.R. § 11.42(b).
349 See Deborah A. Zarin, Kevin M. Fain, Heather D. Dobbins, Tony Tse, & Rebecca J. Williams, 10-Year Update on Study Results Submitted to ClinicalTrials.gov, 381 N. ENG. J. MED. 1966, 1971 (Nov. 14, 2019), (finding that for a substantial number of unpublished trials, ClinicalTrials.gov provided the only public reporting of results).
350 49 C.F.R. § 831.6(b).
351 49 C.F.R. § 831.6(a).
352 The statute does require that any trade secrets disclosed by NTSB be disclosed “only in a way designed to preserve its confidentiality.” 49 U.S.C. § 1114(b)(2). NTSB has construed this statutory language “to require that the agency minimize the scope and extent of information released.” Investigation Procedures, 82 Fed. Reg. 29,670, 29,675 (Jun. 29, 2017). Under the same statute, trade secrets submitted voluntarily by regulated entities to NTSB enjoy greater protection, and NTSB will not disclose them if disclosure “would inhibit the voluntary provision of that type of information.” 49 U.S.C. § 1114(b)(3); see also 49 C.F.R. § 831.6(d) (excepting voluntarily provided safety information from NTSB disclosure under certain circumstances).
354 NTSB has apparently not yet disclosed a trade secret pursuant to the rule.
These examples show that any regulatory agency empowered by its enabling statute to gather and disseminate trade secrets can promulgate an “authorizing” regulation that formalizes this power. With the authorizing regulation in place, the agency need not evaluate whether a given secret is a “trade secret” for purposes of the TSA; the disclosure is legal. This is a feature, not a bug, of the TSA.\textsuperscript{355}

3. State Trade Secrecy Law, via the Takings Clause and Federal Tort Claims Act

The third and final significant legal limit on federal agencies’ authority to disclose corporate secrets is state trade secrecy law, which is made enforceable against the U.S. government, in different ways, by the Takings Clause of the Fifth Amendment and the Federal Tort Claims Act (FTCA). The relevant analyses are complex, but the ultimate punchline is simple: So long as disclosure serves some public purpose, state trade secrecy law cannot stop federal agencies from disclosing trade secrets. State trade secrecy law can only give rise to claims for money damages after disclosure occurs, and even then only under limited circumstances.

a. Takings

Some scholars have concluded that the Takings Clause poses a significant, even impassable, barrier to agency disclosure.\textsuperscript{356} That view is incorrect.

Let’s begin at the beginning. The Fifth Amendment’s Takings Clause guarantees that “private property” will not “be taken for public use, without just compensation.”\textsuperscript{357} Not everything is protected “property” eligible for protection under the Takings Clause\textsuperscript{358}; while the Supreme Court and the federal circuits have held some intangible assets—e.g., certain liens, contracts, and trade secrets—to be “property” eligible for protection under the Takings

\textsuperscript{355} See Chrysler, 441 U.S. at 298 (“We find nothing in the legislative history of [the TSA] and its predecessors which lends support to [the] contention that Congress intended the phrase ‘authorized by law,’ as used in [the TSA], to have a special, limited meaning.”).

\textsuperscript{356} See, e.g., Janka, supra note 44, at 367-68 (“Monsanto should be read as mandating full protection to the core common law right of trade secret protection.”); Epstein, supra note 94, at 300 (arguing that the Biologics Price Competition and Innovation Act of 2009, which requires disclosure of trade secret information in its biosimilar application process, effects both a per se and regulatory taking); Erika Lietzan, A New Framework for Assessing Clinical Data Transparency Initiatives, 18 MARQ. INT’L. PROP. L. REV. 33, 72 (2014) (“Forcible disclosure of trade secrets constitutes a taking.”); Fan, Private Data, supra note 57, at 183 (arguing that regulatory takings analysis poses a “roadblock” to trade secret disclosure statutes).

\textsuperscript{357} U.S. CONST. amend. V.

