10-2019

The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance

Rory Van Loo

The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance

*Rory Van Loo**

An irony of the information age is that the companies responsible for the most extensive surveillance of individuals in history—large platforms such as Amazon, Facebook, and Google—have themselves remained unusually shielded from being monitored by government regulators. But the legal literature on state information acquisition is dominated by the privacy problems of excess collection from individuals, not businesses. There has been little sustained attention to the problem of insufficient information collection from businesses. This Article articulates the administrative state's normative framework for monitoring businesses and shows how that framework is increasingly in tension with privacy concerns. One emerging complication is the perception that the state, through agencies such as the National Security Agency, deploys large technology companies to surveil individuals. As a result, any routine regulatory monitoring of platforms—even for the purpose of prosecuting those platforms—would implicate an overbearing state peering into our personal lives. Moreover, opponents of regulation have weaponized privacy arguments to shield other businesses from monitoring, such as banks. A sharper understanding of the institutional, legal, and informational differences between regulatory monitoring and personal surveillance is needed. Juxtaposing these two state tools reveals that the tension between regulation and privacy is largely illusory. Regulators today—most notably the Federal Trade Commission—have untapped power to monitor emerging risks in big technology and other sectors. They should not hesitate to use that power to pursue a more informed and collaborative path to achieving their missions.

---

* Associate Professor of Law, Boston University; Affiliated Fellow, Yale Law School Information Society Project. For valuable input, I am grateful to Daniela Caruso, Danielle Citron, Julie Cohen, Megan Ericson, Eric Fish, Ahmed Ghappour, Dennis Hirsch, David Hoffman, Chris Hoofnagle, Rebecca Ingber, Orin Kerr, Gary Lawson, Tracey Maclin, Paul Ohm, Nicholas Parrillo, Portia Pedro, David Walker, Philip Weiser, Peter Winn, and participants at the Georgetown Technology Law and Policy Colloquium (2018), the Privacy Law Scholars Conference (2018), and faculty workshops at Northeastern, Suffolk, and Vanderbilt. Jacob Axelrod, Samuel Burgess, Phoebe Dantoin, Haley Eagon, Omeed Firoozgan, Christopher Hamilton, Christina Luo, Allison Mcsorley, Amy Mills, Kelsey Sullivan, and Gavin Tullis provided excellent research assistance.

INTRODUCTION

Information is the "lifeblood" of effective governance.[1] In the wake of major crises throughout history—bank failures that threatened the North's ability to fund the Civil War, oil spills that contaminated American coastlines, or muckrakers' exposés of vermin-infested meatpacking facilities—Congress has repeatedly responded by giving agencies monitoring authority, which is the power to subject businesses to routine on-site inspections or examination of private records.[2]

Once deployed, monitoring authority can have a powerful impact. For instance, increasing the average number of Environmental Protection Agency ("EPA") inspections of factories was found to have reduced the pollutants that reach nearby neighborhoods—the type of pollution that is believed to significantly increase the incidence of dementia and premature death—by 2.7 percent.[3] Regulatory examinations make banks less likely to engage in risky behavior that could collapse the financial system.[4] Monitoring also facilitates more predictable and collaborative regulation by providing a mechanism for regular dialogue between industry and government.[5] Few projects are

---

1. *See* Cary Coglianese et al., *Seeking Truth for Power: Informational Strategy and Regulatory Policymaking*, 89 MINN. L. REV. 277, 277 (2004) ("Information is the lifeblood of regulatory policy."); Thomas O. McGarity, *Regulatory Reform in the Reagan Era*, 45 MD. L. REV. 253, 259 (1986) ("[I]nformation is the lifeblood of a regulatory agency . . . ."); Matthew C. Stephenson, *Information Acquisition and Institutional Design*, 124 HARV. L. REV. 1422, 1423 (2011) (making "the commonplace observation—so obvious that it ought to be uncontroversial—that many public decisions turn on some form of predictive judgment, such that a decisionmaker's choice does and should depend on the quality and content of the information available to her").

