ARTICLE

PUBLICIZING CORPORATE SECRETS FOR PUBLIC GOOD

Federal regulatory agencies in the United States hold a treasure trove of valuable information essential to a functional society. Yet little of this immense and nominally "public" resource is accessible to the public. That worrying phenomenon is particularly true for the valuable information that agencies hold on powerful private actors. Corporations regularly shield vast swaths of the information they share with federal regulatory agencies from public view, claiming that the information contains legally protected trade secrets (or other proprietary "confidential commercial information"). Federal agencies themselves have largely acceded to these claims and even fueled them, by construing restrictively various doctrines of law, including trade secrecy law, freedom of information law, and constitutional law. Today, these laws—and fear of these laws—have reduced to a trickle the flow of information that the public can access. This should not and need not be the case.

This article challenges the conventional wisdom that trade secrecy law restricts public agencies' power to publicize private businesses' secrets. In fact, federal agencies, and regulatory agencies especially, have long held and still hold statutory and constitutional authority to obtain and divulge otherwise secret information on private actors, when doing so serves the public interest. For many regulatory agencies, that authority extends even to bona fide trade secrets. In an age of "informational capitalism," this disclosure authority makes U.S. federal regulatory agencies uniquely valuable—and perhaps uniquely dangerous. Building on recent work that explores this right in the context of drugs and vaccines, and drawing heavily from scholarship in privacy and information law, the article proposes a practical framework that regulators can use to publicize secret information in a way that maximizes public benefit and minimizes private harm. Rather than endorse unconstrained information disclosure—transparency for transparency's sake—this article instead proposes controlled "information publicity," in which regulators cultivate carefully bounded "gardens" of secret information. Within these gardens, agencies admit only certain users and certain uses of information. Drawing on existing but largely overlooked real-world examples, the article shows that regulators can effectively and selectively publicize trade secret information to noncommercial users while thwarting commercial uses. Regulators can protect trade secrets' integrity vis-à-vis competitors while simultaneously unlocking new, socially valuable uses.

Table of Contents

Publicizing Corporate Secrets for Public Good
Last revised February 13, 2022
DRAFT. Please do not share or cite without the author's permission.

Christopher J. Morten*
cjm2002@columbia.edu

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 products' safety and also contains some kernel of proprietary, commercially valuable knowledge. Each regulator thus faces a dilemma. On 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 the threat to their 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 harmed, even killed, by the products in question.

In 1941, inspectors of the Food & Drug Administration (FDA) discovered accidental but 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 competitor antibiotic manufacturers. Winthrop had, among other things, 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] After the inspection, Winthrop assured FDA that it could eliminate contamination quietly and resisted publicity of the problem.[3] Despite Winthrop's efforts to keep its manufacturing processes and problems secret, FDA elected to

* Associate Clinical Professor of Law, Columbia Law School, and Affiliated Fellow, Yale Law School. For helpful input, I thank Victoria Baranetsky, Courtney Cox, Gabrielle Daley, Megan Graham, Gautam Hans, Matthew Herder, Amy Kapczynski, Amanda Levendowski, David Levine, Varoon Mathur, Gabriel Nicholas, Blake Reid, Ira Rubinstein, Sharon Sandeen, Jason Schultz, Kathy Strandburg, Jacob Victor, Salome Viljoen, Michael Weinberg, and commentators at the Works-in-Progress Intellectual Property (WIPIP) Colloquium, Junior Tech Law Scholars Group, and NYU Tri-State Region IP Workshop. I thank Navya Dasari, Emma Li, Andrew Nassar, Elaina Ransford, and Kara Smith for invaluable research assistance. [Further acknowledgments TK, including student editors!]

[1] John P. Swann, *The 1941 Sulfathiazole Disaster and the Birth of Good Manufacturing Practices*, 41 PHARMACY IN HISTORY 16, 20 (1999).

[2] *Id.*

[3] *Id.*

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: 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 industry norm in the pharmaceutical industry today.[7]

In 2018 and 2019, hundreds of people died, tragically, in two separate crashes of Boeing's 737 MAX passenger jet.[8] After the first crash but before the second, regulators at the Federal Aviation Administration (FAA) determined that the cause of the crash was 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 plan was at risk of stalling.[9] After the first crash, the president of a major commercial pilots' union stated, "what 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 FAA withheld documentation of 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, Boeing's

[4] *Id.* ("On March 31st 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] *Id.* at 23.

[7] *Id.*

[8] Alec MacGillis, *After the Crash*, NEW YORKER (Nov. 18, 2019).

[9] Andrew Tangel & Andy Pasztor, *Regulators Found High Risk of Emergency After First Boeing MAX Crash*, WALL STREET JOURNAL (Jul. 31, 2019), https://www.wsj.com/articles/regulators-found-high-risk-of-emergency-after-first-boeing-max-crash-11564565521.

[10] Rob Mark, *Lion Air Investigation Takes an Unexpected Turn*, FLYING MAGAZINE (Nov. 15, 2018), https://www.flyingmag.com/lion-air-investigation-takes-an-unexpected-turn/?enews111518?src=SOC&dom=lkdn&utm_source=lkdn

alleged intellectual property.[11] 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 of the House Committee on Transportation & Infrastructure concluded that Boeing's and FAA's secrecy after the first crash contributed to the second, by preventing pilots and the public from learning of MCAS's design problems. [13] The same committee report documented myriad other regulatory failures of FAA and concluded that the agency had exerted "grossly insufficient oversight" overall—"the pernicious result of regulatory capture."[14]

In choosing public disclosure over secrecy in 1941, FDA kept the American public safe, warning the public away from a deadly product. But FDA did more than 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, 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; safer, higher quality drugs in the decades since; and over time improved public trust in both FDA and the companies it regulates. Despite Winthrop's protestations, FDA never suffered any legal liability for its disclosure of the company's secrets.

---

[11] *See, e.g.*, *Who's inspecting the inspectors of aircraft?*, DUBUQUE TELEGRAPH-HERALD (editorial) (Mar. 24, 2019), https://www.telegraphherald.com/news/opinion/article_04204644-8f06-5ece-8d39-d38daaebf219.html; Ralph Nader, *FAA's Boeing-Biased Officials: Recuse Yourselves or Resign*, COMMON DREAMS (Jun. 8, 2019), https://www.commondreams.org/views/2019/06/08/faas-boeing-biased-officials-recuse-yourselves-or-resign; Joe Cortez, *Consumer Advocate Demands Public Disclosure of 737 MAX Documents*, FLYERTALK (Nov. 30, 2020), https://www.flyertalk.com/articles/consumer-advocate-demands-public-disclosure-of-737-max-documents.html; David Koenig, *Waiting for passengers, American puts Boeing Max in the air*, SEATTLE TIMES (Dec. 2, 2020), https://www.seattletimes.com/business/waiting-for-passengers-american-puts-boeing-max-in-the-air/.

[12] Airworthiness Directives; The Boeing Company Airplanes, 85 Fed. Reg. 74,560, 74,578 (Nov. 20, 2020) (citing 18 U.S.C. § 1905). As I explain below, FAA is wrong here. *See infra* Part III.

[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, at 32, 99, 192. *See also* Mark, *supra* note [TK] (news article indicating that disclosure of flaws in MCAS could have informed pilots sufficiently to avert the second crash).

[14] House Report, *supra* note [TK], at 33, 6.

Eight decades later, 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.[15] In December 2019, an independent airline passengers' group, Flyers Rights, brought a Freedom of Information Act (FOIA) suit against FAA, seeking to compel the agency to disclose technical details of the flight control system.[16] 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."[17] 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.[18]

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"[19] and "infoglut." 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.[20] As Van Loo has described, today's federal regulatory state "emphasize[s] 'continuous' information

[15] *See supra* note [TK – Dubuque Telegraph-Herald, Seattle Times, etc.]

[16] *Flyers Rights Education Fund, Inc. v. FAA*, No. 1:19-cv-03749 (D.D.C. Dec. 16, 2019).

[17] ¶ 6 of Flyers Rights' complaint, *id.*

[18] *See infra* § I.B.1 (discussing NHTSA's new program disclosing information concerning autonomous vehicles).

[19] JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL (2019); Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460 (2020).

[20] *See* Rory Van Loo, *Regulatory Monitors: Policing Firms in the Compliance Era*, 119 COLUMBIA L. REV. 369 (2019); 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). *See also infra* § I.

flows," with regulators receiving and generating "real-time data" on the industries they oversee.[21]

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*."[22] Regulators collect and share information to educate the public on the industries and technologies that shape our lives—a precondition of the formation of public opinion and of democratic oversight of these industries and technologies, and of the regulators that regulate them.[23] Public access to information is essential not just to public health and safety but to democracy itself.[24] A democratic state cannot govern what it cannot understand.[25]

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.[26] Regulators today often decline to publicize harmful corporate activity and instead cooperate with wrongdoers to keep their secrets secret.[27] Why?

---

[21] Van Loo, *Regulatory Monitors*, *supra* note [TK] at 376.

[22] KRISTIN E. HICKMAN & RICHARD J. PIERCE, JR., ADMINISTRATIVE LAW TREATISE 2 (6th ed. 2019).

[23] *See, e.g.*, ROBERT C. POST, DEMOCRACY, EXPERTISE, ACADEMIC FREEDOM & FIRST AMENDMENT JURISPRUDENCE FOR THE MODERN STATE 27–35 (2012) (on relationship between expertise and democracy); Contreras, J. (2017). *Leviathan in the Commons: Biomedical Data and the State*, in K. STRANDBURG, B. FRISCHMANN, & M. MADISON (Eds.), GOVERNING MEDICAL KNOWLEDGE COMMONS 19-45 (on 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) (on FDA's role as information producer).

[24] On theories of the administrative state as essential to democracy, *see supra* note [just above]. *See also* Kirti Datla & Richard L. Revesz, *Deconstructing Independent Agencies (and Executive Agencies)*, 98 CORNELL L. REV. 769 (2013); Marshall J. Breger & Gary J. Edles, *Established by Practice: The Theory and Operation of Independent Federal Agencies*, 52 ADMIN. L. REV. 1111 (2000).

[25] JAMES C. SCOTT, SEEING LIKE A STATE: HOW CERTAIN SCHEMES TO IMPROVE THE HUMAN CONDITION HAVE FAILED (1998)

[26] *See infra* Part I.

[27] *See infra* Part I. *See also* Charles Tait Graves & Sonia Katyal, *From Trade Secrecy to Seclusion*, 109 GEORGETOWN L.J. 1337, 1352-68 (2021); Mary L. Lyndon, *Trade Secrets and Information Access in Environmental Law*, in THE LAW AND THEORY OF TRADE SECRECY (Rochelle C. Dreyfuss & Katherine J. Strandburg, eds., 2011).

This article analyzes one particularly important barrier—real or imagined—to federal regulators' publicizing companies' secrets: trade secrecy.[28]

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.[29] As Graves and Katyal have shown, companies claim that an expanding body of information on their activities meets this definition,[30] and that any sort of public disclosure of that information would constitute a violation of trade secrecy law.[31]

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.[32] Meanwhile, claims of trade secrecy now even hinder some regulators from obtaining, in the first place, information from the entities they supposedly regulate.[33]

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

---

[28] Of course, more than trade secrecy ails the federal regulatory state today. For deeper analysis, *see, e.g.*, Julie E. Cohen, *The Regulatory State in the Information Age*, 17 THEORETICAL INQUIRIES IN LAW 369 (2016); COHEN, BETWEEN TRUTH & POWER, *supra* note [TK], at 170; Rory Van Loo, *The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance*, 72 VAND. L. REV. 1563, 1605 (2019); CARY COGLIANESE, *Preface* to REGULATORY BREAKDOWN: THE CRISIS OF CONFIDENCE IN U.S. REGULATION vii (Cary Coglianese ed., 2012); Gillian E. Metzger, *Foreword: 1930s Redux: The Administrative State Under Siege*, 131 HARV. L. REV. 1, 39 (2017).

[29] Uniform Trade Secrets Act § 1(4); 18 U.S.C. § 1839(3); *Trade Secret*, BLACK'S LAW DICTIONARY (10th ed. 2014).

[30] Graves & Katyal, *supra* note [TK].

[31] *Id*. *See also* Deepa Varadarajan, *Business Secrecy Expansion and FOIA*, 68 UCLA L. Rev. 462 (2021).

[32] *See* Graves & Katyal, *supra* note [TK], 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, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV. 1183, 1240 (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"). *See also infra* Part I.

[33] *See, e.g.*, Varadarajan, *supra* note [TK] at 19 ("firms' invocation of trade secrecy can impede effective government oversight of private activities"); Mary L. Lyndon & David S. Levine, BLM Trade Secrets Comment (August 23, 2013), https://ssrn.com/abstract=2363284.

second contribution is normative—a claim about what federal agencies should do with those powers.

The article's first contribution is disproving the conventional wisdom that trade secrecy law, or any other existing body of law, creates a general bar against federal agencies publicizing corporate secrets. The 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 statute and reaffirmed repeatedly by the Supreme Court, that federal agencies have legal discretion to disclose information within their possession.[34] Even today's Roberts Court has acknowledged this authority, giving regulators meaningful room to maneuver.[35] Various constitutional and statutory sources of federal law—most notably the federal Trade Secrets Act[36] and the Fifth Amendment's Takings Clause—complicate disclosure and can make it expensive for the agency, but they do not prohibit disclosure.

It is simply untrue, as a matter of law, that trade secrecy law must prevent 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.[37]

Yet the view that trade secrecy law categorically prohibits disclose of private trade secrets to the public currently reigns, inside and outside the U.S. government. FAA and other agencies echo, again and again, the premise that federal law prohibits disclosure of private trade secrets.[38] 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."[39] Most

[34] *See infra* Part III.

[35] *See infra* Part III.

[36] 18 U.S.C. § 1905 *et seq*.

[37] *See* Christopher J. Morten & Charles Duan, *Who's Afraid of Section 1498? A Case for Government Patent Use in Pandemics and Other National Crises*, 23 YALE J.L. & TECH. 1 (2020).

[38] *See, e.g.*, *supra* note [TK – FAA stating disclosure is prohibited].