\textsuperscript{358} See, e.g., Air Pegasus of DC Inc. v. United States, 424 F. 3d 1206, 1212 (Fed. Cir. 2005) (“[A] threshold matter, the court must determine whether the claimant has established a property interest for purposes of the Fifth Amendment.”).
Clause,\textsuperscript{359} they have held that other intangible assets—e.g., federal welfare benefits—are not.\textsuperscript{360}

The Court has never articulated a precise test for determining whether a particular intangible asset qualifies as property eligible for protection by the Takings Clause. However, \textit{Ruckelshaus} did identify one dispositive feature of trade secrets that make them protectable under the Takings Clause: whether state law treats them like property.\textsuperscript{361} The same portions of \textit{Ruckelshaus} suggest that any corporate secrets that do \textit{not} meet the relevant state law definition of a trade secret are ineligible for protection under the Takings Clause, and can be disclosed freely by federal agencies without troubling it.\textsuperscript{362}

FOIA confirms this: For decades, federal agencies have disclosed information that qualifies as CCI under FOIA exemption 4 but does not qualify as a trade secret without effecting a taking.\textsuperscript{363}

That said, much confidential information important to regulators and to the public \textit{does} qualify as a trade secret for purposes of state law and consequently does implicate the Takings Clause.\textsuperscript{364} Now that the vast majority of states have adopted the UTSA, which defines a “trade secret” broadly,\textsuperscript{365} state-law definitions of a “trade secret” cover a wide swath of information.\textsuperscript{366} Moreover, the law of trade secrecy varies state-to-state and is

\textsuperscript{359} Ruckelshaus, 467 U.S. at 1003.

\textsuperscript{360} Bowen v. Gilliard, 483 U.S. 587, 605 (1987). The Federal Circuit recently observed that the question of whether patents constitute “property” eligible for protection under the Takings Clause is an open one. See Golden v. United States, 955 F.3d 981, 989 n.7 (Fed. Cir. 2020) ("Despite the Claims Court’s express finding on the status of patent rights under the Fifth Amendment, we decline to address that question here.").

\textsuperscript{361} See Ruckelshaus, 467 U.S. at 1001 ("Monsanto asserts that the health, safety, and environmental data it has submitted to EPA are property under Missouri law, which recognizes trade secrets, as defined in § 755, Comment b, of the Restatement of Torts, as property."); Id. at 1003 ("That intangible property rights protected by state law are deserving of the protection of the Takings Clause has long been implicit in the thinking of this Court.").

\textsuperscript{362} See Pamela Samuelson, \textit{Principles for Resolving Conflicts between Trade Secrets and the First Amendment}, 58 Hastings L.J. 777, 809 (2006) ("While proponents of the trade-secrets-as-property conception tend to invoke \textit{Ruckelshaus} as supporting the property concept, a fuller review of the Court’s ruling demonstrates that trade secret interests are balanced against other societal interests, and sometimes the larger societal interests override trade secret interests.").

\textsuperscript{363} See, e.g., \textit{RECOMMENDATION} 82-1 (June 17, 1982) https://www.acus.gov/sites/default/files/documents/82-1.pdf ("Agencies currently have discretion, subject to the limitations of the Trade Secrets Act (18 U.S.C. 1905), to release a submitter’s exempt (b)(4) information, even though disclosure might cause damage to the submitter.").

\textsuperscript{364} See supra note 363 (summarizing \textit{Ruckelshaus}'s holding that state-law definitions of "trade secret" control whether information is "property" for the purposes of the Takings Clause).

\textsuperscript{365} The UTSA defines a trade secret as any information that "is the subject of efforts that are reasonable . . . to maintain its secrecy" and that "derives independent economic value, actual or potential," from being secret from competitors who can "obtain economic value from its disclosure or use." UNIF. \textit{TRADE SECRET ACT} § 1.4 (UNIF. L. COMM’N 1985).

\textsuperscript{366} The federal DTSA does not create claims for trade secret misappropriation against the U.S. government—see supra note 291—but it does provide a distinct definition of "trade secret," very
less than crystal clear;\textsuperscript{367} as such, federal regulators may be understandably anxious to conclude incorrectly that a particular piece of information is not a trade secret.

Given all that, I turn to whether the Takings Clause actually prohibits disclosure of trade secrets, as defined under federal or state law. The answer is no, so long as the agency takes a single step: It makes no promise of ongoing confidentiality when it obtains the secret. \textit{Ruckelshaus} expressly held that agency disclosure of information obtained from a regulated entity can constitute a taking if and only if the agency provides an assurance of ongoing secrecy.\textsuperscript{368} If an agency provides no assurance of secrecy, disclosure of the secret effects no taking. That makes the takings analysis easy for federal regulatory agencies contemplating implementing forward-looking information publicity programs: Takings liability can be averted simply by refraining from any assurances of secrecy, whether through contract, policy, regulation, or direct communication with the regulated entity.