2. *See* Rory Van Loo, *Regulatory Monitors: Policing Firms in the Compliance Era*, 119 COLUM. L. REV. 369, 371 (2019) (providing a history of regulatory monitoring). Regulatory crises prompt diverse policies beyond monitoring. *See* POLICY SHOCK: RECALIBRATING RISK AND REGULATION AFTER OIL SPILLS, NUCLEAR ACCIDENTS AND FINANCIAL CRISES 5–11 (Edward J. Balleisen, Lori S. Bennear, Kimberly D. Krawiec & Jonathan B. Wiener eds., 2017).

3. Jinghui Lim, *The Impact of Monitoring and Enforcement on Air Pollutant Emissions*, 49 J. REG. ECON. 203, 204 (2016).

4. *See, e.g.*, John Kandrac & Bernd Schlusche, *The Effect of Bank Supervision on Risk Taking: Evidence from a Natural Experiment* 1 (Fed. Reserve Bd., Fin. & Econ. Discussion Series, Working Paper No. 79, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938039 [https://perma.cc/G4AA-X6E9].

5. *See* Van Loo, *supra* note 2, at 397–98 (arguing that regulatory monitoring fits well with new governance models because it is less adversarial than enforcement lawsuits). On new governance emphasizing collaboration and responsiveness, see, for example, IAN AYRES & JOHN BRAITHWAITE, RESPONSIVE REGULATION: TRANSCENDING THE DEREGULATION DEBATE 4–7 (1992); COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY (2006); Kenneth A. Bamberger, *Regulation as Delegation*: *Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L.J. 377 (2006); Jody Freeman, *Collaborative Governance in the Administrative State*, 45 UCLA L. REV. 1 (1997); and Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MINN. L. REV. 342 (2004). On applying collaborative governance to technology firms, see, for example, Margot E. Kaminski, *When the Default is No Penalty: Negotiating Privacy at the NTIA*, 94 DENV. L. REV. 923,

more crucial for the regulatory state than establishing sufficient information flow to enforce laws.

Despite the importance of consistent regulatory access to nonpublic information, regulators often lack visibility into business activities.[6] Most notably today, federal regulators do not regularly monitor the companies that run platforms, defined as sites "where interactions are materially and algorithmically intermediated."[7] Recent events have provoked bipartisan anxiety about the manipulation of U.S. presidential elections through Twitter and Facebook;[8] exposure of user data at companies such as Uber and Yahoo;[9] and the anticompetitive implications of Amazon, Apple, Google, and Microsoft for small businesses and consumers.[10] Yet these companies go to extremes to keep their inner workings secret.[11]

A growing chorus of scholars have proposed regulatory monitoring of private algorithms and online platforms.[12] Because those

939 (2017); William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 983 (2016); and David Thaw, *Enlightened Regulatory Capture*, 89 WASH. L. REV. 329, 373 (2014).

6. *See infra* Part I.A (reviewing which regulators monitor).

7. Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 136 (2017) (including as platforms "online marketplaces, desktop and mobile computing environments, social networks, virtual labor exchanges, payment systems, [and] trading systems").

8. *See* Matt Apuzzo & Sharon LaFraniere, *Indictment Bares Russian Network to Twist 2016 Vote*, N.Y. TIMES, Feb. 17, 2018, at A1.

9. *See, e.g.*, Mike Isaac et al., *Uber Breach, Kept Secret for a Year, Hit 57 Million Accounts*, N.Y. TIMES, Nov. 22, 2017, at B1; Ryan Knutson & Robert McMillan, *Yahoo Hack Swells to 3 Billion Accounts*, WALL ST. J., Oct. 4, 2017, at A1.

10. *Cf.* European Commission Press Release IP/17/1784, Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service (June 27, 2017), http://europa.eu/rapid/press-release_IP-17-1784_en.htm [https://perma.cc/YE5Q-6RCN] [hereinafter Commission Fines Google].

11. *See infra* Section II.B.