[39] U.S. Government Accountability Office, *Biomedical Research: NIH Should Publicly Report More Information about the Licensing of Its Intellectual Property*, GAO21-52 (Nov. 20, 2020), https://www.gao.gov/products/gao-21-52.

scholars, too, seem to have accepted the same premise—even leading scholars who support more disclosure as a normative matter and have advanced important alternative proposals to unearth information protected as trade secrets.[40] Levine, for example, has concluded that "both 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."[41] Wexler has written that, "[s]ince its common law origins, trade secret law has also protected information that is disclosed to government officials, whether the disclosure is compelled or undertaken voluntarily—for example, to obtain regulatory approval."[42] Bloch-Wehba has concluded that agency disclosure of trade secret decision-making algorithms is "legally *precluded* because these materials are the proper subject of trade secret

[40] *See, e.g.*, Van Loo, *The Missing Regulatory State*, *supra* note [TK] at 1605 (2019) (concluding that "[a]ny platform-monitoring [regulator] would need to mitigate the spread of trade secrets by limiting information collected only to that necessary and limiting the sharing of any information once it is collected"); Varadarajan, *supra* note [TK] at 22-23 ("[C]ourts have held that the Trade Secrets Act, a criminal statute, prohibits agencies from releasing information covered by Exemption 4."); Cary Coglianese, Richard Zeckhauser & Edward Parson, *Seeking Truth for Power: Informational Strategy and Regulatory Policymaking*, 662 MINN. L. REV. 277, 338 n. 227 (2004) ("information falling within the narrower category of trade secrets must be protected under the terms of the Trade Secrets Act. 18 U.S.C. § 1905"); Meredith Whittaker et al., AI Now Inst., *AI Now Report 2018*, 5 (2018), https://ainowinstitute.org/AI_Now_2018_Report.pdf [https://perma.cc/L5U6-8KM], at 22 ("When third-party vendors [of algorithmic decisionmaking software used in government] insist on trade secrecy to keep their systems opaque, it makes any path to redress or appeal extremely difficult."); Mary D. Fan, *Private Data, Public Safety: A Bounded Access Model of Disclosure*, 94 N.C. L. Rev. 161, 183 (2015) ("corporate privacy through trade secret protection remains vigorously alive and well in the lower courts after *Ruckelshaus*, posing a roadblock to general public disclosure statutes meant to protect health and safety"); John C. Janka, *Federal Disclosure Statutes and the Fifth Amendment: The New Status of Trade Secrets*, 54 U. CHI. L. REV. 334, 362 n.124 (1987) ("the Trade Secrets Act, 18 U.S.C. § 1905, prohibits government employees from disclosing trade secrets … ."); Joel D. Hesch, *The False Claims Act Creates A "Zone of Protection" That Bars Suits Against Employees Who Report Fraud Against the Government*, 62 DRAKE L. REV. 361, 408 (2014)
("the Trade Secrets Act prohibits government employees from disclosing trade secrets learned during the course of employment or official duties").

[41] David S. Levine, *The Impact of Trade Secrecy on Public Transparency*, in THE LAW AND THEORY OF TRADE SECRECY 406, 431–32 (Rochelle C. Dreyfuss & Katherine J. Strandburg, eds., 2011)

[42] Rebecca Wexler, *Life, Liberty and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1417-18 (2018)

protections."[43] With a few notable exceptions, including Bell,[44] Herder,[45] and Vogel,[46] the premise that trade secrecy law hamstrings government's ability to communicate with the public all has become the reigning conventional wisdom.

To be clear, regulators' trade secret-breaking power is not absolute. Via various enabling statutes, Congress has prohibited some federal regulators from disclosing trade secrets, as I explain below.[47] The most notable regulator so limited is the Federal Trade Commission (FTC); given FTC's unmatched information-gathering ability,[48] FTC's bar on disclosure of agency-held trade secrets is momentous. Nonetheless, numerous other powerful regulators, including the Environmental Protection Agency (EPA), FAA, Federal Communications Commission (FCC), FDA, and the Department of Health and Human Services' (HHS) Office for Civil Rights, retain broad authority to obtain and disclose trade secrets (and other secrets) they obtain from the companies they regulate.[49]

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 to share, and with whom, and on what terms? Real harms surely flow from overbroad disclosure, not just to individual companies affected but to entire industries and to the broader economy and public.

---

[43] Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265, 1270 (2020) (emphasis in original).

[44] Bernard Bell, *Food Marketing Institute: A Preliminary Assessment (Part II)*, YALE J. ON REGUL: NOTICE & COMMENT (Jul. 8, 2019), https://www.yalejreg.com/nc/food-marketing-institute-a-preliminary-assessment-part-ii [https://perma.cc/Y9P2-5BP2] (recognizing that a federal agency, "by notice and comment rulemaking, may grant itself the power to release" trade secret information).

[45] Mathew Herder, *Reviving the FDA's Authority to Publicly Explain Why New Drug Applications Are Approved or Rejected*, 178 JAMA INTERNAL MED. 1013, 1013 (2018) ("the barrier to greater disclosure is the FDA's interpretation of its governing laws rather than the laws themselves").

[46] David A. Vogel, *Government Agencies Can Misuse Your Trade Secret and You Can't Stop Them*, 28 PUB. CONTRACT L. J. 159 (1999).

[47] *See infra* section III.B.1.

[48] *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-we-do/enforcement-authority (last revised May 2021) (on investigative authority delegated under section 6(b) of the FTCA); *What the FTC Could Be Doing (But Isn't) To Protect Privacy*, Electronic Privacy Information Center (Jun. 2021), https://epic.org/wp-content/uploads/privacy/consumer/EPIC-FTC-Unused-Authorities-Report-June2021.pdf (same).

[49] *See infra* section III.B.1.

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. [50] 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.[51] 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 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*."[52]

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.

The bounded garden model of information publicity I propose here builds on recent proposals for "controlled" or "bounded" disclosure from Fan[53] and Kapczynski & myself.[54] It also draws heavily from recent work from scholars of

[50] Amy 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).

[51] For two leading analyses, *see* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1197 (2002); David Pozen, *Transparency's Ideological Drift*, 128 YALE L. J. 100, 108 (2018).

[52] Amy Kapczynski, *Data and Democracy: An Introduction*, The Knight First Amendment Institute (Data and Democracy Essay Series) (Nov. 10, 2021), https://knightcolumbia.org/content/data-and-democracy-an-introduction (emphasis in original).

[53] Fan, *Private Data, Public Safety*, *supra* note [TK] at 183; Mary D. M. Fan, *The Right To Benefit from Big Data as a Public Resource*, 96 NYU L. REV. 1438 (2021).

[54] Morten & Kapczynski, *supra* note [TK].

privacy and information law, especially Nissenbaum[55] and Solove.[56] To borrow Nissenbaum's term, what I propose is, in effect, a kind of "contextual integrity for trade secrets."[57] My proposal also draws on largely overlooked but vital and contemporary real-world experience with controlled disclosure of valuable information by regulators in contexts where trade secrecy, individual privacy, and other interests militate against unfettered disclosure.[58] In other words, I show that successful agency-run information publicity is already happening under our noses.

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 the normative case for reviving "information publicity"—controlled, conditioned disclosure of corporate secrets—and prescribes how it should be done. Part III presents a practical 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 perspective. 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 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 nonetheless has some commercial or financial value and is accordingly protected by FOIA's exemption for "commercial or financial information that is confidential or privileged" (also known as "confidential commercial information," or "CCI").[59] 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

[55] *Infra* note [TK – in Part II (Nissenbaum contextual integrity book and papers)].

[56] *Infra* note [TK – in Part II (Solove papers)].

[57] *See infra* section II.B for elaboration.

[58] *See infra* section II.B.2.d.

[59] 5 U.S.C. § 552(b)(4).

as embarrassing evidence of "illegal or unethical payments to government officials or violations of civil rights, environmental or safety laws."[60]

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, in general, legally disclose a corporate secret no matter whether it is a trade secret or CCI, assuming the agency takes certain preparatory steps.[61] 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.[62]

I. A Dangerous Status Quo

This Part tells a story of information flowing 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 number 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 increasingly inadequate. The problem of obsessive corporate secrecy has become deadly 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 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 remains today the dominant means by which the public obtains information from federal regulators. This picture forms the

[60] *Public Citizen Health Research Group v. FDA*, 704 F.2d 1280, 1291, n.30 (D.C. Cir 1983).

[61] *See infra* § III.

[62] *See infra* § II.

backdrop for a better solution: the proactive information publicity proposed in Part II.

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

U.S. federal regulators hold a massive amount of information, much of it gathered from the companies they regulate.[63] 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 (and double-checked by) FDA.[64] EPA maintains numerous databases on (*inter alia*) air and water pollution, environmental radiation, and the chemical and toxicological properties of pesticides.[65] The National Transportation Safety Board (NTSB) and FAA each hold vaults of information on commercial aircraft and airline accidents.[66]

These examples are just the tip of the informational iceberg frozen inside the federal regulatory state. Van Loo[67] and Coglianese, Zeckhauser & Parson[68] have analyzed federal administrative agencies' vast informational resources and mapped 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.

---

[63] *See generally* Van Loo, *Regulatory Monitors*, *supra* note [TK]; *see also* 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."); 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.").

[64] FDA, DRIVING BIOMEDICAL INNOVATION: INITIATIVES TO IMPROVE PRODUCTS FOR PATIENTS 22 (2011), https://www.celebrationofscience.org/assets/Uploads/DrivingBiomedicalInnovation-ImprovingProductsforPatients.pdf [https://perma.cc/U2XC-XHGA]; *see also* Morten & Kapczynski, *supra* note [TK].

[65] Philip Wexler et al., *Health effects of toxicants: Online knowledge support*, 145 LIFE SCI. 284 (2016), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4744126/.

[66] Justin T. Green, *When Rescue Is Too Risky: Medevac Flights Too Often Endanger the Lives They Were Dispatched to Save*, EMSWORLD (Feb. 27, 2006), https://www.hmpgloballearningnetwork.com/site/emsworld/news/10411580/when-rescue-too-risky-medevac-flights-too-often-endanger-lives-they-were-dispatched-save.

[67] Van Loo, *Regulatory Monitors*, *supra* note [TK]. *Inter alia*, Van Loo provides detailed data on various agencies' resources, including the size of their investigative workforces.

[68] Coglianese, Zeckhauser & Parson, *Seeking Truth for Power*, *supra* note [TK] at 305.

First, the federal administrative state has changed significantly in recent decades and continues to change. Several interrelated trends have joined forces to sap many federal 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.[69] Rebuilding the federal regulatory state will require, *inter alia*, restoring agencies' information-gathering authority. Thus, the question of what precise information the federal regulatory state holds at this moment 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—as Parts II and III propose—will jeopardize other vital elements of the regulators' work. That concern has been elaborated most thoroughly by Rowe,[70] but it has been echoed by courts[71] and by administrative agencies themselves.[72] 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 within a given industry, its "collegial" relationship with that industry may be permanently altered. 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.[73]

---

[69] *See, e.g.*, Metzger, *supra* note [TK]; Pozen, *Transparency's Ideological Drift*, *supra* note [TK]; Cohen, *The Regulatory State in the Information Age*, *supra* note [TK]; Lisa Heinzerling, *Quality Control: A Reply to Professor Sunstein*, 102 CAL. L. REV. 1457 (2014); Frank Pasquale, *Cost-Benefit Analysis at a Crossroads: A Symposium on the Future of Quantitative Policy Evaluation*, LPE BLOG (Sep. 27, 2021), https://lpeproject.org/blog/cost-benefit-analysis-at-a-crossroads-the-future-of-quantitative-policy-evaluation/.

[70] Rowe, *Striking A Balance*, *supra* note [TK].

[71] The canonical case is *Critical Mass Energy Project v. NRC*, 975 F.2d 871 (D.C. Cir. 1992) (en banc), *cert. denied*, 507 U.S. 984 (1993). *Critical Mass* is preoccupied with how to encourage "voluntary" submissions of information by regulated entities to regulators. *See id.* at 878. [cite addnl cases in memo in *National Parks*-era "impairment" cases under FOIA exemption 4]

[72] *See, e.g.*, Securities & Exchange Commission, *Requests for Confidential Treatment of Records Obtained by the Commission*, 45 Fed. Reg. 1627, 1628 (1980) ("The 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 …."); EPA, *Nanoscale Materials Stewardship Program*, 73 Fed. Reg. 4861, 4864 (2008) (similar).

[73] Rowe, *Striking A Balance* at 794 ("[S]ometimes they 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.")

That concern is important but entirely manageable, in my view. It is manageable because, as this subpart shows, federal regulators have power to get information even if their relationships with industry become less "collegial." And, as Cohen[74] and others have written, 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 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. I summarize here two varieties of that power—premarket approval and investigative.[75]

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 market or sell that good or service.[76] Among the federal regulators that wield premarket approval power are FDA (with respect to essentially all prescription drugs[77] and vaccines[78] and many, though not all, medical devices[79]), EPA (pesticides[80]), Department of Defense (military equipment and other defense contracting[81]), and FAA (design and manufacture of commercial airplanes, operation of commercial airlines[82]).

---

[74] Cohen, *The Regulatory State in the Information Age*, *supra* note [TK] at 2.

[75] 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.

[76] *See, e.g.*, FDA, Premarket Approval (PMA), https://www.fda.gov/medical-devices/premarket-submissions/premarket-approval-pma ("The applicant must receive FDA approval of its PMA application prior to marketing the device.").

[77] 21 U.S.C. § 355 & 42 U.S.C. § 262.

[78] 42 U.S.C. § 262.

[79] 21 U.S.C. § 360e.

[80] 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).

[81] 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).

[82] 49 U.S.C. §§ 40113, 44701, 44704, 44709, 44711, and 44713 establish FAA's certification process and mandate that aircraft cannot fly in U.S. airspace without FAA certification. FAA's premarket approval rules are set out at 14 CFR Subchapter C.

Under premarket approval review regimes, regulators require applicants to make certified submissions of large quantities of information on their products and services, which is 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.[83] Regulated entities that decline to submit the required information are barred from the market.[84]

Regulated entities have argued in the past[85] 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[86] or other constitutional theory. But the Supreme Court has foreclosed this argument: in *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.[87] *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."[88]

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.[89] A 2002 en banc decision of the First Circuit attempted to cabin

[83] Morten & Kapczynski, *supra* note [TK].

[84] *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* Rowe, *Striking a Balance*, *supra* note [TK] at 818; Amy Kapczynski, *The Public's Secrets: The Law and Political Economy of Trade Secrets*, U.C. DAVIS L. REV. (forthcoming 2022).

[85] *See supra* note [TK] (discussing *Philip Morris*).

[86] For a more thorough discussion of the Takings Clause and its interaction with federal agencies' disclosure authority, s*ee infra* § III.B.3.

[87] *Ruckelshaus*, 467 U.S. at 1007.

[88] *Id.* at 1007 (internal quotation marks and citations omitted). *See also Corn Products 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, *The Public's Secrets*, *supra* note [TK].

[89] *See* Janka, *supra* note [TK]; Richard A. Epstein, *The Constitutional Protection of Trade Secrets and Patents Under the Biologics Price Competition and Innovation Act of 2009*, 66 FOOD & DRUG

Ruckelshaus into near-oblivion, suggesting that it had effectively been overruled *sub silentio* by subsequent Supreme Court decisions.[90] In that case, the tobacco giant Philip Morris managed to defeat a Massachusetts state law that would have required it to disclose to regulators and the public a complete list of the ingredients in its cigarettes.[91] But, unlike the First Circuit, the Supreme Court has consistently reaffirmed *Ruckelshaus*, and this specific holding, as good law, as recently as 2019.[92] If this aspect of *Ruckelshaus* has been cabined at all by the Court, 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.[93]

2. Investigation

Most federal regulators—even those that lack premarket approval authority—possess a second, similarly potent tool to collect data from regulated entities:

L.J. 285 (2011). Epstein argues extensively that this element of *Ruckelshaus*'s holding exists in some tension with later Supreme Court decisions on the unconstitutional conditions doctrine and the reach of the Takings Clause. Epstein, *Constitutional Protection* at 304-13. Yet even Epstein acknowledges that the Court "tiptoe[d] around" *Ruckelshaus* rather than overrule it. *Id.* at 308.

[90] *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 *Ruckelshaus*, and electing instead to apply the reasoning of a later Supreme Court decision, *Nollan v. Cal. Coastal Comm'n*, 483 U.S. 825, 833 n. 2 (1987)).

[91] *Id.*

[92] *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 Agriculture*, 576 U.S. 350, 365 (2015); *Knick v. Township of Scott, PA*, 139 S. Ct. 2162, 2173 (2019).