\textsuperscript{368} As the Court stated in \textit{Ruckelshaus},

\textquote{[T]he statute . . . gave Monsanto explicit assurance that EPA was prohibited from disclosing publicly . . . any data submitted by an applicant if both the applicant and EPA determined the data to constitute trade secrets. Thus, . . . the Federal Government had explicitly guaranteed . . . an extensive measure of confidentiality and exclusive use. This explicit governmental guarantee formed the basis of a reasonable investment-backed expectation."}

467 U.S. at 1011 (citation omitted). \textit{See also id. at 1007 ([A]s long as Monsanto is aware of the conditions under which the data are submitted, and the conditions are rationally related to a legitimate Government interest, a voluntary submission of data by an applicant in exchange for the economic advantages of a registration can hardly be called a taking.)); Love Terminal Partners, L.P. v. United States, 889 F.3d 1331, 1345 (Fed. Cir. 2018), cert. denied, 139 S. Ct. 2744 (2019) ("In \textit{Ruckelshaus}, . . . the Supreme Court concluded that plaintiffs only had a reasonable expectation in the confidentiality of trade secrets disclosed to the EPA in pesticide registration applications to the extent that the relevant statute explicitly guaranteed confidentiality at the time of submission."); Rowe, \textit{Striking A Balance}, supra note 68, at 802 ("Monsanto is . . . a mixed bag for trade-secret owners . . . . There is a real risk that when a company submits business information to an agency and it falls into the hands of a competitor, a court could find there was no promise of confidentiality, and thus no taking."). In this regard, the takings analysis for corporate secrets and other secret information dovetails with broader regulatory takings doctrine, which focuses on "the character of the governmental action, its economic impact, and its interference with reasonable investment-backed expectations." \textit{Pruneyard Shopping Ctr. v. Robins}, 447 U.S. 74, 83 (1980). If the submitter of confidential information to the government receives no assurance of continuing secrecy, then it has no "reasonable investment-backed expectation" of the same. \textit{Id.}
What about corporate secrets that regulators currently hold and have already promised to keep confidential? For these secrets, the takings analysis is more complex, but disclosure is nonetheless legal so long as it serves some public purpose. That is, so long as the regulator can articulate some public benefit that flows from the disclosure—straightforward enough in cases of publicizing corporate malfeasance, hazards to safety, public health, or the environment, and so on—then the taking will be deemed one for public use rather than private.369 A recent Supreme Court decision confirms a centuries-old principle: If a taking is for public use, the taking cannot be enjoined.370 The Takings Clause “is designed not to limit the governmental interference with property rights per se, but rather to secure compensation in the event of otherwise proper interference amounting to a taking.”371

Because a regulated entity whose secret has been disclosed by the U.S. government to serve the public interest cannot use the Takings Clause enjoin the disclosure, it may only seek money damages sufficient to make it whole—otherwise known as “just compensation.”372 The appropriate “just compensation” owed for an agency’s disclosure of a corporate secret shared pursuant to some assurance of secrecy may be small or large, depending on the scale of economic harm.373

---

369 Even the First Circuit’s errant Philip Morris decision acknowledges that disclosure of a trade secret to serve a significant state interest may be constitutional. 312 F.3d at 44 (noting that Massachusetts’ interest in promoting the health of its citizens could have been compelling enough to alter the court’s holding, but nevertheless finding a taking because the regulation was not sufficiently tailored to achieve this interest).

370 See Knick v. Twp. of Scott, Pa., 139 S. Ct. 2162, 2179 (2019) (“As long as just compensation remedies are available . . . injunctive relief will be foreclosed.”); see also Ruckelshaus, 467 U.S. at 1016 (“Equitable relief is not available to enjoin an alleged taking of private property for a public use, duly authorized by law, when a suit for compensation can be brought against the sovereign subsequent to the taking.”); Vogel, supra note 49, at 180 (“[I]f the Government misappropriates the secret for a public use, the owner is entitled only to just compensation . . . .”).


372 See Katrina Miriam Wyman, The Measure of Just Compensation, 41 U.C. DAVIS L. REV. 239, 248-50, 252 (2008) (analogizing the purpose of takings compensation to corrective justice’s goal of returning victims to their baseline and making them whole); see also Christopher Serkin, The Meaning of Value: Assessing Just Compensation for Regulatory Takings, 99 NW. U. L. REV. 677, 678 (2005) (discussing valuation theories of just compensation). In this scenario, the Taking Clause functions as a liability rule, entitling a party injured by government disclosure of its trade secret to some court-ordered measure of compensatory damages but not permitting it to charge an arbitrary price or prevent disclosure altogether.