12. *See, e.g.*, Ryan Calo & Alex Rosenblat, *The Taking Economy: Uber, Information, and Power*, 117 COLUM. L. REV. 1623, 1662–86 (2017) (drawing on Rory Van Loo's *Helping Buyers Beware* to discuss the need for agencies to "detect" wrongdoing in the sharing economy); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 24–25 (2014) (proposing that the Federal Trade Commission ("FTC") audit consumer scoring systems); Julie E. Cohen, *The Regulatory State in the Information Age*, 17 THEORETICAL INQUIRIES L. 369, 372–73 (2016) ("[P]olicymakers must devise ways of enabling regulators to evaluate algorithmically-embedded controls . . . ."); Deven R. Desai & Joshua A. Kroll, *Trust but Verify: A Guide to Algorithms and the Law*, 31 HARV. J.L. & TECH. 1, 16–17 (2017) (discussing how to make algorithms able to be audited by regulators); Frank Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, 104 NW. U. L. REV. 105, 169–71 (2010) (calling for monitoring of search engines and considering the possibility of the FTC playing that role); W. Nicholson Price II, *Regulating Black-Box Medicine*, 116 MICH. L. REV. 421, 464 (2017) (calling for greater scrutiny of medical algorithms by the Food and Drug Administration ("FDA") and third parties); Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J. 1321, (1992) (calling for "independent governmental monitoring of data processing systems"); Rory Van Loo, *Helping Buyers Beware: The Need for Supervision of Big Retail*, 163 U. PA. L. REV. 1311, 1382 (2015) (proposing that the FTC monitor Amazon); Shlomit Yanisky-Ravid & Sean K. Hallisey,

proposals are typically made in passing as part of broader discussions about technology governance, they address neither the regulatory state's legal foundation nor its normative framework for compelling private parties to hand over nonpublic information. Administrative law scholarship, which would be a plausible source for such a framework, has produced relevant insights into regulators' tools and motivations for information collection.[13] But the legal and normative questions surrounding state compulsion of private parties to hand over information, even for administrative searches of businesses, have been dominated instead by a vast scholarship on privacy and criminal surveillance.[14] The animating problem in that scholarship, and in the privacy literature more broadly, is how to *restrict* excess information collection.[15]

"Equality and Privacy by Design": A New Model of Artificial Intelligence Data Transparency via Auditing, Certification, and Safe Harbor Regimes, 46 FORDHAM URB. L.J. 428, 429 (2019) (proposing "an auditing regime and a certification program, run either by a governmental body or, in the absence of such entity, by private institutions"); *see also* Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 121–24 (2014) (considering auditing by public agencies to address predictive privacy harms).

13. Administrative law scholars' insights into agencies' techniques, organizational design, and incentives for collecting adequate information provide valuable foundations, but do not address the focus of this Article: the legal framework and normative considerations justifying monitoring authority to compel businesses to provide nonpublic information to regulators. *See, e.g.*, Coglianese et al., *supra* note 1, at 324–25 (focusing on regulatory incentives to pursue voluntary information collection for policymaking); Daniel E. Ho, *Fudging the Nudge: Information Disclosure and Restaurant Grading*, 122 YALE L.J. 574, 650–54 (2012) (suggesting institutional improvements for regulatory inspectors); Stephenson, *supra* note 1, at 1483 (identifying legal-institutional design choices for incentivizing information gathering).

14. *See*, *e.g.*, BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 246 (2017) (identifying surveillance concerns and the misuse of administrative subpoenas); Orin S. Kerr, *Searches and Seizures in A Digital World*, 119 HARV. L. REV. 531, 533 (2005) ("This Article develops a normative framework for applying the Fourth Amendment to searches of computer hard drives and other electronic storage devices."); Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 261–62 (2011) (examining inspections of businesses and other administrative searches and situating "the dilution of Fourth Amendment rights in the administrative search context within the larger story of diminishing criminal procedure rights . . . ."); Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 92–95 (2016) (drawing on the Supreme Court's regulatory inspection decisions to illuminate the Fourth Amendment and policing); *see also infra* Section IV.C (situating monitoring within the literature on surveillance and privacy).