[93] *Horne v. Dep't of Agric.*, 576 U.S. 350, 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.").

investigation.[94] 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.[95] As Van Loo has written, "[i]n many agencies, regulatory monitors combine prosecutors' enforcement and adjudication authority with the patrol function of police officers and the investigatory function of detectives." The only real limit is that the information gathering must serve the regulator's statutorily-defined regulatory function.[96]

Among the many federal regulators with strong investigative authority resources are the U.S. Department of Agriculture (USDA) (which, *inter alia*, sends investigators into slaughterhouses and meat processing plants[97]), CMS (which investigates, *inter alia*, medical testing laboratories[98]), EPA (which investigates, *inter alia*, water pollution,[99] oil tankers,[100] and makers and distributors of pesticides[101]), FAA (which investigates, *inter alia*, aircraft manufacturers and commercial airlines[102]), FDA (which investigates, *inter alia*, drug manufacturing

[94] In this paper, I use the term "investigative" broadly, to refer to all information-gathering activities that do not involve premarket approval and do not 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. "Investigation" includes what Van Loo terms "visitation" and "reporting" and encompasses regulators' on-site inspections, subpoenas of records, interviews with employees, etc. *See* Van Loo, *Regulatory Monitors* at 381.

[95] Coglianese, Zeckhauser & Parson, *Seeking Truth for Power*, *supra* note [TK] at 307; KRISTIN E. HICKMAN & RICHARD J. PIERCE, JR., ADMINISTRATIVE LAW TREATISE 940 (6th ed. 2019) ("Most agencies have broad powers to compel reports."); *id.* at 950 (the prevailing "legal framework renders it difficult for any private party to prevail in a subpoena enforcement dispute"); Van Loo, *Regulatory Monitors*, *supra* note [TK] 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").

[96] KRISTIN E. HICKMAN & RICHARD J. PIERCE, JR., ADMINISTRATIVE LAW TREATISE 941, 946, 950, 983 (6th ed. 2019).

[97] 21 U.S.C. § 601 et seq. *See, e.g.*, Michael Moss, *The Burger That Shattered Her Life*, N.Y. TIMES (Oct. 3, 2009), https://www.nytimes.com/2009/10/04/health/ 04meat.html (describing USDA investigation of *E. coli*. contamination at a beef-packing plant).

[98] *CLIA Program & Medicare Lab Services*, CMS (Dec. 2021), https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/CLIABrochure.pdf.

[99] 33 U.S.C. § 1318.

[100] 33 U.S.C. § 1321.

[101] 7 U.S.C. § 136g.

[102] 49 U.S.C. § 44709(a).

facilities[103] and clinical trials[104]), FTC (which has wide-ranging authority to investigate most any corporate activity that affects competition and consumer welfare[105]), the Department of Health and Human Services's (HHS) Office for Civil Rights (OCR) (which investigates compliance with medical data privacy rules and with federal civil rights laws in the health care context[106]), and the NTSB (which possesses authority to, *inter alia*, investigate the causes of aviation and other transportation accidents[107]). 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 the industries they regulate. This subpart turns to how regulators share those secrets with the public—or 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, highlighted in the Introduction, these programs inform the public of corporate malfeasance and keep the regulators themselves publicly accountable.

---

[103] 21 U.S.C. § 374.

[104] *Bioresearch Monitoring Program Information*, FDA (Sep. 9, 2020), https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/fda-bioresearch-monitoring-information/bioresearch-monitoring-program-information.

[105] *See* 15 U.S.C. §§ 43, 46(a). For analysis of FTC's potent investigative powers, *see* Van Loo, *The Missing Regulatory State*, *supra* note [TK] at 1617; *see also* Andrea Vittorio, *FTC's Demand for Tech Company Data Shows 'Underutilized' Power*, BLOOMBERG LAW (Dec. 16, 2020), https://www.bloomberglaw.com/document/X4QGLMRK000000;

[106] *Infra* § III.B.

[107] *The Investigative Process*, NTSB, https://www.ntsb.gov/investigations/process/Pages/default.aspx

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.[108] For example, between 2016 and 2020 FDA published a series of these reports documenting ongoing mold contamination at an ostensibly sterile drug manufacturing plant in Kansas, operated by Pfizer.[109] Ensuing media coverage[110] (plus FDA's chastisement) helped prompt Pfizer to improve its safety protocols—just in time for the plant to begin packaging and shipping the Pfizer-BioNTech COVID-19 vaccine.[111]

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.[112] In CMS's words, the agency makes such reports—so-called "Form CMS-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."[113] 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

[108] *Inspection Observations*, FDA (Nov. 24, 2020), https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/inspection-references/inspection-observations (describing reports); *ORA FOIA Electronic Reading Room*, FDA, https://www.fda.gov/about-fda/office-regulatory-affairs/ora-foia-electronic-reading-room (links to reports). FDA denotes these as "Form 483" reports.

[109] 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/

[110] *See, e.g.*, Suzanne Elvidge, *Troubled Pfizer plant faces more criticism in Form 483*, BIOPHARMA DIVE (Dec. 13, 2018), https://www.biopharmadive.com/news/pfizer-mcpherson-form-483-fda-warning-manufacturing/544242/.

[111] Tribble, *supra* note [TK].

[112] 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.");

[113] 82 Fed. Reg. 19,796, 20,143 (Apr. 28, 2017).

Theranos.[114] 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."[115] 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.[116] CMS's disclosure thus helped to drive a dangerous device out of public 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.[117] 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."[118] NHTSA's acting administrator stated that "gathering data will help instill public confidence that the federal 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."[119]

---

[114] John Carreyrou, *U.S. Health Regulators Release Lightly Redacted Theranos Letter, Inspection Report*, WALL STREET JOURNAL (Apr. 25, 2016), https://www.wsj.com/articles/u-s-health-regulators-release-lightly-redacted-theranos-letter-inspection-report-1461631843.

[115] 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.

[116] John Carreyrou, *Theranos Voids Two Years of Edison Blood-Test Results*, WALL STREET JOURNAL (May 18, 2016), https://www.wsj.com/articles/theranos-voids-two-years-of-edison-blood-test-results-1463616976; Ken Alltucker, *As Theranos drama unwinds, former patients claim inaccurate tests changed their lives*, USA TODAY (Jul. 5, 2018), https://www.usatoday.com/story/news/nation/2018/07/05/theranos-elizabeth-holmes-lawsuits-patients-harm-arizona/742008002/.

[117] Audrey LaForest, *NHTSA orders mandatory crash reports for cars with automated-driving tech*, AUTOMOTIVE NEWS (Jun. 29, 2021), https://www.autonews.com/regulation-safety/nhtsa-orders-mandatory-crash-reports-cars-automated-driving-tech.

[118] Standing General Order 2021-01, NHTSA (Jun. 29, 2021), https://www.nhtsa.gov/sites/nhtsa.gov/files/2021-06/Standing_General_Order_2021_01-digital-06292021.pdf at 11.

[119] *NHTSA Orders Crash Reporting for Vehicles Equipped with Advanced Driver Assistance Systems and Automated Driving Systems*, NHTSA (Jun. 29, 2021), https://www.nhtsa.gov/press-releases/nhtsa-orders-crash-reporting-vehicles-equipped-advanced-driver-assistance-systems

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—have resisted calls to share secret information on the businesses they regulate. Some have retreated from past practices of disclosure. The story of FAA's ongoing refusal to disclose data on Boeing's 737 MAX, told in the introduction, 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. Under both Democratic and Republican presidents, the federal regulators that hold this information—the EPA and Bureau of Land Management (BLM)—have refused to disclose it.[120] A representative of the environmental group Environmental Integrity Project (EIP) said EIP 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 public database of hazardous chemicals and wastes the regulator compiles."[121] "The regulator, not the company, determines if chemicals can be kept from public view as a trade secret"—and the EPA chose secrecy.[122] 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 of the secret formulas.[123] President Biden has not reinstated the rule.

In fact, under the Trump administration, multiple federal regulators that had historically cultivated important proactive disclosure programs ended them. As of writing, these disclosure programs have not been revived under President Biden. For example, for decades, the USDA disclosed inspection reports compiled by the

---

[120] *See* Graves & Katyal, *supra* note [TK] at 1358. *See also* Lyndon, *Trade Secrets and Information Access in Environmental Law*, *supra* note [TK]; Lyndon & Levine, *BLM Trade Secrets Comment*, *supra* note [TK].

[121] Neela Banerjee, *Fracking Companies Keep 10% of Chemicals Secret, EPA Says*, INSIDE CLIMATE NEWS (Mar. 31, 2015), https://insideclimatenews.org/news/31032015/fracking-companies-keep-10-chemicals-secret-epa-says/.

[122] *Id.*

[123] Charles T. Wehland, Will Taylor & Diane Myers, *Litigation Update: Repeal of the Obama Fracking Rule*, ABA ENVIRONMENTAL & ENERGY LITIGATION COMMITTEE (Jun. 14, 2018), https://www.americanbar.org/groups/litigation/committees/environmental-energy/articles/2018/spring2018-litigation-update-repeal-of-the-obama-fracking-rule/.

Animal and Plant Health Inspection Service (APHIS). These reports document mistreatment, abuse, and death of animals in research laboratories, zoos, equestrian centers, and other businesses that rely on animals.[124] In 2017, the USDA removed all such reports from its website, reportedly under pressure from businesses that had been criticized by animal rights groups after disclosures of abuse.[125]

Similarly, for decades FDA maintained a program in which, upon approval of a new drug or vaccine, it disclosed detailed "reviews" prepared by its expert scientists that summarize the product's therapeutic, chemical, and other properties for the public.[126] In July 2019, FDA announced that it will cease posting complete reviews and instead make public only a single condensed "integrated review."[127] FDA's shift from to less information-rich, more "integrated" reviews was welcomed by industry[128] 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.[129]

Around the same time, 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[130] and abandoned a second initiative to publicize near-complete Clinical Study Reports (CSR) that would have provided a detailed look at important "pivotal" clinical trials on FDA-approved

---

[124] Kevin Brulliard, *USDA abruptly purges animal welfare information from its website*, WASHINGTON POST (Feb. 3, 2017).

[125] *Id.*

[126] 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).

[127] *Id.*

[128] *See, e.g.*, Pharmaceutical Research and Manufacturers of America (PhRMA), Comment Letter on FDA's Notice, "New Drugs Regulatory Program Modernization: Improving Approval Package Documentation and Communication" (Aug. 26, 2019), https://www.regulations.gov/comment/FDA-2019-N-2012-0022; Biotechnology Industry Organization (BIO), Comment Letter on FDA's Notice, "New Drugs Regulatory Program Modernization: Improving Approval Package Documentation and Communication" (Aug. 25, 2019), https://www.regulations.gov/comment/FDA-2019-N-2012-0012.

[129] Peter Doshi et al., Comment Letter on FDA's Notice, "New Drugs Regulatory Program Modernization: Improving Approval Package Documentation and Communication" (Aug. 23, 2019) https://www.regulations.gov/comment/FDA-2019-N-2012-0010.

[130] 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.

drugs and vaccines.[131] Medical researchers and consumer watchdog groups such as Public Citizen had advocated these disclosure programs for years and lamented FDA's retreats.[132] But the pharmaceutical industry cheered. One of the two leading pharma industry trade organizations had expressed "serious concerns" with FDA's rescinded plan to publicize CSRs, alleging (unsubstantiated) incompatibility "with global disclosure and data protection policies."[133] The other leading trade organization similarly contended that the same rescinded plan had threatened "commercially confidential information" necessary "to protect a Sponsors' [*sic*] intellectual property rights and further commercial development."[134]

In summary, as of today, regulators' programs for proactive disclosure of corporate secrets of public interest within their possession are important but scattered. [135] 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."[136] Over the past two decades or so, major federal initiatives along these lines, including the Obama Administration's Open Government Initiative[137] and 2019's OPEN Government Data Act,[138] have expanded public access to some forms of data held by the U.S. government. It may seem paradoxical for the government to grow at once more secretive and more open, but the distinction is straightforward: These open government and open data

[131] Zachary Brennan, *FDA Ends CSR Pilot, Plots New Approach for Disclosing Study Reports*, RAPS REGULATORY FOCUS (Mar. 26, 2020), https://www.raps.org/news-and-articles/news-articles/2020/3/fda-ends-csr-pilot-plots-new-approach-for-disclosi.

[132] Sammy Almashat & Michael Carome (Public Citizen), *Withholding Information on Unapproved Drug Marketing Applications: The Public Has a Right to Know* (Feb. 1, 2018), https://www.citizen.org/news/withholding-information-on-unapproved-drug-marketing-applications-the-public-has-a-right-to-know/.

[133] PhRMA Comment, *supra* note [TK].

[134] BIO Comment, *supra* note [TK].

[135] Graves & Katyal document additional recent examples of federal regulators withholding information despite public outcry, such as EPA's refusal to share data on Teflon. *Supra* note [TK] at 1355.

[136] For a summary of recent open government and open data initiatives, *see*, Daniel Berliner, Alex Ingrams & Suzanne J. Piotrowski, *The Future of FOIA in an Open Government World: Implications of the Open Government Agenda for Freedom of Information Policy and Implementation*, 63 VILL. L. REV. 867, 870-76 (2019).

[137] *See*, Fact Sheet: Data by the People, for the People — Eight Years of Progress Opening Government Data to Spur Innovation, Opportunity, & Economic Growth, White House Press Secretary (Sep. 28, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/09/28/fact-sheet-data-people-people-eight-years-progress-opening-government.

[138] Pub.L. 115–435.

initiatives mandate broader access to data generated by the government itself—on climate, transportation, and so on. Much of this data is not just generated by the government but is *about* the government—it concerns the U.S. government's own spending and its performance in health, education, and other fields. Via various open government initiatives, the U.S. government has today arguably made itself more open to public scrutiny than ever, even as it shields the industries it regulates from the same.[139]

C. The Public Has No Good Alternatives

The preceding subpart showed that today's federal regulators do not maintain consistent, effective proactive disclosure programs to share secret information on corporate activity, even 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 that information 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.[140] FOIA makes disclosure the default rule, thought it carves out nine seemingly narrow categories of information as exempt from the presumption of disclosure.

Yet, in reality, FOIA has four key flaws.[141] First, FOIA requests are reactive and require the requester to know precisely what information she needs before she

[139] *See*, generally, Pozen, *Transparency's Ideological Drift*, *supra* note [TK]; *see also* Kapczynski, *Dangerous Times*, *supra* note [TK]. As Pozen, Kapczynski, and others have argued, it's no surprise to see these two trends occur in tandem; transparency has been weaponized as a tool against the state.

[140] 5 U.S.C. § 552.

[141] Kapczynski and I described these at greater length in a recent paper. Morten & Kapczynski, *supra* note [TK] at 520.

asks.[142] Second, FOIA requests are slow, sometimes taking years to produce the documents the requester seeks.[143] Third, FOIA requests are resource-intensive for requesters, often requiring sophisticated and expensive legal help.[144] Fourth, FOIA requests are highly deferential to industry; agencies can and do legally withhold information that regulated entities ask the agencies to keep secret.[145]

The second and fourth flaws are intertwined; agencies defer to industry in significant part because it is much easier to defer. Today, FOIA offices throughout the federal administrative state are overwhelmed with requests. Kwoka has calculated that in just two years (2013 and 2014), the U.S. government received over 700,000 FOIA requests.[146] The average FOIA request takes months to fulfill, and complex requests often linger for years.[147] 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 55 years to fulfill it.[148] At federal regulators, the never-ending flood of requests comes mostly from commercial users—often public corporations using FOIA to gather "competitive intelligence" on the regulator's plans as well as their direct competitors. [149]

Each FOIA request requires a bespoke response, even if numerous requesters seek the same types of information over and over again. 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."[150]

---

[142] *Id.* at 520.