373 See United States v. 564.54 Acres of Land, 441 U.S. 506, 511 (1979) (articulating the objective standard for just compensation). In this case, the court reasoned that just compensation was the “fair market value” of the property, which equaled “what a willing buyer would pay in cash to a willing seller at the time of the taking” and excluded the value that “springs from [an owner’s] subjective needs and attitudes” (citations omitted); see also Fla. Rock Indus. v. United States, 18 F.3d 1560, 1569 (Fed. Cir. 1994) (“[T]he amount of just compensation should be proportional to the value of the interest taken as compared to the total value of the property . . . .”).
b. Federal Tort Claims Act

As a background rule, the U.S. government enjoys sovereign immunity and may only be sued if it has waived that immunity.\(^{374}\) Via the Federal Tort Claims Act (FTCA), Congress enacted a limited waiver of immunity to permit private parties to sue the U.S. government in federal district court for some state law torts committed by its officials and agencies.\(^{375}\)

The Second,\(^{376}\) Fifth,\(^{377}\) D.C.,\(^{378}\) and Federal Circuits\(^{379}\) have held that the FTCA authorizes aggrieved plaintiffs to bring claims against the U.S. government for state-law trade secret misappropriation. Such claims are limited to compensatory money damages and can be brought only after agency disclosure occurs; trade secret holders cannot use the FTCA to enjoin agency disclosure or obtain punitive damages.\(^{380}\)

These circuits agree that in this sort of FTCA case, just as in takings and state law trade secret misappropriation cases, the defendant’s assurance of ongoing secrecy is key.\(^{381}\) The Supreme Court itself has observed, “[a]s a matter of state law, property rights in a trade secret are extinguished when a company discloses its trade secret to persons not obligated to protect the confidentiality of the information.”\(^{382}\) If the defendant agency did not promise secrecy, there is no viable FTCA claim.

\* \* \*

\(^{374}\) See, e.g., United States v. Sherwood, 312 U.S. 584, 586 (1941) (“The United States, as sovereign, is immune from suit save as it consents to be sued.”).


\(^{376}\) Kramer v. Sec’y, U.S. Dept of Army, 653 F.2d 726, 729-30 (2d Cir. 1980) (“he disclosed that information in confidence . . . . Under New York law, then, Kramer’s complaint states a cause of action . . . . [that] brings her claim within the purview of the Federal Torts Claim Act . . . .”).


\(^{379}\) U.S. Marine, Inc. v. United States, 722 F.3d 1360, 1365-66 (Fed. Cir. 2013) (“In the liability-imposing section of the FTCA . . . .Congress unequivocally imposed liability on the United States for torts, using state law to define the torts.”).


\(^{381}\) See Kramer, 653 F.3d at 730 (“[G]overnment employees agreed to honor [Kramer’s] demand that the information, once disclosed, be treated in confidence, and that she disclosed it only in reliance on this commitment.”); see also Jerome, supra note 376, at 1256 (“FDA induced JSP to disclose its trade secrets in confidence, and then it divulged that information to others in breach of that confidence.”).

By undertaking the controlled information publicity I propose in Part II, federal agencies can limit their liability under the Takings Clause and FTCA. Part II’s “bounded garden” model of information discourages commercial uses of publicized trade secrets, which limits financial harm inflicted on the source of the secret. By limiting this harm, agencies correspondingly limit their own financial downside. In this regard, the goals of regulators and regulated entities are helpfully aligned; regulators also have financial incentives to get the bounds on information publicity right.

Here is one example. In earlier work, Kapczynski and I proposed that the FDA begin disclosing certain currently-secret data on the safety and efficacy of pharmaceuticals submitted by pharmaceutical companies, despite past assurances of secrecy by the agency. The FDA can do this in harmony with the Takings Clause and FTCA by imposing data use agreements on any users of the data that prohibit them from using the data to compete directly with the companies that submitted the data.383 These agreements limit the risk of financial harm to the sources of this data and thereby limit the FDA’s own financial risk. In effect, they make information publicity affordable and pragmatic even for a cautious and penny-pinching federal agency—especially given the large social benefits of (controlled) disclosure and cost savings from mooting complex FOIA requests.384 FDA’s counterparts in Canada and the European Union already publicize exactly this kind of data and impose exactly this kind of data use agreement on data users—with a growing track record of success.385

C. Protecting Regulators from Challenge with Two Simple Steps

This Part’s preceding sections explained the wide-ranging legal authority that federal regulators have to disclose corporate secrets and the significant but navigable legal limits on that authority: (1) agencies’ enabling statutes, (2) the federal TSA, and (3) state trade secrecy law, made enforceable against the U.S. government via the Takings Clause and FTCA.

A bit of synthesis is in order. Imagine a federal regulator that seeks to build a long-term program of information publicity to inform the public of corporate activities and technologies that affect public welfare. What should that regulator do to ensure the program’s legality?