15. *See, e.g.*, Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CALIF. L. REV. 735 (2017) (analyzing how the law can delineate boundaries for worker surveillance); Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 U. CHI. L. REV. 75, 76 (2008) (assessing the efficacy of agency privacy impact assessments); G.S. Hans, *Curing Administrative Search Decay*, 24 B.U. J. SCI. & TECH. L. 1, 2–3 (2018) ("This Article focuses on the role of regulatory agencies in the collection of user data from private businesses. It argues that the government should not be able to so easily collect sensitive information without a warrant, active oversight, or robust limitations."); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1153, (2004) ("It is a commonplace, moreover, that our privacy is peculiarly menaced by the evolution of modern society, with its burgeoning technologies of surveillance and inquiry."); Andrew McCanse Wright, *Civil*

This Article builds on that literature to examine the opposite problem: insufficient information collection. It offers a framework for why lawmakers have pervasively granted collection authority to agencies and develops that framework through a case study of online platforms. To comprehend the inattention and resistance to monitoring platforms,[16] and more broadly, how the norms for monitoring businesses are evolving in the twenty-first century, it is necessary to broaden the doctrinal and administrative lens to include agencies that at first seem unrelated to regulatory monitoring: the Federal Bureau of Investigation ("FBI"), National Security Agency ("NSA"), U.S. Immigration and Customs Enforcement ("ICE"), and other federal and local agencies that are primarily concerned with crime and national security. For ease of exposition, these agencies are referred to below as "crime agencies" to contrast them with "regulators," which focus on enforcing civil laws against businesses, although important distinctions exist within each category and both types of agencies can play a role in enforcing diverse laws.[17]

The literature on crime surveillance has remained mostly disconnected from that on regulatory monitoring.[18] Crime agencies often engage in surveillance, defined in the surveillance studies literature as "the focused, systematic and routine attention to personal details."[19] Most prominently, following the 9/11 terrorist attacks, intelligence agencies built databases that enabled them to conduct warrantless computer scans of the metadata from most U.S. citizens' email, phone, and internet records.[20] Regulators, unlike crime agencies,

---

Society and Cybersurveillance, 70 ARK. L. REV. 745, 745 (2017) ("There is no such thing as benign surveillance."); sources cited *supra* note 14.

16. Some observers in favor of regulating tech prefer public disclosures or an ex post, litigation-oriented approach. The reasons for the hostility include concerns about the independent spirit of the internet, a lack of regulatory sophistication, and the possibility that heavier regulation would stifle innovation. *See infra* Section II.C; *see also* Lawrence B. Solum, *Models of Internet Governance*, *in* INTERNET GOVERNANCE: INFRASTRUCTURE AND INSTITUTIONS 48, 57–58 (2009) (discussing early resistance to internet regulation).

17. Criminal law and national security law are two distinct bodies that primarily pursue the punishment of incarceration. When regulators identify criminal wrongdoing in the course of their affairs, they may then refer the matter to other agencies for prosecution. *See infra* Section III.B. Although the terms elide major differences within each category worthy of study, they facilitate the exposition and examination of broader themes crucial to understanding monitoring.

18. *See, e.g.*, DAVID LYON, SURVEILLANCE STUDIES 17–21 (2007) (providing a review of surveillance studies without mentioning regulatory monitoring). *But see* Robert A. Mikos, *Can the States Keep Secrets from the Federal Government?*, 161 U. PA. L. REV. 103 (2012); Slobogin, *supra* note 14.

19. LYON, *supra* note 18, at 14.

20. *See, e.g.*, Slobogin, *supra* note 14, at 107 ("[T]he federal government at one time routinely swept up virtually everyone's 'metadata'—the identifying information about our communications—and may well have collected (and continued to collect) much more than that.").

do not have a history of personal surveillance provoking public outcry. Yet scholars and judges routinely use "surveillance" to refer to regulatory monitoring of businesses.[21] In addition, the same clause of the Fourth Amendment and section of the Administrative Procedure Act ("APA") govern each type of information collection.[22] Above all, privacy concerns have shaped both underlying legal frameworks since colonial times.[23] Regulatory monitoring and crime surveillance thus share close conceptual and legal ties.