[143] *Id.* at 521.

[144] *Id.*

[145] *Id.* at 522.

[146] Margaret B. Kwoka, *FOIA, Inc.*, 65 DUKE L.J. 1361, 1364 (2016).

[147] *Id.* at 1374-75. *See also* Morten & Kapczynski, *supra* note [TK] at 521.

[148] Jenna Greene, *Wait what? FDA wants 55 years to process FOIA request over vaccine data*, REUTERS (Nov. 18, 2021), https://www.reuters.com/legal/government/wait-what-fda-wants-55-years-process-foia-request-over-vaccine-data-2021-11-18/.

[149] *See generally* Kwoka, FOIA, Inc., *supra* note [TK]. *See also* Margaret B. Kwoka, *Inside FOIA, Inc.*, 126 YALE L.J.F. 265, 266 (2016), www.yalelawjournal.com/forum/inside-foia-inc. ("[T]he majority of requests at some agencies are made by commercial requesters. These agencies include large regulatory agencies … ."); Pozen, *Transparency's Ideological Drift*, *supra* note [TK] (describing capture of FOIA and other transparency programs by commercial users).

[150] Kwoka, *Inside FOIA, Inc.*, *supra* note [TK] at 267.

FDA alone spent over $300 million responding to FOIA requests between 2008 and 2017.[151]

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 do so—in fact, a legal obligation to do so. Pursuant to a Reagan-era executive order, E.O. 12,6000,[152] that has since been encoded into ubiquitous regulations,[153] 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.[154] The category of CCI has always been broad, and thus problematic for FOIA requesters.[155] But in 2019, the Supreme Court made an already bad situation even worse. As Varadarajan has described, the Court's *Food Marketing Institute v. Argus Leader* decision "dramatically expand[ed] the private sector's ability to shield from public view information provided to the government."[156] "Wiping away four decades of circuit court precedent, the Court held that commercial information be withheld under Exemption 4, provided that the submitted customarily treated it as private"[157]—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.[158]

---

[151] 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 RSCH. INTEGRITY & PEER REV. 26, 4 (2019).

[152] Exec. Order No. 12,600, 52 Fed. Reg. 23,781 (Jun. 23, 1987).

[153] *See, e.g.*, 21 C.F.R. § 20.61(e) (FDA rule obliging 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").

[154] 5 U.S.C. § 552(b)(4).

[155] Deepa Varadarajan, Business Secrecy Expansion and FOIA, 68 UCLA L. Rev. 462 (2021).

[156] *Id.* at 462.

[157] *Id.*

[158] *Id.* at 499-500.

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, especially after *Food Marketing Institute*. That is undoubtedly true in some cases. But Koningisor has shown that state public records requests tend to be even more difficult than federal FOIA requests, and state agencies even more secretive.[159]

Civil and criminal litigation can provide a trickle of invaluable, otherwise secret information on corporate activity that threatens public health and other interests.[160] For example, tort litigation has for decades unearthed otherwise secret information on the safety and efficacy of medical products.[161] However, information via litigation is no systemic solution. Litigation is rare. It is also slow; information on troubling corporate conduct may not emerge for years or even decades.[162] And overprotection of trade secrets is a problem for courts just as it is for agencies. For example, 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.[163] A team of investigative journalists at Reuters has shown that judges' negligent sealing of information purported to be trade secrets (but often not actually trade secrets) hid, for decades, everything from the extent of opioid abuse knowingly

---

[159] Christina Koningisor, *Transparency Deserts*, 114 NORTHWESTERN L. REV. 1461 (2020); *see also* Christina Koningisor, *Secrecy Creep*, 129 U. PENN. L. REV. 1751 (2021).

[160] *See, e.g.*, Alexander C. Egilman, Aaron S. Kesselheim, Harlan M. Krumholz, Joseph S. Ross, Jeanie Kim & Amy Kapczynski, *Confidentiality Orders and Public Interest in Drug and Medical Device Litigation*, 180 JAMA INTERNAL MED. 292 (2020) (information on pharmaceutical and medical device industries unearthed and disseminated via tort litigation); Alex Moss, *Court Refuses To Keep Patent Licensor's Secrets*, EFF (May 8, 2019), https://www.eff.org/deeplinks/2019/05/court-refuses-keep-patent-licensing-secrets (EFF's ongoing efforts to unearth information about software patents via unsealing).

[161] Christopher J. Morten, Aaron S. Kesselheim & Joseph S. Ross, *The Supreme Court's Latest Ruling on Drug Liability and its Implications for Future Failure-to-Warn Litigation*, 47 J.L. MED. & ETHICS 783, 785 (2019).

[162] *See, e.g.*, Egilman et al., *Confidentiality Orders and Public Interest in Drug and Medical Device Litigation*, *supra* note [TK].

[163] Wexler, *supra* note [TK].

fueled by prescription drug manufacturers to the deadly rollover risk of General Motors' SUVs.[164]

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.[165] However, reliance on individual employees to blow the whistle on dangerous corporate activity is no structural solution. In addition, existing whistleblower laws provide employees with insufficient incentives and protections. Those same Theranos employees, Cheung and Shultz, faced intense legal threat from Theranos's lawyers and incurred substantial financial and personal losses as a result of their decision to divulge Theranos's secrets in this way.[166] 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."[167]

That leaves federal regulators' information publicity as our best hope. The next Parts explain what it is and how to achieve it.

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, the United States' 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?

---

[164] Benjamin Lesser, Dan Levine, Lisa Girion & Jaimi Dowdell, *How judges added to the grim toll of opioids*, REUTERS (Jun. 25, 2019), https://www.reuters.com/investigates/special-report/usa-courts-secrecy-judges/ (opioids); Jaimi Dowdell & Benjamin Lesser, *These lawyers battle corporate America – and keep its secrets*, REUTERS (Nov. 7, 2019), https://www.reuters.com/investigates/special-report/usa-courts-secrecy-lawyers/ (rollover).

[165] Erin Griffith, *Theranos whistle-blower testifies she was alarmed by company's blood tests*, NEW YORK TIMES (Sep. 14, 2021), https://www.nytimes.com/2021/09/14/technology/elizabeth-holmes-trial-theranos.html.

[166] CARREYROU, BAD BLOOD, *supra* note [TK] at 247 (Shultz), 255 (Cheung).

[167] Graves & Katyal, *supra* note [TK] at 1365. *See also id*. at 1367 ("despite the DTSA, employers have continued to bring state law trade secret misappropriation claims against whistleblower employees, again with mixed success."). *See also* Laurel Rogal, *Secrets, Lies, and Lessons from the Theranos Scandal*, 72 HASTINGS L.J. 1663 (2021); Deepa Varadarajan, *The Uses of IP Misuse*, 68 EMORY L.J. 739 (2019).

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 the paper'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 users 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 informational 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 the paper'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 O'Reilly's *Federal Information Disclosure* puts it, "except 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."[168]

But others will be surprised to learn that federal agencies make their own rules when they disclose information proactively. The same O'Reilly treatise observes that this key insight is "a crucial fact, often overlooked."[169] 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.[170]

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

---

[168] James J. O'Reilly, *Federal Information Disclosure*, § 9:1.

[169] *Id.*

[170] *See, e.g.*, ¶ 2147 Documents Requested Under Freedom of Information Act, Food Drug Cosm. L. Rep. P 2147, 2015 WL 7803315 (stating, overbroadly, that "The Freedom of Information Act (FOIA) governs the public's access to information held by federal agencies in the conduct of their business"); Matthew B. Tropper, *Patentability of Genetically Engineered Life-Forms: Legal Issues and Solutions*, 25 J. MARSHALL L. REV. 119, 140 (1991) (stating, overbroadly, that "[t]he FOIA controls dissemination of government-held information"). Part III, *infra*, shows that FOIA alone does not actually control federal agencies' information disclosure.

to any and all who request it, regardless of who the requester is or how they plan to use it.[171] FOIA treats all requesters equally, with minor exceptions.[172] 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.[173] As DOJ put it in 2009, "[n]either 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.[174] "The question is whether 'public disclosure' would cause harm; there is no 'middle ground between disclosure and nondisclosure.'"[175] Faced with FOIA's all-or-nothing, dichotomistic choice between total secrecy and total disclosure, courts and agencies alike have 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.[176] 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

---

[171] 5 U.S.C. § 552(a)(3). *See also* David E. Pozen, *Freedom of Information Beyond the Freedom of Information Act*, 165 U. PA. L. REV. 1097 (2017) (discussing FOIA's decontextualized quality); Kwoka, *FOIA, Inc.*, *supra* note [TK] at 1366-78 (summarizing the FOIA process); Morten & Kapczynski, *supra* note [TK] at 520. *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).

[172] 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. Neither fee waivers nor expedited processing affect the ultimate level of access the FOIA requester receives.

[173] *See, e.g.*, *Public Citizen Health Research Group v. FDA*, 185 F.3d 898, 904 (D.C. Cir. 1999); *but see Pub. Citizen Health Research Grp. v. FDA*, 185 F.3d 898, 908-10, & n.2, n.3 (D.C. Cir. 1999) (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) (similar).

[174] DOJ, Department of Justice Guide to the Freedom of Information Act, Exemption 4, https://www.justice.gov/archive/oip/foia_guide09/exemption4.pdf, at 322.

[175] *Id.* (quoting *Seawell, Dalton, Hughes & Timms v. Exp.-Imp. Bank*, No. 84-241, slip op. at 2 (E.D. Va. July 27, 1984)).

[176] O'Reilly, *Federal Information Disclosure*, § 9:1. *See* Part III for more.

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,[177] Nissenbaum,[178] and Hartzog[179] 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 wholly private or wholly public."[180] The way forward for privacy law, argued Solove, was to "abandon the secrecy paradigm" and create gradated, context-specific "controls over and limitations on certain uses of information, even if the information is not concealed" entirely.[181] In parallel, Nissenbaum developed the concept of "contextual integrity" and a related framework for understanding and protecting the privacy of personal information.[182] 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.[183] 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."[184]

---

[177] Solove, *Access and Aggregation*, *supra* note [TK]; DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004); DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011).

[178] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 89-100 (2010) ("[T]he line dividing public and private … is neither static nor universal."); *see also* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004); Helen F. Nissenbaum, *A Contextual Approach to Privacy Online*, 140(4) DAEDALUS 32 (2011).

[179] Woodrow Hartzog, *The Public Information Fallacy*, 98 B.U. L. REV. 459, 518, 519-20 (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." Yet "[p]rivacy law, it seems, is often content to treat disclosures to anyone outside of narrowly prescribed, formalized confidential relationships as 'public.'").

[180] Solove, *Access and Aggregation*, *supra* note [TK] at 1177.

[181] *Id.* at 1178.

[182] *See supra* Nissenbaum, note [TK].

[183] NISSENBAUM, PRIVACY IN CONTEXT, *supra* note [TK] at 140.

[184] *Id.* at 142.

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 law of trade secrecy and the administrative law of information are overdue for precisely the sort of shake-up that privacy scholars have 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, limits that constrict which information users get access to and constrict what uses those users make of that information. This is "information publicity," distinct from blunt, unfettered information disclosure. This Subpart 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 Subpart, 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? 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 the power but the 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 Pozen has described, [185]

> For 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.

From that origin, regulatory "publicity" has always been distinct from mere disclosure. It has always emphasized selective, contextual disclosure to particular audiences to serve particular goals and values within the agency's ambit. In the 20th Century, regulators collected secret information from industry and then disseminated and contextualized it, at turns warning, outraging, teaching, and "improving" the

[185] Pozen, *Transparency's Ideological Drift*, *supra* note [TK] at 108.

public, and helping, over time, to form democratic competence and will. [186] 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.[187] (Recall the Winthrop Chemical example told in the Introduction, wherein FDA not only warned the public away from a specific unsafe product but educated a nascent, then-cutting-edge industry about safe manufacturing.) Effective information publicity spurred and ensured effective legislation, substantive regulation, and democratic oversight of industry and government alike.[188] As Brandeis wrote, a century ago, regulators' "publicity" can be "a remedy for social and industrial diseases."[189]

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 traditional delegates to administrative agencies because of their unique expertise and structure[190]—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

---

[186] *Id.* at 107; *see also* Matthew Herder, *Denaturalizing Transparency in Drug Regulation*, 8 MCGILL J. L. & HEALTH S57, S61 (2015) (explaining the progressive tradition of "publicity" in Canadian consumer protection law and policy in the late 19th and early 20th Centuries).

[187] *See* Pozen, *Transparency's Ideological Drift*, *supra* note [TK] at 107; Herder, *Denaturalizing Transparency*, *supra* note [TK] at S61 (explaining the progressive tradition of "publicity" in Canadian consumer protection law and policy in the late 19th and early 20th Centuries). For more examples of effective "publicity" in action, *see* Kapczynski, *Dangerous Times*, *supra* note [TK]; 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).

[188] Pozen, *Transparency's Ideological Drift*, *supra* note [TK] at 108.

[189] Louis D. Brandeis, *What Publicity Can Do*, in LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT (1914), http://3197d6d14b5f19f2f440-5e13d29c4c016cf96cbbfd197c579b45.r81.cf1.rackcdn.com/collection/papers/1910/1913_12_20_What_Publicity_Ca.pdf.

[190] *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).

secret information.[191] 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 support. (Consider that in the wake of the George W. Bush administration—widely perceived as secretive[192]—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."[193]) 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 a word 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 core harm is use by competitors. The dominant theoretical justifications for legal protection of trade secrets[194] are that such protections incentivize the creation of socially valuable inventions, discourage overprotection of these inventions through actual secrecy, and promote "ethical competition."[195] All these justifications for trade secrecy law focus on mediation of

---

[191] *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"). *See also infra* section III.B.1.

[192] 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.").

[193] Andrew Kaczynski, *Obama's 2008 Campaign Booklet Promises Transparency and Accountability*, Buzzfeed News (Aug. 2, 2012), https://www.buzzfeednews.com/article/andrewkaczynski/obamas-2008-campaign-booklet-promises-transparenc.

[194] And related categories of information, such as CCI.

[195] Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STANFORD L. REV. 311 (2008); Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L. REV.

relationships among existing and potential commercial competitors, and more specifically on protecting the rightful holder of commercially valuable information from misappropriation.[196] Thus, the core harm that trade secrecy law seeks to avert is competitive use of the information by a direct competitor of the holder of the trade secret. When 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, services, and business practices, and often focus on harms—poisoned water, toxic drugs, erratic autonomous vehicles, racial discrimination against employees or customers, and so on.

Of course, if users of a corporate secret establish a harm to the public and publicize it, the source's business may suffer. 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*,[197]

> [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*."

---

1 (2007); Michael Risch, *Trade Secret Law and Information Development Incentives*, *in* THE LAW AND THEORY OF TRADE SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH (Rochelle C. Dreyfuss, Katherine J. Strandburg, eds., 2009); Kapczynski, *The Public's Secrets*, *supra* note [TK]; Robert G. Bone, *The (Still) Shaky Foundations of Trade Secret Law*, 92 TEX. L. REV. 1803 (2014).

[196] 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; Kapczynski, *The Public's Secrets*, *supra* note [TK].

[197] *Ruckelshaus*, 467 U.S. at 1011 n.15 (emphasis added).