383 See Morten & Kapczynski, supra note 54, at 499-500 (“Data use agreements will be an important component of data disclosures . . .”).
384 Morten & Kapczynski, supra note 54, at 520-22 (“FOIA at the FDA has . . . flaws.”).
385 See supra § II.B.2.d (discussing Health Canada’s information publicity program); see also Egilman et al., Transparency of Regulatory Data, supra note 256, at 457 (describing the European Union’s information publicity program).
Recall that secrets that do not meet state or federal definitions of a trade secret are uncomplicated to disclose; these can generally be disclosed without any preparatory steps. It is only publicity of information that might meet the state or federal definition of a trade secret that can trigger legal liability.

To protect publicity of bona fide trade secrets from legal challenge, an agency should take two steps. First, the agency should promulgate an appropriate “authorizing regulation,” pursuant to some authority in the agency’s enabling statute, that formalizes the process of disclosing those secrets. The federal TSA permits disclosure of trade secrets so long as disclosure is permitted by a valid authorizing regulation promulgated by the agency (or is authorized by the plain text of an enabling statute).\footnote{Supra § III.B.2.b. (describing how a federal agency whose enabling statute permits the disclosure of trade secrets can overcome the federal TSA).} A regulation ensures adequate deliberative process. In proposing its authorizing regulation, and in the text of the rule itself, the agency should notify not just regulated entities but the broader public of its plan for information publicity. The agency should seek feedback from the industry and public alike on what sorts of technical and legal constraints on information access are acceptable. The final rule itself should articulate precisely what those constraints are.

Consider, again, the FAA. It currently asserts, categorically, that “[t]he Trade Secrets Act (TSA) prohibits the FAA and its employees from disclosing companies’ proprietary information” including details of the 737 MAX’s faulty MCAS.\footnote{Airworthiness Directives, \textit{supra} note 12, at 74578.} As I have argued here, the FAA’s categorical statement is incorrect as a matter of law. The TSA actually complicates disclosure only of information that meets the TSA’s narrow definition of a trade secret—\footnote{See supra § III.B.2.} not every scrap of Boeing’s purported “proprietary information.” In addition, if the FAA wanted to disclose information from Boeing that meets the TSA’s definition of a trade secret, it could do so if the agency first promulgated an appropriate authorizing regulation. The agency appears to have the requisite statutory authority to do so—Congress has delegated to the FAA sweeping authority to “issue, rescind, and revise such regulations as are necessary to carry out” the agency’s functions,\footnote{49 U.S.C. § 106(f)(3)(A).} and no provision of the FAA’s enabling statutes prohibits disclosure of trade secrets. Thus, the question of whether the FAA has legal authority to publicize trade secrets in the public interest is fundamentally a matter of regulation and agency will. And, on my reading, the FAA’s existing regulations do not
actually appear to prohibit the agency from disclosing trade secrets in its possession.\(^\text{390}\)

As a second step, the agency should ensure that it makes no assurances of secrecy to the entities from which it obtains those secrets, whether through separate rule,\(^\text{391}\) guidance or other publication, contract, or simple promise made directly to a regulated entity. By avoiding assurances of secrecy, the agency will preempt takings claims, and the agency will not be obliged to pay “just compensation” under the Takings Clause or damages under the FTCA.

While the FAA continues to keep Boeing’s secrets, another major regulator of transportation is gearing up for wider disclosure of secret details of errant transportation software, and it recently rescinded assurances of secrecy to smooth the way. As noted above,\(^\text{392}\) the NHTSA announced in 2021 that it will exercise discretionary authority to begin a laudable new proactive information disclosure program, sharing data on accidents involving self-driving cars. In announcing the program, the NHTSA made crystal clear that it is rescinding any assurance of ongoing secrecy:\(^\text{393}\) “The NHTSA . . . will not keep this information confidential, intends to make it publicly available, and is providing no assurance to you to the contrary.”\(^\text{394}\)

If a regulatory agency has taken these two preparatory steps—(1) promulgate an authorizing rule and (2) cease assurances of secrecy—it can legally publicize trade secrets within its possession. The agency cannot be enjoined, will not owe compensation, and will not be otherwise liable to the entity from whom the secret has been taken.

---

\(^{390}\) In fact, some FAA regulations are explicit that the FAA holds legal authority to disclose certain trade secrets when doing so is in “the public or national interest.” See 14 C.F.R. § 431.9(d) (governing confidentiality of materials submitted in connection with licensure of commercial space transportation—e.g., satellite launches).