The conflation of these two distinct administrative activities is problematic in underappreciated ways. The pervasiveness of technological surveillance "has helped spark an anti-surveillance, proprivacy movement that extends across legal scholarship, policy debates, civil rights advocacy, political discourse, and public consciousness."[24] The salience of this controversy complicates the regulatory monitoring of platforms because crime agencies use technology firms as "the real data-mining masterminds" of their surveillance.[25] When one of the most pressing concerns among the populace and leading jurists is the state accessing information about individuals through technology companies, regulatory monitoring of those companies is easily confused with inviting the state to invade our privacy.[26] Accordingly, accusations of endangering personal privacy have put regulators on the defensive, even at one point shutting down vital Consumer Financial Protection Bureau ("CFPB") regulatory information collection.[27] At the extreme, privacy may even follow a

---

21. *See, e.g.*, Watters v. Wachovia Bank, N.A., 550 U.S. 1, 21 (2007) (referring to regulation of national banks as "audits and surveillance"); Dow Chem. Co. v. United States, 476 U.S. 227, 229, 252 (1986) (discussing the EPA's warrantless "surveillance" of businesses); Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1344 (2015) (noting that "the language and framing used in surveillance debate is diverse, inconsistent, and over-generalized"); Price, *supra* note 12, at 462–65 (using surveillance and monitoring to describe FDA oversight of medical devices). To facilitate exposition, this Article refers to regulators' information collection as monitoring and to crime agencies' as surveillance, but surveillance and monitoring can be used interchangeably.

22. *See* U.S. CONST. amend. IV (regulating searches and seizures); Administrative Procedure Act § 6, 5 U.S.C. § 555(c) (2012) (governing "investigative acts").

23. *See infra* Sections I.C.1. and III.A.

24. Mary Anne Franks, *Democratic Surveillance*, 30 HARV. J.L. & TECH. 425, 426 (2017).

25. Nancy S. Kim & D. A. Jeremy Telman, *Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent*, 80 MO. L. REV. 723, 723 (2015); *see also* Samuel J. Rascoff, *Presidential Intelligence*, 129 HARV. L. REV. 633, 662 (2016) ("A critically important . . . feature of the new intelligence oversight ecosystem is the role of American technology and telecommunications firms."); David C. Vladeck, *Consumer Protection in an Era of Big Data Analytics*, 42 OHIO N.U. L. REV. 493, 498 (2016) ("[T]here is little question that the major data brokers know more about each of us than say, for example, the National Security Agency, the Internal Revenue Service, the Social Security Administration, or any other governmental institution.").

26. *See infra* Section IV.C.

27. *See infra* Section IV.C.

trajectory seen with transparency and free speech: moving from a tool deployed by those engaged in state-building to a tool deployed by antistatists seeking to obstruct regulation.[28]

The conceptual association of regulatory monitoring and crime surveillance obscures important institutional and informational differences. Regulators target information about businesses, while crime agencies target personal information.[29] Moreover, throughout history public outcry has often driven Congress to force regulators to use more of the monitoring authority they already had, while scandals have prompted Congress to do the opposite with crime agencies—to restrict their surveillance activities.[30] Outside of crises, however, lawmakers have passed important laws such as the APA without distinguishing between agencies—thereby potentially restricting business regulators through legislation meant to respond to unease about crime agencies.[31] By overlooking the significant differences between crime agencies and regulators, the legal framework may inadvertently hinder regulators that instead need encouragement to collect adequate information.[32]

This Article's main contributions are to illuminate the legal framework for monitoring businesses and to show how that vital enforcement tool is hindered by operating in the shadow of widely maligned personal surveillance.[33] These insights also have important