The DC 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."[198] Indeed, as Sandeen and Kapczynski have shown, trade secrecy law writ large was never intended to restrict *non*competitors' use of trade secrets in the same way it restricts competitors'.[199] To quote Sandeen,[200]

> 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.[201] As Fan put it, "[b]ounded disclosure thus optimizes the utility of

---

[198] *Pub. Citizen Health Rsch. Grp. v. FDA*, 704 F.2d 1280, 1291 n.30 (D.C. Cir. 1983) (quoting Mark Q. Connelly, Secrets and Smokescreens: A Legal and Economic Analysis of Government Disclosures of Business Data, 1981 Wis. L. Rev. 207, 230).

[199] Sandeen, *Out of Thin Air*, *supra* note [TK]; Kapczynski, *The Public's Secrets*, *supra* note [TK] ("Historically, and now, the primary ways to violate a trade secret are relational: they involve a breach of confidence or the violation of a promise."). *See also* Graves & Katyal, *supra* note [TK] at 1345-47 (tracing trade secrecy's historical origins as mediating relationships among competitors); *Du Pont v. Masland*, 244 U.S. 100, 102 (1917) (stating that the starting point for a trade secrecy dispute "is not property or due process of law, but that the defendant stood in confidential relations with the plaintiffs").

[200] Sandeen, *Out of Thin Air*, *supra* note [TK] at 374.

[201] Among other things, bounded disclosure is likely to preserve the legal status of trade secrets as trade secrets for purposes of private misappropriation litigation. That is, any corporate secrets that meet the relevant legal definition of a trade secret and are publicized by administrative agencies to a limited number of information users, subject to prohibitions on commercial use imposed by the agency, will likely remain a trade secret in the eyes of the law. As Sandeen and Rowe have explained, "pursuant to the relative secrecy doctrine, the owner of information that would otherwise qualify for trade secret protection does not lose protection if the information is shared with others in a manner

disclosure so that the benefits are enhanced while the costs are reduced."[202] In effect, information publicity enables federal agencies to have their cake and eat it, too.

Here, again, the parallels with privacy law are instructive. 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.[203] Privacy law and trade secrecy law alike are designed not to *thwart* all flows of information but to *govern* them toward normatively desirable ends. In a recent piece, Sanfilippo, Frischmann, and 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 in 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.[204] 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."[205]

---

that is reasonable under the circumstances to maintain its secrecy." SHARON K. SANDEEN & ELIZABETH A. ROWE, TRADE SECRET LAW IN A NUTSHELL 2nd Ed., at 76. Trade secret owners routinely share trade secrets with licensees, pursuant to contracts that require confidentiality from the licensee; such sharing of trade secrets does not destroy the information's status as a trade secret. *Id.* And consider that 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* Env't Prot. Agency, Pesticide Registration Manual: Chapter 10 - Data Compensation Requirements, https://www.epa.gov/pesticide-registration/pesticide-registration-manual-chapter-10-data-compensation-requirements.

[202] Fan, *Private Data, Public Safety*, *supra* note [TK] 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).

[203] *See* Nissenbaum, *supra* note [TK – collecting Nissenbaum].

[204] 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).

[205] *Id.* at 44.

The next Subpart 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 unlock new informational uses and 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 other contexts where similar pro-secrecy and pro-disclosure interests clash. For example, a combination of legal and technical constraints successfully 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[206] than from the better-developed literatures around privacy law[207] and the open science movement.[208]

---

[206] 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, Public Safety*, *supra* note [TK]—and the "data publicity" for clinical trial data held by FDA, proposed by Kapczynski and me—*see* Morten & Kapczynski, *supra* note [TK].

[207] Solove, *Access and Aggregation*, *supra* note [TK] 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, *supra* note [TK]; Sanfilippo, Frischmann & Strandburg, *supra* note [TK].

[208] *See* INST. OF MED. OF THE NAT'L ACADS., SHARING CLINICAL TRIAL DATA: MAXIMIZING BENEFITS, MINIMIZING RISK 149-53 (2015); Comm. on Strategies for Responsible Sharing Clinical Trial Data, Bd. on Health Scis. Pol., Inst. Med., *Discussion Framework for Clinical Trial Data Sharing: Guiding Principles, Elements, and Activities (*2014), https://www.ncbi.nlm.nih.gov/books/NBK253383/. For broader discussion of knowledge governance in the "open science" movement, *see* Jorge L. Contreras, *Constructing the genome commons*, *in* GOVERNING KNOWLEDGE COMMONS (Brett M. Frischmann, Michael J. Madison & Katherine J. Strandburg, eds., 2014); Jorge L. Contreras, *Leviathan in the Commons: Biomedical Data and the*

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 secret information without destroying its commercial value.

a) Information Use Applications

When sharing corporate secrets proactively, federal agencies can discriminate. That is, they can elect to publicize secret information to certain members of the public, 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 whom to share corporate secrets with, and on what terms.[209] 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."[210] 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, Centers for Medicare and Medicaid Services, and Canada's national drug regulator require exactly this.[211] Agencies may refuse access 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

---

State, *in* GOVERNING MEDICAL KNOWLEDGE COMMONS (Katherine J. Strandburg, Brett M. Frischmann & Michael J. Madison, eds., 2017); Amy Kapczynski, *Order Without Intellectual Property Law: Open Science in Influenza*, 102 CORNELL L. REV. 1539 (2017).

[209] Information use applications—more often called data use applications—are widespread in voluntary programs for sharing of commercially valuable or otherwise sensitive data. For an example from the pharmaceutical and biotech context, *see* INST. OF MED. OF THE NAT'L ACADS., SHARING CLINICAL TRIAL DATA, *supra* note [TK] at 149-53.

[210] Fan, *Private Data, Public Safety*, *supra* note [TK] at 199. Fan proposes that bounded access is the right model for disclosure "where public disclosure is otherwise barred by protections for trade secrets, property law, or contractual confidentiality terms." *Id.* As I explain elsewhere in this paper, trade secrecy law, property law, and other sources of law do not actually prohibit outright disclosure even of bona fide trade secrets, as a general matter, though some federal agencies' enabling statutes prohibit them from disclosing trade secrets. However, I believe that Fan's bounded access proposal is correct for normative reasons, as it maximizes benefits while minimizing costs.

[211] *See infra* section II.B.2.d.

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 for constraining information users, and the constraints imposed can be positive as well as negative—they can disincentivize or prohibit information users from doing certain things and can equally well incentivize or require information users to do other things.[212] These agreements can be paired with the information use applications described above; a prospective information user that clears the application be 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, which might include a ban on future participation in the information publicity program or financial penalties.

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 deploy law and policy to regulate information and protect its integrity.

[212] *Discussion Framework for Clinical Trial Data Sharing*, *supra* note [TK].

But, as Lessig[213] and others[214] 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 constrain and shape access and use. These technical limits may prove even more effective than legal ones. For example, regulators could build information publicity portals that permit information users to "visit," view, and/or query proprietary information but not to download or copy in full.[215] Such constraints may successfully permit noncommercial uses of secret information while discouraging or preventing the directly competitive uses most harmful to the secret's source. 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 EPA for the answer; EPA could then publicize the presence or absence of the chemical, and its concentration, without revealing the entire chemical makeup of the fluid. Similarly, 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—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 do I focus on these three constraints on information access and use—information use applications, information use agreements, and technical limits on access to information? 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 federal government). These constraints determine which users access information; they dictate the range of uses users make of information;

---

[213] LAWRENCE LESSIG, CODE: VERSION 2.0 120-25 (2006).

[214] *See, e.g.*, WILLIAM J. MITCHELL, CITY OF BITS: SPACE, PLACE, AND THE INFOBAHN 112 (1996).

[215] For an example in the pharma and biotech context, *see* INST. OF MED. OF THE NAT'L ACADS., SHARING CLINICAL TRIAL DATA, *supra* note [TK] at 147 ("Several data sharing programs are granting some access to clinical trial data to secondary users but not allowing 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, compromising participant privacy, or using data for" purposes that compete directly with the data's source."); *Discussion Framework for Clinical Trial Data Sharing*, *supra* note [TK] at 30. ("In some cases, the actual data are not provided to the requestor. Instead, data holders might run specific data analyses for approved requestors and deliver to the requestors only the results of the requested analyses. In another model, recipients receive credentials to access and run queries on the data, but are not able to download or obtain copies of the data.").

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. They are, in effect, proofs-of-concept for the information publicity I propose in this paper.

NIH's BioLINCC: Information Use Applications & Information Use Agreements

Since the 2000s, the U.S. National Institutes of Health (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.[216] 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.[217]) 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.[218]

---

[216] Nat'l Heart, Lung, & Blood Inst., *The BioLINCC Handbook: A Guide to the NHLBI Biologic Specimen and Data Repositories*, Nat'l Inst. Health (2021), https://biolincc.nhlbi.nih.gov/media/guidelines/handbook.pdf; Nat'l Heart, Lung, and Blood Inst., *Biologic Specimen and Data Repository Coordinating Center (BioLINCC)*, Nat'l Inst. Health, https://www.nhlbi.nih.gov/science/biologic-specimen-and-data-repository-information-coordinating-center-biolincc; Joseph S. Ross, Jessica D. Ritchie, Emily Finn, Nihar R. Desai, Richard L. Lehman, Harlan M. Krumholz & Cary P. Gross, *Data Sharing Through an NIH Central Database Repository: A Cross-Sectional Survey of BioLINCC Users*, BMJ Open (2016), https://bmjopen.bmj.com/content/6/9/e012769. https://bmjopen.bmj.com/content/6/9/e012769. BioLINCC also shares physical samples of materials useful in biomedical research.

[217] Nat'l Heart, Lung, & Blood Inst., *Guidelines for Preparing Clinical Study Data Sets for Submission to the NHLBI Data Repository*, Nat'l Inst. Health https://www.nhlbi.nih.gov/grants-and-training/policies-and-guidelines/guidelines-for-preparing-clinical-study-data-sets-for-submission-to-the-nhlbi-data-repository.

[218] Sean A. Coady, George A. Mensah, Elizabeth L. Wagner, Miriam E. Goldfarb, Denise M. Hitchcock & Carol A. Giffen, *Use of the National Heart, Lung, and Blood Institute Data Repository*, N. Eng. J. Med. (May 11, 2017), https://www.nejm.org/doi/full/10.1056/NEJMsa1603542, [https://perma.cc/SM98-VPDL]; Ross et al., Data Sharing Through an NIH Central Database Repository, *supra* note [TK]; Carol A. Giffen, Leslie E. Caroll, John T. Adams, Sean P. Brennan, Sean A. Coady & Elizabeth L. Wagner, *Providing Contemporary Access to Historical Biospecimen Collections: Development of the NHLBI Biologic Specimen and Data Repository Information Coordinating Center (BioLINCC)*, 13 Biopreservation and Biobanking 571 (2015), https://www.liebertpub.com/doi/pdfplus/10.1089/bio.2014.0050.

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.[219] Before getting access to any BioLINCC data, information users must execute, with NIH, an information use agreement termed a "Research Materials Distribution Agreement" (RMDA).[220] The RDMA prohibits transfer of BioLINCC data, a prohibition on use of data to identify specific medical study subjects, obligates users to destroy all downloaded data after research is complete, and obligates users to provide NIH with yearly updates on use of the data.[221] NIH warns that any information users who breach the RMDA may be denied further access to BioLINCC data.[222] No misuse of BioLINCC data has been reported in the many years of the center's existence. BioLINCC thus appears to be a successful information publicity program already administered by the U.S. government.

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

The Centers for Medicare and Medicaid Services (CMS) is the single largest payer for health care in the United States, and important federal regulator.[223] Under the Affordable Care Act, in 2011 CMS began publicizing certain information on the quality and costs of health care services and supplies that it pays for through

[219] *The BioLINCC Handbook*, *supra* note [TK] 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.").

[220] *Id.*

[221] NHLBI Research Materials Distribution Agreement (RMDA), https://biolincc.nhlbi.nih.gov/media/BioLINCC.RMDA.V02.d20120806.pdf; *The BioLINCC Handbook*, *supra* note [TK].

[222] The BioLINCC Handbook, *supra* note [TK] 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.").

[223] Ctrs. for Medicare & Medicaid Servs., *CMS Roadmaps for the Traditional Fee-for-Service (FFS) Program: Overview*, https://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/QualityInitiativesGenInfo/Downloads/RoadmapOverview_OEA_1-16.pdf.

Medicare—data for so-called "performance measurement."[224] By 2017, public sharing of this and other similar CMS data had served a wide variety of useful ends: "to 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."[225]

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.[226] 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."[227] As of December 2021, about 30 institutions—a mix of commercial and academic—had met CMS's criteria and become so-called "qualified entities."[228] 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.[229] Qualified

---

[224] *See* Availability of Medicare Data for Performance Measurement, 76 Fed. Reg. 76,542, 76,567 (Dec. 7, 2011); 42 C.F.R. §§ 401.709, 401.713; Ctrs. for Medicare & Medicaid Servs., Final Rule on Release of Medicare Data to Be Used for Performance Measurement, Dec. 5, 2011 https://www.cms.gov/newsroom/fact-sheets/final-rule-release-medicare-data-be-used-performance-measurement.

[225] 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 (2017), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5433516/.

[226] Ctrs. for Medicare & Medicaid Servs., 2021 Program Guide, 2021, https://www.hhs.gov/guidance/sites/default/files/hhs-guidance-documents/2021%20QECP%20Program%20Guide%20Final%20Version%20Clean_April_2021.pdf.

[227] 42 C.F.R. § 401.705.

[228] Ctrs. for Medicare & Medicaid Servs., Qualified Entity Program, https://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/QEMedicareData.

[229] Ctrs. for Medicare & Medicaid Servs., Instructions for Completing the Data Use Agreement (DUA) Form CMS-R-0235 (Agreement for Use of Centers for Medicare & Medicaid Services (CMS) Data Containing Individual Identifiers), 2010, https://resdac.org/sites/datadocumentation.resdac.org/files/RIF%20Data%20Use%20Agreement%20%28DUA%29.pdf.

entities that use CMS data must provide annual updates to the agency,[230] 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.[231] 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 data's integrity and reduces access and infrastructure costs for data users (who no longer need to invest in storing and securing local copies of the data). Combining data use applications, data use agreements, and technical limits on access, CMS's Medicare data for performance measurement program is a second example of an information publicity program already being administered by the federal administrative state.

Health Canada's Public Release of Clinical Information and Paragraph 21.1(3)(c): Information Use Applications & Information Use Agreements

Since 2019, Canada's central regulator of drugs, vaccines, and medical devices—Health Canada—has shared rich data sets from clinical trials of products it has approved, under a program it calls "Public Release of Clinical Information" (PRCI).[232] The data shared through PRCI is generated and compiled not by Health Canada but by the drug and device companies who submit it to the regulator when seeking product approval. As of August 2021, data on over 160 distinct products, gathered from dozens of companies, had been posted to PRCI.[233] 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, FDA, and other national regulators without evaluation

[230] 42 C.F.R. § 401.719.

[231] *Id.*

[232] Gov't Can., Clinical Information on Drugs and Health Products, https://www.canada.ca/en/health-canada/services/drug-health-product-review-approval/clinical-information-drugs-health-products.html.