\(^{391}\) For example, the FDA has constitutional and statutory authority to disclose trade secrets and CCI—see supra § III.B.2; see also Morten & Kapczynski, supra note 54, at 541 (“The FDA has all the statutory authority it needs to proactively disclose safety and efficacy data on pharmaceuticals.”). But also has, via rulemaking, promised not to exercise this authority. See 21 C.F.R. § 20.61(c) (“Data and information submitted or divulged to the Food and Drug Administration which fall within the definitions of a trade secret or confidential commercial or financial information are not available for public disclosure.”).

\(^{392}\) Supra § I.B.1.


\(^{394}\) Id. at 11.
D. Judicial Review Favors Agencies That Publicize Corporate Secrets

To bolster this Part’s claim that regulators can legally disclose private trade secrets, this Subpart briefly surveys a century of judicial review. In the small number of cases we have, the agencies almost always prevailed and paid no damages. Despite frequent saber-rattling, actual litigation over federal agencies’ disclosure of trade secrets is rare, and it favors the agencies.

Monsanto’s lawsuit against the EPA in the U.S. Supreme Court is the best-known of such litigation.395 As Pamela Samuelson has observed, Monsanto won only a qualified victory in that challenge: “[t]he strong property right theory [of trade secrecy] that Monsanto propounded was soundly trounced in Ruckelshaus.”396 The Supreme Court held that the EPA could legally share Monsanto’s trade secrets with the company’s competitors, and that the EPA was required to pay compensation to Monsanto only for sharing secrets gathered between 1972 and 1978—years during which the EPA had promised to keep Monsanto’s secrets secret.397 The Court held that Monsanto had no legal basis on which to enjoin or demand compensation for EPA’s sharing of trade secrets gathered from Monsanto in other years.398

Though Ruckelshaus was only a qualified victory for Monsanto, it constitutes a high-water mark for corporations that have sought to use federal courts to block administrative agencies from disclosing their trade secrets or to demand compensation after such disclosures. The facts of Ruckelshaus were unusual insofar as the agency shared Monsanto’s secrets with direct competitors, therefore giving, in the words of the District Court, “Monsanto’s competitors a free ride at Monsanto’s expense.”399 (Such pro-competitive sharing was precisely the point of FIFRA, the federal statute that provoked EPA’s disclosure; as the Supreme Court observed, “Congress believed that [FIFRA’s data-sharing] provisions would eliminate costly duplication of research and streamline the registration process, making new end-use products available to consumers more quickly.”400) The Supreme Court remanded for further proceedings and encouraged Monsanto to bring a takings claim for compensation in the Claims Court,401 but it appears Monsanto never actually did, let alone win and collect compensation from EPA.

395 Ruckelshaus, 467 U.S. at 998-99.
396 Samuelson, supra note 332, at 809.
397 Ruckelshaus, 467 U.S. at 1013-14.
398 Id. at 1013.
399 Id. at 999.
400 Id. at 1015.
401 Id. at 1020.
Where federal regulatory agencies have shared private trade secrets not with competitors but with noncommercial users, the regulators have successfully defended legal challenges. Despite Ruckelshaus’s long shadow, I cannot find a single case in which a court has actually ordered a federal agency to pay compensation under either the Takings Clause or FTCA for disclosure of a trade secret (or for disclosure of confidential commercial information).

Since 1982, all claims against the U.S. government for “just compensation” under the Takings Clause must be brought to a specialty court—until 1992, the U.S. Claims Court, and, since 1992, the U.S. Court of Federal Claims—and all appeals of such claims must be taken to the U.S. Court of Appeals for the Federal Circuit. Searches of these courts’ dockets turn up zero damages awards for taking of a trade secret. Corroborating this premise, takings claims seeking compensation for a federal agency’s disclosure of a trade secret are apparently so rare that the first precedential decision of the Federal Circuit that even mentions the possibility of such a claim was published in 2013. The small handful of merits decisions in cases concerning federal agencies’ disclosure of alleged trade secrets were all decided in the agencies’ favor, on the grounds that the information at issue did not actually contain trade secrets or that the agency in question had legal authority to disclose it.

Similarly, I cannot find a single case in which a district court has actually reached the merits and awarded an aggrieved trade secret holder compensation under the FTCA.

Owners of purported trade secrets have also sought to use Administrative Procedure Act (APA) litigation to enjoin agencies’ disclosures of private trade

403 United States Marine, Inc. v. United States, 722 F.3d 1360, 1373-74 (Fed. Cir. 2013) (recognizing the possibility of “a takings claim involving trade secrets” and citing Ruckelshaus).
404 See, e.g., Ervin & Assoc. v. United States, 59 Fed. Cl. 267, 313-315 (2004) (no taking because the relevant agency had contractual rights “to provide this information to third parties”); Block v. United States, 66 Fed. Cl. 68, 75 (2005) (no taking because the plaintiff had not sought or received any assurance of confidentiality from the relevant agency); Grayton v. United States, 92 Fed. Cl. 327, 337 (2010) (“[A]ny property interest he possessed in those ideas was destroyed when he shared those ideas without reservation with the SSA.”).
secrets. When the agency has an appropriate authorizing regulation in place, sanctioning disclosure of trade secrets, agencies win these APA challenges.406

In fact, I can find just one APA case decided since the Supreme Court’s 1979 Chrysler decision—which clarified the reach of the federal TSA407—in which a court actually enjoined a federal agency from proactive disclosure of alleged trade secrets because of what the court concluded was a violation of the TSA.408 That case concerned the Navy’s attempt to disclose confidential drawings and data a military contractor, Dowty Decoto, had submitted to the agency when fulfilling a supply contract.409 Over a decade after first submission of the information, the Navy informed Dowty Decoto that it intended to “disclose the data to third parties for the purpose of obtaining competitive bids.”410 In Dowty Decoto, the Ninth Circuit observed, correctly, that disclosure of trade secrets is permissible under the TSA whenever “authorized by law” and so focused on the Navy’s own “regulations governing [its] authority to disclose the data.”411 The court concluded that the relevant

---


407 See supra section III.B.

408 The case is Dowty Decoto, Inc. v. Dep’t of Navy, 883 F.2d 774, 781 (9th Cir. 1989). To be sure, other courts have, since Chrysler, restated the legal principle that a private entity can use APA litigation in federal district court enjoin a federal agency from disclosing trade secrets if such disclosure would violate the Trade Secrets Act or other federal law. See, e.g., Megapulse, Inc. v. Lewis, 672 F.2d 959, 971 (D.C. Cir. 1982) (holding that Megapulse’s suit alleging a violation of the Trade Secrets Act “was properly brought under the APA, and injunctive relief, preliminary or permanent, is available in the district court”). Some courts have enjoined federal agencies’ reactive disclosures to third party FOIA requests in so-called “reverse FOIA” APA litigation; in these cases, the sources of secret information can prove that the information requested by the FOIA requester is a trade secret for purposes of § 1905, that agency disclosure is “not authorized by law,” and thus that an injunction barring release is appropriate. See, e.g., Sealed Appellee #1 v. Sealed Appellant, 199 F.3d 437 (5th Cir. 1999) (prohibiting disclosure of certain materials); Canadian Com. Corp. v. Dep’t of Air Force, 514 F.3d 37, 43 (D.C. Cir. 2008) (holding that disclosure of materials is prohibited). In some of these “reverse FOIA” cases, courts have mistakenly conflated the proper APA analysis with the separate question of whether the information at issue is covered by FOIA exemption 4. See, e.g., Canadian Com., 514 F.3d at 39 (conflating those two separate analyses). As noted above, supra § III.A, this is incorrect, as FOIA itself should never bar an agency from disclosure.

409 The drawings and data described “repeatable holdback bars” used in launching fighter planes from aircraft carrier decks. Dowty Decoto, 883 F.2d at 775.

410 Id.

411 Id. at 776.
regulations did not authorize disclosure and that an injunction was therefore appropriate.412

CONCLUSION

This article has argued that federal regulators can and should embrace “information publicity”: controlled sharing with the public of certain secret information gathered from the industries they regulate. Regulators can and should legally share corporate secrets of intense public interest, even when those secrets are trade secrets. Rather than disclose trade secrets without condition, regulators should publicize these secrets in carefully bounded “gardens” that privilege socially valuable noncommercial users and uses while simultaneously protecting the information’s legitimate commercial value by thwarting competitive uses. By embracing information publicity, regulators can reconceive and reestablish their relationship the public they represent. In so doing, regulators can protect and educate the public and embrace, anew, a core feature of the original big-P Progressive vision of federal regulation.

Of course, not all agency-held secrets should be publicized. When prospective users of corporate secrets, and regulators themselves, cannot articulate socially valuable uses of the information, the secrets should stay secret. Likewise, secrecy should prevail when the regulator determines the risk of harm to a secret’s source or to other stakeholders to be particularly high. As I’ve argued above, the decision of whether and how to publicize information is a quintessential question for agency expertise and discretion—and for democratic contestation.