[233] Alexander C. Egilman, Joseph S. Ross, Matthew Herder, *Optimizing the Data Available Via Health Canada's Clinical Information Portal*, 193 CANADIAN MED. ASSOC. J. 1305 (2021), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8412426/; Alexander C. Egilman, Amy Kapczynski, Margaret E. McCarthy, Anita T. Luxkaranayagam, Christopher J. Morten, Matthew Herder, Joshua D. Wallach & Joseph S. Ross, *Transparency of Regulatory Data Across the European Medicines Agency, Health Canada, and US Food and Drug Administration*, 49 J.L. MED. & ETHICS 456 (October 19, 2021).

of the risks of misuse and addiction, even though opioids were widely known at the time to be addictive.[234]

The clinical trial data shared by Health Canada through the PRCI program implicates both patient privacy and trade secrecy. To protect these interests, Health Canada asks regulated entities to redact what it deems "confidential business information" (CBI)—essentially, trade secrets[235]—as well as information identifying individual trial participants before making the data accessible to routine users of PRCI.[236] 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 CBI. According to Paragraph 21.1(3)(c) of the Canadian Food and Drugs Act,[237] Health Canada will share 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."[238] The application must also explain "[h]ow the results of the proposed project will be disseminated to the Canadian public."[239] 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."[240] In the event that a data user detects a safety, efficacy, or quality problem, Health

---

[234] Matthew Herder et al. Unpublished manuscript on file with the author.

[235] 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, 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.

[236] Gov't Can., Guidance Document on Public Release of Clinical Information: Profile Page, https://www.canada.ca/en/health-canada/services/drug-health-product-review-approval/profile-public-release-clinical-information-guidance.html.

[237] Gov't Can., Disclosure of Confidential Business Information, https://www.canada.ca/en/health-canada/services/drug-health-product-review-approval/request-disclosure-confidential-business-information/disclosure-confidential-business-information.html.

[238] Gov't Can., Guidance Document - Disclosure of Confidential Business Information Under Paragraph 21.1(3)(c), *supra* note [TK].

[239] *Id.*

[240] *Id.*

Canada requests that the user notify Health Canada as well as the public at large.[241] In 2016, 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 vaccines for human papillomavirus (HPV).[242] The researcher's access to this CBI—and his legal authority to disseminate analysis of it—was upheld by the Canadian Federal Court.[243]

Health Canada's data-sharing programs summarized here, PRCI and Paragraph 21.1(3)(c), together constitute a third example of information publicity "in the wild." Health Canada's controlled sharing of CBI—information that we in the United States would deem trade secrets—is particularly significant, as it shows a major national regulator cultivating bounded gardens of information, to unlock beneficial noncommercial uses of trade secrets while simultaneously protecting their integrity against competitors of the trade secrets' sources.

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, how to know which bounds to impose on access and use? The answers to these questions turn on a deeper set of complex factual questions. For example, does any of the secret information held by the agency qualify as a bona fide trade secret? Will a particular prospective user's use of the information cause competitive harm to the source? Will that user's use meaningfully benefit the public? What information can reasonably be disclosed without condition to all comers? What information should not be publicized at all? In short, how to get the overall balance of secrecy and disclosure right, to unlock socially valuable uses while protecting its integrity?

---

[241] *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.").

[242] Trudo Lemmons, Precedent Pushing Practice: Canadian Court Orders Release of Unpublished Clinical Trial Data, BMJ Opinion (Jul. 19, 2018), https://blogs.bmj.com/bmj/2018/07/19/precedent-pushing-practice-canadian-court-orders-release-of-unpublished-clinical-trial-data/. [Once available, add cite to Doshi's forthcoming paper on analysis of safety, efficacy, and the quality of regulatory decisionmaking—performed with this data.]

[243] *Doshi v. Att'y Gen. Canada*, [2018] F.C. 710 (Can. Ont.) https://www.canlii.org/en/ca/fct/doc/2018/2018fc710/2018fc710.pdf.

In my view, the process of publicity of 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.[244] To gather information from the secret's source(s), the regulator can adapt the process that already exists for responding to FOIA requests: Pursuant to a Reagan-era executive order, E.O. 12,6000,[245] and ubiquitous agency rules,[246] regulators already routinely ask regulated entities to designate information those entities believe should be kept confidential—whether because it contains trade secrets, CCI, or some other protected category of information—and notify those entities before contemplating disclosure of any of it.

But to build effective information publicity programs, regulators should do more than simply ask regulated entities to identify secret information and propose line-by-line redactions of pages that contain it; regulators should ask those entities to articulate the competitive value of the information and the corresponding harm that would flow from 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."[247] There are good efficiency reasons to ask regulated entities to submit this analysis to regulators, rather than forcing agencies to guess at potential harms; 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 and the public at large, whenever time and resources permit. Particularly if contemplating an ongoing, long-term information publicity program

---

[244] *See supra* section II.B.2.a.

[245] Exec. Order No. 12,600, 52 Fed. Reg. 23,781 (Jun. 23, 1987), https://www.archives.gov/federal-register/codification/executive-order/12600.html.

[246] *See, e.g.*, 21 C.F.R. § 20.61(e) (FDA rule obliging 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")

[247] *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; it will also help the agency preempt any challenges made under the Due Process Clause.

rather than urgent, one-time release of information, regulators may choose to use notice-and-comment rulemaking to generate detailed feedback. (As I explain below,[248] 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 on information, organizing and analyzing it, deciding whether to publicize it, implementing an information publicity program, and maintaining it—imposes burdens on the regulatory agencies that undertake these processes. Rulemaking is itself burdensome and takes years. Yet each of these burdens is already borne by the same agencies, as they respond to FOIA requests. Indeed, the costs of responding to FOIA requests may be uniquely high, as producing documents to FOIA requesters requires painstaking page-by-page, line-by-line redaction of each document to excise information protected by FOIA's mandatory exemptions and agencies' own secrecy-promising regulations. 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 (such as the information use agreements and technical limits described above). 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,[249] 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 currently regularly demands months, and sometimes years, of FOIA officers' time to fulfill even a single significant FOIA request.[250]

One final thought: Neither the process for publicizing a corporate secret nor the substantive limits imposed on users' access and use of the secret should turn on

[248] *See infra* section III.B.C.

[249] Morten & Kapczynski, *supra* note [TK].

[250] Christopher J. Morten, Reshma Ramachandran, Joseph S. Ross & Amy Kapczynski, *55 Years to Fulfill a Records Request? Clearly, the FDA Needs Serious Reform of its Data-Sharing Practices.*, WASH. POST (Dec. 13, 2021).

the secret's legal category. In other words, agencies' analysis should not begin or end with preoccupation over whether the information constitutes a trade secret (under UTSA or any other relevant definition). As I show below,[251] 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 will flow from use of the secret—both the benefits that would flow from sharing with independent analysts and the public at large and the harms that would flow from sharing with competitors.[252] In weighing 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, national security, and the agency's own privileged deliberative processes. Some secrets can and should be disclosed outright, without restriction. Other secrets should never be shared under any circumstances. The point is that in each case, the weighing is unique, and the appropriate bounds on publicizing a given secret are likely to be as well.

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 begin to undertake proactive information publicity programs within the confines of existing law—and survive the scrutiny of a deregulatory Supreme Court. 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

[251] *See infra* Part III.

[252] 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.'" *See* Sanfilippo, Frischmann & Strandburg, *supra* note [TK] at 13.

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) the Takings Clause of the U.S. Constitution. It then explains how most regulators can navigate these limits to achieve meaningful information publicity. Subpart III.C identifies the straightforward 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" about what information to disclose, and when, and how.[253]

Whence arises federal agencies' general background authority to disclose information within their possession? From 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."[254] This statute—5 U.S.C. § 301, sometimes called the federal "housekeeping statute"[255]—began in an

[253] O'Reilly, *Federal Information Disclosure*, § 9:1.

[254] 5 U.S.C. § 301. The plain statutory text is explicitly *not* a grant of authority to *withhold* information: "[t]his section does not authorize withholding information from the public or limiting the availability of records to the public." *Id.* By negative implication, § 301 *does* authorize *disclosure* of information to the public—an implication that the Supreme Court endorsed in *Chrysler*. Chrysler, 441 U.S. at 309 n.40 ("This does not mean, of course, that disclosure regulations promulgated on the basis of § 301 are" improper.). Agencies promulgated proactive disclosure regulations under the general authority of section 301 at least as recently as the 1960s and 70s. *See, e.g., Sears Roebuck & Co. v. Eckerd*, 575 F.2d 1197 (7th Cir. 1978). While I am not aware of an agency promulgating a proactive disclosure regulation under § 301 since then, nothing in subsequent cases prevents an agency from doing so.

[255] *Chrysler*, 441 U.S. at 309 n.39.

act of the very first Congress of 1789, which delegated to federal agencies broad authority to control their own records.[256]

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 disclosure. The background presumption that federal agencies have authority to disclose information within their possession has been affirmed repeatedly by the Supreme Court, on at least three occasions, including in 2019's *Food Marketing Institute* decision, authored by Justice Gorsuch.[257] The same background authority was recognized by President Obama[258] and by the Department of Justice under Presidents Obama and Trump.[259]

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) the Takings Clause of the U.S. Constitution. 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 state trade secrecy law.

---

[256] Act of July 27, 1789, ch. 4, § 4, 1 Stat. 29; Act of Aug. 7, 1789, ch. 7, § 4, 1 Stat. 50. *See* William Bradley Russell Jr., *A Convenient Blanket of Secrecy: The Oft-Cited But Nonexistent Housekeeping Privilege*, 14 WM. & MARY BILL RTS. J. 745, 749 (2005).

[257] *Chrysler*, 441 U.S. at 293 ("Congress did not limit an agency's discretion to disclose information when it enacted the FOIA."); *Ruckelshaus*, 467 U.S. at 1008–09; *Food Marketing Institute*, 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).

[258] Freedom of Information Act: Memorandum from Barack Obama, 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.").

[259] Memorandum from the Attorney General for Heads of Executive Departments and Agencies Concerning the Freedom of Information Act (FOIA), 74 Fed. Reg. 51,879 (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)).

Despite some misconceptions, FOIA does not restrict in any way federal agencies' power to disclose confidential information within their possession. As the Supreme Court has announced, "the FOIA is exclusively a disclosure statute."[260] "Congress did not design the FOIA exemptions to be mandatory bars to disclosure."[261] FOIA's exemption 4 specifically permits but does not require agencies to withhold information that qualifies as a trade secret or as CCI.[262] Indeed, in 1977, Congress considered *and rejected* a statutory amendment to FOIA that would have made withholding of CCI and trade secrets mandatory rather than discretionary.[263]

Neither does state trade secrecy law prohibit federal agencies from disclosing information. The scope and depth of trade secret protection that states have extended has expanded dramatically in recent years.[264] But that expansion leaves federal regulators untouched, because state legislation does not govern federal agencies.[265] State trade secrecy laws cannot and do not give injured trade secret holders a right of action against the sovereign U.S. government.[266] Only Congress may waive the U.S. government's sovereign immunity from trade secret misappropriation suits,[267] and it has not done so vis-à-vis state trade secrecy law.[268]

---

[260] *Chrysler*, 441 U.S. at 292.

[261] *Id.* at 293.

[262] *Id.* at 291. *See also Food Marketing Institute*, 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).

[263] John Badger Smith, *Public Access to Information Privately Submitted to Government Agencies: Balancing the Needs of Regulated Businesses and the Public*, 57 WASH. L. REV. 331, 341 (1982).

[264] *See* Kapczynski, *The Public's Secrets*, *supra* note [TK]; Katyal & Graves, *From Trade Secrecy to Seclusion*, *supra* note [TK] at 1341.

[265] Directly, at least. As discussed in depth below, state-level definitions of what constitutes a trade secret can influence the question of whether disclosure or use of trade secret information by a federal agency constitutes a taking under the 5th Amendment of the U.S. Constitution. The Takings Clause can complicate agency disclosure of a state-law trade secret, but it cannot prohibit disclosure if the taking is for public use. For detailed analysis, *see infra* section III.B.3.

[266] *See United States v. McLemore*, 45 U.S. 286, 288 (1846) ("[T]he government is not liable to be sued, except with its own consent, given by law."); *State of Arizona v. State of California*, 283 U.S. 423, 451 (1931) ("The United States may perform its functions without conforming to the police regulations of a state.").

[267] *See, e.g.*, *United States v. Sherwood*, 312 U.S. 584, 589 (1941).

[268] In the federal DTSA, enacted in 2016, Congress declined to waive the U.S. government's immunity from trade secret misappropriation suits brought that act. *See infra* note [TK – citing Bloch].

Let's turn to the three sources of law that *do* impose limits on agencies' disclosure of corporate secrets. They are (1) agencies' own enabling statutes, (2) the federal TSA, and (3) the Takings Clause of the Fifth Amendment.[269] Agencies' enabling statutes are arguably most important, so I turn to them first.

B. Navigating Three Legal Limits

1. Agencies' Enabling Statutes

"Enabling statutes" are the statutes through which Congress establishes the powers and responsibilities of an administrative agency.[270] Through these statutes, Congress decides exactly 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 as it pleases,[271] though in practice its investigations tend to be focused on specific companies, or even specific incidents, and it exercises this power sparingly.)

In the enabling statutes of several federal regulators, Congress has chosen 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

[269] Vogel suggests a possible fourth limit, the Economic Espionage Act (EEA), 18 U.S.C. §§ 1831-39. David A. Vogel, *Government Agencies Can Misuse Your Trade Secret and You Can't Stop Them*, 28 PUB. CONTRACT L. J. 159, 166 (1999). Vogel acknowledges, however, that the EEA governs private contact, not governmental, and that no court has concluded that the EEA applies against the U.S. government or its employees. Vogel at 168. Separately, the First Amendment could conceivably constrain how federal agencies disseminate information. But, as Solove has shown, 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 [TK] at 1200. This is true even when agencies discriminate among information users and uses. *See 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.

[270] *See Enabling statute*, MERRIAM-WEBSTER, https://www.merriam-webster.com/legal/enabling%20statute (last visited Dec. 12, 2020).

[271] Rowe, *Striking a Balance*, *supra* note [TK] at 803; Alissa M. Dolan, Todd Garvey & Walter J. Oleszek, Cong. Rsch. Serv. 7-5700, Congressional Oversight and Investigations (Dec. 1, 2014), https://www.everycrsreport.com/files/20141201_IF10015_ccb287d103532943616db2d04515374727b6cab3.pdf ("Generally, Congress's power to obtain information, including classified and/or confidential information, is extremely broad."); MILGRIM ON TRADE SECRETS § 12.02 n.78 (trade secrets obtained by Congress via FTC subpoena "is subject to investigatory review—and possible dissemination—by Congress itself").

"trade secrets"[272] obtained from regulated entities, unless those entities consent.[273] Most notably, the Federal Trade Commission Act prohibits FTC from disclosing to the public any "any trade secret or any commercial or financial information which is obtained from any person and which is privileged or confidential."[274] The FTCA's statutory prohibition on disclosure has major consequences, as FTC has broader oversight and information-gathering resources than any other federal regulator. (FTC can and does publicize much other non-trade-secret information.) The Consumer Product Safety Act similarly prohibits the Consumer Product Safety Commission from disclosing trade secrets as defined by either the federal TSA[275] or FOIA.[276] Some agencies' enabling 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[277] and another that generally prohibits the agency from disclosing trade secrets submitted by medical device manufacturers.[278]

But 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, FAA, FCC,[279] NHTSA, NTSB, USDA, and HHS (which encompasses, *inter alia*, CMS, FDA, and HHS's Office for Civil Rights, an investigative office entrusted with enforcing HIPAA and federal civil rights laws).

If a federal regulatory agency prohibited by its enabling statute from disclosing a trade secret does so anyway, the aggrieved holder of the trade secret may be able to seek to enjoin future disclosures by bringing an Administrative Procedure Act suit.[280] The subset of federal regulators whose enabling statutes expressly limit disclosure of certain or all trade secrets must therefore tread carefully.

---

[272] These statutes do not define "trade secret," and as such the scope of the prohibition on disclosure is not entirely clear.