The preceding Parts presented a handful of pressing, practical examples where we might today imagine urging federal regulators to implement and expand information publicity: EPA with still-secret information on the safety of fracking; FAA and NHTSA with secret information on the “smart” software that governs the latest generation of autonomous transportation technology; FDA with secret data on the safety and efficacy of drugs, vaccines, and medical devices; and on and on. There are more potential applications of information publicity within the existing federal regulatory state that I lack space to sketch here but intend to explore in future work. I will mention one such application: HHS’s Office for Civil Rights (OCR) may have both authority413 and resources to investigate and publicize the uses that data brokers and artificial intelligence developers, including Google and

412 Id. at 776, 781.
413 See supra Part III.
Amazon, are secretly and controversially making of millions of Americans’ sensitive electronic health record (EHR) data.  

All this is not to say information publicity will be easy to achieve, particularly in a moment of industry capture and political crisis. My hope, perhaps Pollyannaish, is that federal regulatory officials will recognize information publicity as a pragmatic and relatively low-cost way to begin to rebuild public trust in the federal regulatory state without any compromise to the regulators’ “core” regulatory functions. (Elsewhere, Kapczynski and I have argued that FDA has far more to gain—in public health, in public esteem, and in concrete financial savings for the agency itself—from adopting information publicity than it has to lose.) Another hope, perhaps also Pollyannish, is that industry will cooperate, or at least come to accept regulators’ information publicity as a normal part of doing business.

Recall that the global pharmaceutical industry seems so far to have accepted, without much fight, Canada’s drug regulator’s flourishing data publicity program. Rowe has observed that regulated entities “may be willing to provide the information if and only if the integrity and safety of the information will be fully protected against direct or indirect disclosure to competitors.” This article’s proposal for information publicity seeks to protect them against disclosure to competitors and may be tolerable to industry for that reason.

While this article has focused on information publicity for noncommercial uses, to protect public health, environmental safety, and so on, I will observe briefly that the article raises even more provocative questions about the U.S. government’s legal authority to take and use trade secrets for commercial purposes. It seems to me, based on the analysis of Part III, that some federal regulators likely have constitutional and statutory authority share or use a private trade secret even in ways that compete directly with the trade secret’s source—subject, of course, to the same three legal limits presented in subpart III.B. Indeed, the now-decades-old pesticide-data-sharing program scrutinized by the Supreme Court in Ruckelshaus does precisely this. Of

---


415 See generally Morten & Kapczynski, *supra* note 52; Morten, Ramachandran, Ross, & Kapczynski, *supra* note 260.

416 See Kapczynski, *supra* note 87, at 1414, 1434-36 (arguing, both normatively and doctrinally, that regulators can condition access to the marketplace on market participants’ sharing of otherwise secret information, including trade secrets).

417 See *supra* section II.B.2.d.

418 Rowe, *supra* note 66, at 794. See also Sanfilippo, Frischmann & Strandburg, *supra* note 212, at 9 (observing that in the knowledge commons and privacy contexts, governance structures that “provide for the beneficial and managed flow of [] information within a legitimate and trusted institutional structure . . . encourage[e] subjects to share it”).
course, when agencies hand trade secrets to competitors of the secrets’ sources, the normative considerations involved are very different. So too when agencies themselves enter into competition with a secret’s source. I suspect that there are relatively few instances where this sort of exercise of regulators’ discretionary power over information is wise public policy. But the possibility is interesting indeed. Perhaps scholars preoccupied with the arm-in-arm march of corporate power and economic inequality should investigate the possibility of federal regulatory agencies as vehicles to “socialize” valuable information and bring it under public control.

I will close with an observation on both the present-day limits of information publicity and of its grander potential. Part III showed that the single most important constraint on federal regulators’ information publicity powers, and their governance of information more broadly, is federal statute. If Congress wishes to encourage, or even mandate, existing federal agencies to publicize more, it can do so simply by rewriting federal statute—especially the federal TSA and individual regulators’ enabling statutes. In addition, at this moment, essential spheres of social and economic activity exist largely or entirely outside the clear jurisdiction of an extant federal regulator, and a colorful panoply of legislators, policymakers, and scholars of many ideological persuasions have proposed to legislate new ones into being: a federal “Data Protection Agency,” a “Federal Robotics Commission,” an “FDA for Algorithms,” and so on. As we collectively debate the wisdom of these proposals, I think it is worth asking how, exactly, these would-be agencies would govern secrets, including trade secrets, drawn from the secretive industries they would regulate. Information publicity was once conceived as a core function of the federal regulatory state, and it could be again.