[273] For a non-exhaustive list of such enabling statutes, *see* MILGRIM ON TRADE SECRETS § 12.04.

[274] 15 U.S.C. § 46(f) (FTCA § 6(f)).

[275] 18 U.S.C. § 1905.

[276] 5 U.S.C. § 552(b)(4).

[277] 21 U.S.C. § 331(j). *See also* Morten & Kapczynski, *supra* note [TK] at 532-33.

[278] 21 U.S.C. § 360j(c). This provision prohibits disclosure not just of trade secrets but of any CCI deemed withholdable under FOIA exemption 4.

[279] *See Qwest Comm'ns Int'l, Inc. v. FCC*, 229 F.3d 1172 (D.C. Cir. 2000); *see also* MILGRIM ON TRADE SECRETS § 12.02[5] (elaborating on FCC's authority to disclose certain trade secrets obtained from regulated entities).

[280] *See infra* section III.D.

This is, of course, perfectly consistent with foundational theories of administrative law; federal agencies must always stay within the bounds of their enabling statutes 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.[281] Despite widespread misperception that the TSA constitutes an outright prohibition on federal agencies' disclosure of private trade secrets,[282] the statute's constraints are more procedural than 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

[281] 18 U.S.C. §§ 1905-1909. The federal TSA is distinct from the DTSA. 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). The DTSA does not apply against the federal government. *See* David S. Bloch, *Can the Government Be Sued Under the Defend Trade Secrets Act?*, 45 AIPLA Q.J. 407, 411 (2017) ("[W]hile 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*.").

[282] *See, e.g.*, Janka, *supra* note [TK], at 362 n.124 ("While the Trade Secrets Act, 18 U.S.C. § 1905, prohibits government employees from disclosing trade secrets … ."); Joel D. Hesch, *The False Claims Act Creates A "Zone of Protection" That Bars Suits Against Employees Who Report Fraud Against the Government*, 62 DRAKE L. REV. 361, 408 (2014) ("[T]he Trade Secrets Act prohibits government employees from disclosing trade secrets learned during the course of employment or official duties"); 15 Fed. Proc., L. Ed. § 38:132 ("the Trade Secrets Act prohibits an agency from releasing any information that falls within [FOIA] Exemption 4"); *see also supra* note [TK – on conventional wisdom].

> this title, or imprisoned not more than one year, or both; and shall be removed from office or employment.[283]

The severe criminal penalties contemplated by the TSA have never been applied in the many decades since the statute was enacted.[284]

By its 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.[285] Yet, despite that broad text, the TSA has historically been construed narrowly by the Supreme Court—more narrowly than state trade secrecy laws.[286] Many corporate secrets held by regulators fall outside the TSA as currently construed and can consequently be disclosed without implicating it at all.[287] Of course, it is not clear that the current Supreme Court, with a self-proclaimed "textualist" wing now ascendant,[288] 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 that is properly "authorized by law" is

---

[283] 18 U.S.C. § 1905.

[284] Milgram on Trade Secrets § 12.02 n.13.

[285] 18 U.S.C. § 1905.

[286] In *Ruckelshaus*, certain pesticide "health and safety data" was deemed by the Court to be a trade secret under Missouri state law, but not protected by the TSA's prohibition on unauthorized disclosure. 467 U.S. at 1001-02. *See also id.* at 1008-09 ("[T]he Trade Secrets Act is not a guarantee of confidentiality to submitters of data, and, absent an express promise, Monsanto had no reasonable, investment-backed expectation that its information would remain inviolate in the hands of EPA. In an industry that long has been the focus of great public concern and significant government regulation, the possibility was substantial that the Federal Government, which had thus far taken no position on disclosure of health, safety, and environmental data concerning pesticides, upon focusing on the issue, would find disclosure to be in the public interest."). Last year, 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 the majority opinion authored by Justice Gorsuch. 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*, 139 S. Ct. at 2362. For further analysis of the TSA's origins and narrow construction, *see* Morten & Kapczynski, *supra* note [TK] at 537.

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

[288] *See, e.g.*, Diarmuid F. O'Scannlain, *"We Are All Textualists Now": The Legacy of Justice Antonin Scalia*, 91 ST. JOHN'S L. REV. 303 (2017).

expressly permitted by the TSA.[289] "Authorization by law" is *the* key constraint on the TSA; this statutory text contemplates 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 as disclosable information that would otherwise be protected by § 1905.[290] 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."[291]

As the D.C. Circuit has explained, the 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."[292] 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.[293] 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*

---

[289] *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." (citing *Chrysler*)).

[290] *See, e.g.*, 15 U.S.C. § 2217 (empowering the Federal Emergency Management Agency to disclose to the public certain fire prevention and control information, "notwithstanding the provisions of … section 1905 of Title 18").

[291] *Chrysler*, 441 U.S. at 301.

[292] *CNA Fin. Corp. v. Donovan*, 830 F.2d 1132, 1141 (D.C. Cir. 1987) (emphasis added).

[293] *Chrysler*, 441 U.S. at 302-03. *See also Qwest Commc'ns Int'l Inc. v. F.C.C.*, 229 F.3d 1172, 1177 (D.C. Cir. 2000) (interpreting *Chrysler* and holding that the relevant question is "whether [a] reviewing court could reasonably conclude that the statutory grant of authority contemplated the regulations providing for release of information").

decision: There must be "a nexus between the regulation[] and some delegation of the requisite legislative authority by Congress."[294] 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 corporate secret, the agency has the requisite legislative authority.[295] The nexus standard is relaxed and permissive; as the Supreme Court has held, "[t]he pertinent inquiry is whether under any of the arguable statutory grants of authority the … disclosure regulations … are reasonably within the contemplation of that grant."[296] 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 authorizing regulation to pass muster under § 1905.[297]

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.

- ***EPA:*** The Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA) requires that pesticide manufacturers submit to EPA detailed, otherwise confidential information about the formulas and

[294] *Chrysler*, 441 U.S. at 304.

[295] Recall that an all-purpose federal housekeeping statute, 5 U.S.C. § 301, gives *all* administrative agencies legal authority to manage their own records and thus formalizes the background principle that agencies have discretion to disclose information in their own possession. *See supra* § III.A. The housekeeping statute authorizes disclosure of agency-held information, but the Supreme Court has held that the centuries-old housekeeping statute is circumscribed by the later-enacted TSA and does not provide requisite "authorization" under 18 U.S.C. § 1905 to support agency rules authorizing disclosure of trade secrets. *Chrysler,* 441 U.S. at 310, 312. 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.

[296] *Id.* at 309. *See also id.* 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) (holding generally that "[w]hen 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 disclosure-authorizing regulation from NASA failing the nexus test: *J.H. Lawrence Co. v. Smith*, 545 F. Supp. 421, 426 (D. Md. 1982).

[297] *Qwest Commc'ns Int'l Inc. v. F.C.C.*, 229 F.3d 1172, 1178 (D.C. Cir. 2000)

properties of their pesticides.[298] FIFRA also delegates to EPA authority to determine whether and when this secret information can be disclosed outside the agency.[299] 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 entitled to confidential treatment under this subpart."[300] The rule also permits disclosure of pesticides' formulas to the public: "Information 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."[301] The same rule explicitly references the TSA and specifies the agency can disclose trade secrets.[302] This rule has been on the books since the 1970s[303] and has 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.[304]

- ***FDA:*** In 2001, FDA proposed a rule that would have empowered the agency to begin disclosing secret data submitted by regulated entities on the safety and efficacy of gene therapies, which were viewed by the agency as promising but risky.[305] The statutory basis of the

[298] *See* 7 U.S.C. § 136 et seq. FIFRA was the statute at issue in *Ruckelshaus*.

[299] 7 U.S.C. § 136(j)(2)(D).

[300] 40 C.F.R. § 2.307(h)(1).

[301] 40 C.F.R. § 2.307(h)(4).

[302] 40 C.F.R. § 2.201(e).

[303] General Provisions; Confidential Business Information, 43 Fed. Reg. 39,997, 40,005 (1978).

[304] A Westlaw search turned up no instances of EPA disclosing 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/; *Ctr. for Env't. Health v. McCarthy*, 192 F. Supp. 3d 1036, 1042 (N.D. Cal. 2016).

[305] Availability for Public Disclosure and Submission to FDA for Public Disclosure of Certain Data and Information Related to Human Gene Therapy or Xenotransplantation, 66 Fed. Reg. 4688, 4689 (Jan. 18, 2001).

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 promulgate regulations for the efficient enforcement of" the FDCA as a whole.[306] 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)."[307] FDA 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.[308]

- ***HHS & NIH:*** Pursuant to the Food and Drug Administration Amendments Act of 2007 (FDAAA), National Institutes of Health (NIH) operates the ClinicalTrials.gov website, the world's largest public database of clinical trial data.[309] NIH operates the website and manages the submission and publication of data from hundreds of thousands of clinical trials. 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.[310] 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 trade secrets protected by the TSA.[311] HHS and NIH responded that Congress had, through FDAAA, delegated legal authority to gather

[306] *Id.* at 4694 (citing section 701(a) of the FDCA, codified at 21 U.S.C. § 371(a)).

[307] *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 substantive regulations that are binding); *Pharmaceutical Mfrs. v. Food & Drug Admin*., 484 F. Supp. 1179, 1183 (D. Del. 1980) (same). In past work, Amy 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 [TK].

[308] *See* Unified Agenda of Federal Regulatory and Deregulatory Actions, 67 Fed. Reg. 33,040, 33,045 (2002).

[309] Guodong Liu, Gang Chen, Lawrence I. Sinoway, Arthur Berg, *Assessing the Impact of the NIH CTSA Program on Institutionally Sponsored Clinical Trials*, 6 Clinical & Translational Sci. 196 (2013), https://ascpt.onlinelibrary.wiley.com/doi/full/10.1111/cts.12029.

[310] Clinical Trials Registration and Results Submission, 79 Fed. Reg. 69,566 (2014).

[311] Clinical Trials Registration and Results Submission, 81 Fed. Reg. 64,982, 64,994 (2016).

trade secrets and subsequently to disclose them to the public through ClinicalTrials.gov:

> [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 section 402(j) of [the Public Health Service (PHS) Act, which contains the relevant provisions of 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*.[312]

Since the FDAAA Final Rule took effect in 2017, trial sponsors have been legally required to submit protocols and results of trials of unapproved products to ClinicalTrials.gov,[313] and NIH has promptly published them. Much of this information would otherwise remain unpublished and hidden from the public.[314] Despite industry's objections during the notice-and-comment period, no company has actually challenged the FDAAA Final Rule in court.

- ***NTSB:*** The NTSB has a rule that permits it to disclose trade secrets. According a 2017 rule, "[t]he NTSB is 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."[315] 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)."[316] Congress expressly delegated to NTSB the authority it

[312] *Id.* The relevant portions of FDAAA are codified at 42 U.S.C. § 282(j)(3)(D).

[313] 42 C.F.R. § 11.42(b).

[314] 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), https://www.nejm.org/doi/pdf/10.1056/NEJMsr1907644.

[315] 49 C.F.R. § 831.6(b).

[316] 49 C.F.R. § 831.6(a).

> 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.[317] 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'"[318]—but has not been challenged in court.[319]

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 that power. Once that authorizing regulation is in place, the agency *need not evaluate* whether a given secret is or is not a "trade secret" for the purposes of the TSA; the disclosure is legal. Again, this is a key feature, not a bug, of the TSA. The Act is a narrow criminal statute not designed to override Congress's other statutory delegations of investigative and disclosure authority to the federal regulatory state.[320]

3. The Takings Clause

The third and final significant legal limit on federal agencies' authority to disclose corporate secrets is constitutional: the Takings Clause of the Fifth Amendment. Some scholars have concluded that the Takings Clause poses a significant, even impassable, barrier to agency disclosure,[321] but case law does not bear that out. Instead, takings claims will *never* prohibit outright agency disclosure of corporate secrets if disclosure serves some public purpose. That said, takings claims may impose financial costs on an agency when—and only when—the disclosed information constitutes a genuine trade secret under the relevant state law and the agency has promised secrecy. When information does not qualify as a trade secret, or the agency has not promised secrecy, then no takings claim attaches at all, and the agency may disclose the information without financial penalty.

---

[317] Trade secrets submitted voluntarily by regulated entities enjoy greater protections, but the NTSB reserves the right to disclose them, too. *See* 49 C.F.R. § 831.6(a); *see also* 49 U.S.C. § 1114(b)(3).

[318] Investigation Procedures, 82 Fed. Reg. 29,670, 29,674 (Jun. 29, 2017).

[319] NTSB has apparently not yet disclosed a trade secret pursuant to the rule.

[320] *Chrysler*, 441 U.S. at 296-301.

[321] See Janka, *supra* note [TK]; Epstein, *supra* note [TK]; Erika Lietzan, A New Framework for Assessing Clinical Data Transparency Initiatives, 18 MARQ. INTELL. PROP. L. REV. 33 (2014); Fan, *Private Data, Public Safety*, *supra* note [TK] at 183.

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." Not all property is protected "property" eligible for protection under the Takings Clause[322]; while the Supreme Court and the circuits have held some intangible assets—e.g., certain liens, contracts, and trade secrets—to be "property" eligible for protection under the Takings Clause,[323] they have held that other intangible assets—e.g., federal welfare benefits—are not.[324]

The Court has never articulated a precise test for determining whether a particular intangible asset does or does not qualify as property eligible for protection by the Takings Clause. However, in *Ruckelshaus*, it did identify one dispositive feature of trade secrets that made them protectable under the Takings Clause: Trade secrets are treated like property under state law.[325] The same portions of *Ruckelshaus* suggest that any corporate secrets that do *not* meet the relevant state law definition of a trade are ineligible for protection under the Takings Clause, and can be disclosed freely by federal agencies without troubling it.[326] 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.[327]

---

[322] *See, e.g.*, *Air Pegasus of DC Inc. v. United States*, 424 F. 3d 1206, 1212 (Fed. Cir. 2005) ("as a threshold matter, the court must determine whether the claimant has established a property interest for purposes of the Fifth Amendment").

[323] *Ruckelshaus*, 467 U.S. at 1003.

[324] *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. *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 … .").

[325] *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 § 757, 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 Taking Clause has long been implicit in the thinking of this Court"); *see also* Pamela Samuelson, *Principles for Resolving Conflicts between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777 (2006).

[326] *See* Samuelson, *supra* note [TK] at 809 ("While proponents of the trade-secrets-as-property conception tend to invoke *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.").

[327] *See, e.g.*, 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.").

That said, much confidential information important to regulators and to the public *does* qualify as a trade secret for purposes of state law and consequently does implicate the Takings Clause. [328] This is increasingly true given the expanding scope of trade secrecy protection under state law[329]; now that the vast majority of states have now adopted the Uniform Trade Secrets Act (UTSA), which defines a "trade secret" expansively,[330] state-law definitions of a "trade secret" cover a broad swath of information.[331] Moreover, the law of trade secrecy varies state-to-state and is less than crystal clear; as such, federal regulators may understandably be anxious about concluding 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, not at all, so long as the agency takes a single step: It makes no promise of ongoing confidentiality when it obtains the secret. *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.[332] "As a matter of

---

[328] *See supra* note [TK – on how *Ruckelshaus* held state-law definitions of "trade secret" control whether information is "property" for the Takings Clause]

[329] *See supra* note [TK – Katyal & Graves; Kapczynski]

[330] The UTSA defines a trade secret as "any information that is secret, is subject to reasonable efforts 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." UTSA § 1.4.

[331] The federal DTSA does not create claims for trade secret misappropriation against the U.S. government—*see supra* note [TK]—but it does define a category of information as "trade secrets," protectable from misappropriation via civil litigation in federal court. *See* 18 U.S.C. §§ 1836, 1839(3). It is possible that future courts and administrative agencies may recognize the DTSA as having created a new form of "property" protected by the Takings Clause, with protections that mirror the existing constitutional protections accorded state law trade secrets.

[332] *Ruckelshaus*, 467 U.S. at 1011 ("[T]he statute also gave Monsanto explicit assurance that EPA was prohibited from disclosing publicly, or considering in connection with the application of another, any data submitted by an applicant if both the applicant and EPA determined the data to constitute trade secrets. Thus, with respect to trade secrets submitted under the statutory regime in force between the time of the adoption of the 1972 amendments and the adoption of the 1978 amendments, the Federal Government had explicitly guaranteed to Monsanto and other registration applicants an extensive measure of confidentiality and exclusive use. This explicit governmental guarantee formed the basis of a reasonable investment-backed expectation." (citation omitted)). *See also id.* at 1008 ("[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 *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

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."[333] If an agency provides no assurance of secret, 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 avoiding making any assurances of secrecy, whether through contract, policy, regulation, or direct communication with the regulated entity.[334]

What about corporate secrets 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.[335] Recent Supreme Court decisions confirm a centuries-old principle: If a taking is for public use, the taking cannot be enjoined.[336] As the Supreme Court has said, 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."[337]

---

the time of submission."); Rowe, *Striking A Balance, supra* note [TK] at 802 ("*Monsanto* is therefore 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.").

[333] *Thomas v. Union Carbide Agricultural Products Co*., 473 U.S. 568 (citing *Ruckelshaus*, 467 U.S. at 1002).

[334] Many federal agencies have promulgated rules that assure regulated entities that trade secrets or CCI will remain confidential and will not be disclosed without consent.

[335] Even the First Circuit's errant *Philip Morris* decision acknowledges that disclosure of a protected trade secret to serves a significant state interest may be constitutional. 312 F.3d at 44 ("I recognize that appellants have asserted a significant, perhaps compelling, state interest: a right for Massachusetts to protect and promote the health of its citizens. If I was convinced that this regulation was tailored to promote health and was the best strategy to do so, I might reconsider our analysis. Numerous cases show that a crucial part of the regulatory takings equation is the government interest.").

[336] *See Knick v. Tp. of Scott, Penn*., 139 S. Ct. 2162, 2179 (2019) ("As long as just compensation remedies are available … injunctive relief will be foreclosed."); *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 [TK] at 180.

[337] *First English Evangelical Lutheran Church v. County of Los Angeles,* 482 U.S. 304, 315 (1987) (emphasis in original).

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—"just compensation."[338] 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 harm.[339]

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

One example: In earlier work, Kapczynski and I proposed that 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. FDA can do this in harmony with the Takings Clause by imposing data use agreements on any users of the data that prohibit those users from using the data to compete directly with the companies that submitted the data.[340] These agreements limit the risk of financial harm to the sources of this data, and thereby limit FDA's own financial risk. In effect, they make information publicity affordable and pragmatic even for a cautious and penny-pinching federal agency—especially when compared to the large social benefits of (controlled) disclosure.[341] FDA's counterparts in Canada and the European Union already publicize exactly this kind

[338] *See generally* see Katrina Miriam Wyman, *The Measure of Just Compensation*, 41 U.C. DAVIS L. REV. 239 (2008); Christopher Serkin, *The Meaning of Value: Assessing Just Compensation for Regulatory Takings*, 99 NW. U. L. REV. 677, 678, 682 (2005). 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 to prevent disclosure altogether.

[339] *United States v. 564.54 Acres of Land*, 441 U.S. 506, 511 (1979). *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 … .").

[340] Morten & Kapczynski, *supra* note [TK].

[341] Morten & Kapczynski, *supra* note [TK].

of data and impose exactly this kind of data use agreement on data users—with a growing track record of success.[342]

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) the Takings Clause. 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 in some way. What should that regulator do to ensure the legality of its disclosure?

Recall that secrets that do not meet the 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 might meet the state or federal definition of a trade secret that can trigger legal liability.

To protect publicity of 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 statute or regulation promulgated by the agency.[343] A regulation ensures adequate deliberative process. In its 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 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, 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.[344] As I have argued here, FAA's categorical statement is incorrect as a matter of law. The TSA actually complicates disclose only of information that meets the TSA's narrow

[342] *See supra* § II.B.2.d (discussion of Health Canada's information publicity program); *see also* Egilman et al., *Transparency of Regulatory Data*, *supra* note [TK].

[343] *Supra* § III.B.2.b.

[344] Airworthiness Directives, *supra* note [TK].

definition of a trade secret[345]—not every scrap of Boeing's purported "proprietary information." In addition, if 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 FAA sweeping authority to "issue, rescind, and revise such regulations as are necessary to carry out" the agency's functions,[346] and no provision of FAA's enabling statutes prohibits disclosure of trade secrets. Thus, the question of whether FAA has legal authority to publicize trade secrets in the public interest is less a matter of statute than a matter of regulation and agency will. And, on my reading, FAA's existing regulations do not actually appear to prohibit the agency from disclosing trade secrets in its possession.[347]

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 rule,[348] 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.

In fact, while FAA continues to keep Boeing's secrets, another major regulator of transportation is gearing up for wider disclosure of secret details of transportation software, and it recently rescinded assurances of secrecy to smooth the way to disclosure. As noted above,[349] 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, NHTSA made crystal clear that it is rescinding any

[345] *See supra* § III.B.2.

[346] 49 U.S.C. § 106(f)(3).

[347] In fact, some FAA regulations are explicit that FAA holds legal authority to disclose certain trade secrets when doing so is in "the public or national interest." *See, e.g.*, 14 C.F.R. § 413.9 (governing confidentiality of materials submitted in connection with licensure of commercial space transportation—e.g., satellite launches).

[348] For example, FDA has constitutional and statutory authority to disclose trade secrets and CCI—*see infra* § III.B.2 and Morten & Kapczynski, *supra* note [TK]—but 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.").

[349] *Supra* § I.B.1.

assurance of ongoing secrecy[350]: "NHTSA … will not keep this information confidential, intends to make it publicly available, and is providing no assurance to you to the contrary."[351]

If it has taken these two preparatory steps—(1) promulgate an authorizing rule and (2) cease assurances of secrecy—a regulatory agency 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.

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 prevailed, as courts find there was no taking and that disclosure was legally authorized, consistent with the TSA and other relevant statutes. The history shows that, despite frequent saber-rattling, actual litigation over federal agencies' disclosure of trade secrets is rare, and it favors the agencies.

Monsanto's lawsuit against EPA is the best-known such litigation, as it made its way all the way to the U.S. Supreme Court.[352] As 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*."[353] The Supreme Court held that EPA could legally share Monsanto's trade secrets with the company's competitors, and EPA was required to pay compensation to Monsanto only for sharing secrets gathered during a period of six years (1972-78) in which EPA had promised to keep Monsanto's secrets secret.[354] The Court held that Monsanto had no legal basis on which to enjoin or demand

---

[350] In the same order, NHTSA does exempt three narrow categories of "confidential business information," defined by the agency itself in the same order, from mandatory disclosure. *In re: Standing General Order 2021-01*, U.S. Dep't Transp., Nat'l Highway Traffic Safety Admin., https://www.nhtsa.gov/sites/nhtsa.gov/files/2021-06/Standing_General_Order_2021_01-digital-06292021.pdf.

[351] *Id.*

[352] *Ruckelshaus*, 467 U.S. at 986.

[353] Samuelson, *supra* note [TK] at 809.

[354] *Ruckelshaus*, 467 U.S. at 1013-14.

compensation for EPA's sharing of trade secrets gathered from Monsanto in other years.[355]

Though *Ruckelshaus* was only a qualified victory for Monsanto, it constitutes something of a high-water mark among cases in which corporations 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 its direct competitors, giving, in the words of the district court, "Monsanto's competitors a free ride at Monsanto's expense."[356] (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."[357]) The Supreme Court remanded for further proceedings and encouraged Monsanto to bring a takings claim for compensation in the Claims Court,[358] but it appears Monsanto never actually pursued such a claim, let alone won and collected compensation from EPA.

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 the Takings Clause for disclosure of a trade secret. 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.[359] 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.[360]

---

[355] *Id.* at 1013.

[356] *Id.* at 999.

[357] *Id.* at 1015.

[358] *Id.* at 1020.

[359] *See* 28 U.S.C. §§ 1295(a)(3) & 1491(a)(1). *See also, e.g.*, *Eastern Enterprises v. Apfel*, 524 U.S. 498, 520 (1998).

[360] *US Marine, Inc. v. United States*, 722 F.3d 1360, 1374 (Fed. Cir. 2013) (recognizing the possibility of "a takings claim involving trade secrets" and citing *Ruckelshaus*).

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.[361]

In other instances, owners of purported trade secrets have sought to use Administrative Procedure Act (APA) litigation to enjoin agencies' disclosures of private trade secrets before they occur. When the agency has an appropriate authorizing regulation in place, sanctioning disclosure of trade secrets,[362] agencies win these APA challenges.[363] Since the Supreme Court's 1979 *Chrysler* decision—which clarified the reach of the federal TSA[364]—I can find no case in which a court actually enjoined a federal agency under the APA from disclosing alleged trade secrets because of the what the court concluded was a violation of the TSA.[365]

Finally, despite understandable anxiety among U.S. government officials[366] and scholars[367] alike about the TSA's status a criminal statute and the fearsome

[361] [string cite from research memo]

[362] *See supra* § III.B.2.b.

[363] *See, Parkridge Hospital, Inc. v. Califano*, 625 F.2d 719 (6th Cir. 1980); *St. Joseph's Hospital Health Center v. Blue Cross of Central New York, Inc.*, 489 F. Supp. 1052 (N.D.N.Y. 1979); *RSR Corp. v. Browner*, 924 F. Supp. 504 (S.D.N.Y. 1996).

[364] *Supra* § III.B.2.

[365] To be sure, courts have, since *Chrysler*, restated the abstract legal principle that a private entity can enjoin a federal agency from disclosing trade secrets if such disclosure would violate the Trade Secrets Act. *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"). But I cannot find a case in which a court has awarded an injunction.

[366] *See, e.g.*, Dep't of Energy, *Treatment of Confidential Materials* (Oct. 29, 2019), https://www.energy.gov/sites/prod/files/2019/10/f68/DOE-LPO_Treatment_of_Confidential_Materials.pdf ("The Trade Secrets Act makes Federal employees criminally liable for sharing business-sensitive information with anyone outside of their respective agencies. … Violations of the Trade Secrets Act may result in the loss of employment, fines and imprisonment.")

[367] *See, e.g.*, Levine, *The Impact of Trade Secrecy*, *supra* note [TK] at 431–32 ("both 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").

penalties it contemplates,[368] no U.S. government employee has ever been criminally prosecuted for alleged mishandling of a trade secret.[369]

Conclusion

This article has argued that federal regulators can and should embrace what I deem "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.

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.

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.

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 authority[370] and resources to investigate and publicize the uses that data brokers

[368] Fines, imprisonment, and removal from government employment. *See* 18 U.S.C. § 1905.

[369] MILGRIM ON TRADE SECRETS § 12.02 (18 U.S.C. § 1905 "has not yet been applied in the criminal context").

[370] *See supra* Part III.

and artificial intelligence developers, including Google and Amazon, are secretly and controversially making of millions of Americans' sensitive electronic health record (EHR) data.[371]

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.[372]) 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.[373] Recall that the global pharmaceutical industry seems so far to have accepted, without much fight, Canada's drug regulator's flourishing data publicity program.[374] 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."[375] 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

---

[371] *See, e.g.*, Melanie Evans, *Hospitals Give Tech Giants Access to Detailed Medical Records*, WALL STREET JOURNAL (Jan. 20, 2020), https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200.

[372] Morten & Kapczynski, *supra* note [TK]; *see also* Morten et al., 55 Years, *supra* note [TK].

[373] *See* Kapczynski, *The Public's Secrets*, *supra* note [TK] (arguing, both normatively and doctrinally, that regulators can condition access to the marketplace on market participants' sharing of otherwise secret information, including trade secrets).

[374] *See supra* section II.B.2.d.

[375] Rowe, *Striking a Balance*, *supra* note [TK] at 794. *See also* Sanfilippo, Frischmann & Strandburg, *supra* note [TK] 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 … encourag[e] subjects to share it").

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 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 and others preoccupied with the arm-in-arm march of corporate power and economic inequality should explore the prospect of federal regulatory agencies as vehicles to "nationalize" valuable information and bring it under greater public control.

Consider just one example along these lines, and a desperately urgent one: I write at a moment when the COVID-19 pandemic has killed millions of people and seems nearly certain to kill millions more unless and until the world expands manufacturing and distribution of life-saving vaccines. As Ouellette has recognized, the primary "barrier to expanding vaccine manufacturing isn't patents—it's trade secrets and scarce physical supplies."[376] Sarpatwari, Rizvi, and I—and many others in legal academia, public health, and civil society—have argued that there are compelling ethical, epidemiological, and economic justifications for the U.S. government to share whatever information it has within its own files on COVID-19 vaccine manufacturing with the World Health Organization, to jump-start vaccine manufacturing overseas.[377] To date, the Biden administration has responded, flatly, that it simply lacks legal authority to share the proprietary blueprints it holds on COVID-19 vaccine manufacturing.[378] Given the analysis presented in this article—including as to HHS specifically[379]—I suspect that legal question merits another look.

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

[376] Dan Diamond, *Moderna halts patent fight over coronavirus vaccine with federal government*, WASHINGTON POST (Dec. 17, 2021), https://www.washingtonpost.com/health/2021/12/17/moderna-vaccine-patent-dispute-nih/.

[377] Christopher J. Morten, Zain Rizvi & Ameet Sarpatwari, *President Biden Already Has The COVID Vaccine Recipe. He Should Share It*, HEALTH AFFAIRS BLOG (Sep. 22, 2021), https://www.healthaffairs.org/do/10.1377/forefront.20210922.937772/full/.

[378] *See, e.g.*, Dan Diamond, *White House: We don't have 'unlimited rights' to Moderna vaccine recipe*, WASHINGTON POST (Oct. 25, 2021), https://www.washingtonpost.com/nation/2021/10/25/covid-delta-variant-live-updates/#link-BRKB4URRRNFAHA5EO27QLBN6UM ("The Biden administration has concluded that it lacks the authority to share details of Moderna's vaccine process … .").

[379] HHS houses the U.S. government's Operation Warp Speed and thus much of the data in question.

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,"[380] a "Federal Robotics Commission,"[381] an "FDA for Algorithms,"[382] and so on. As we collectively debate the wisdom of these proposals, I think it 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.

[380] *Gillibrand Introduces New And Improved Consumer Watchdog Agency To Give Americans Control Over Their Data* (Jun. 17, 2021), https://www.gillibrand.senate.gov/news/press/release/gillibrand-introduces-new-and-improved-consumer-watchdog-agency-to-give-americans-control-over-their-data.

[381] Ryan Calo, *The Case for a Federal Robotics Commission*, Brookings Inst. (Sept. 15, 2014), https://www.brookings.edu/research/the-case-for-a-federal-robotics-commission/ [https://perma.cc/C69K-NMSG].

[382] Andrew Tutt, *An FDA for Algorithms*, 69 ADMIN. L. REV. 83 (2017).