---

28. On the link between privacy origins and state-building, see Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553, 565 (2007) (tracing privacy origins not to the Constitution but to the early Post Office and "those who sought independence"); Jeremy K. Kessler, *The Administrative Origins of Modern Civil Liberties Law*, 114 COLUM. L. REV. 1083, 1085 (2014) (arguing that that "[p]rogressive lawyers within the executive branch took the lead in forging a new civil-libertarian consensus and that they did so to strengthen rather than to circumscribe the administrative state," and mentioning privacy as historically analogous to civil liberties). For arguments that transparency and free speech have served deregulatory agendas, see, for example, David E. Pozen, *Transparency's Ideological Drift*, 128 YALE L.J. 100, 102 (2018) (arguing that transparency serves to "reduce other forms of regulation"); Amanda Shanor, *The New Lochner*, 2016 WIS. L. REV. 133, 133 (2016) ("Once the mainstay of political liberty, the First Amendment has emerged as a powerful deregulatory engine . . . .").

29. *See infra* Section III.B.1.

30. *See infra* Section III.B.1.

31. *See infra* Section III.B.1.

32. Scholars have concluded that agency overzealousness varies, and as a result, oversight mechanisms designed to check overzealous bureaucrats ignore important agency heterogeneity. *See* Nicholas Bagley & Richard L. Revesz, *Centralized Oversight of the Regulatory State*, 106 COLUM. L. REV. 1260, 1262 (2006) (arguing that "the claim that agencies are systematically biased in a proregulatory direction finds little support in public choice theory, the political science literature, or elsewhere"); Michael A. Livermore & Richard L. Revesz, *Regulatory Review, Capture, and Agency Inaction*, 101 GEO. L.J. 1337, 1354–55 (2013) ("There is no compelling argument that agencies will be more inclined to overreach than underperform . . . .).

33. Scholars have discussed a distinct but related tension between the need to protect trade secrets and the need to regulate businesses. *See, e.g.*, FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 163–64 (2016).

policy implications across the regulatory state, including for the primary regulator of platforms, the Federal Trade Commission ("FTC").[34] The newly appointed FTC commissioners have expressed an interest in greater oversight of platforms.[35] Yet the agency does not monitor businesses, except in limited contexts currently required by law.[36] In early 2019, nine months after an early draft of this Article was circulated at a conference attended by FTC officials, the agency announced a task force to monitor technology companies.[37] However, the task force is focused on competition—which leaves out consumer protection and privacy—and it is unclear how far the group will move beyond the FTC's traditional light-touch, ex post information collection approach.[38] This Article concludes that the FTC's authorizing statute, when viewed in the context of judicial precedent and the normative foundations for monitoring, indicates that the FTC could—without any congressional action—monitor businesses far more extensively than it traditionally has.[39] FTC monitoring of the surveillance economy would bring the regulatory governance of the world's most valuable industry more in line with that of other large industries.

The issues facing regulatory monitoring of platforms portend larger tensions building for regulatory monitoring in the surveillance era. Other agencies, such as the Federal Communications Commission ("FCC"), likely sit on similar untapped authority.[40] Companies ranging from Citibank to Target to American Airlines increasingly amass customers' personal data and connect with platforms—thereby producing harms similar to those that platforms produce.

---

34. The FTC regulates online platforms for antitrust, privacy, and consumer protection. *See* 15 U.S.C. §§ 41–58 (2012).

35. Diane Bartz, *FTC Nominees Open to Tech Probes, Concerned About High Drug Prices*, REUTERS (Feb. 14, 2018, 1:42 PM), https://www.reuters.com/article/us-usa-ftc-congress/ftc-nominees-open-to-tech-probes-concerned-about-high-drug-prices-idUSKCN1FY2RN [https://perma.cc/4QHW-XGY3].

36. *See, e.g.*, 15 U.S.C. § 18 (2012) (requiring pre-merger notification).

37. *See 2018 Privacy Law Scholars Conference*, BERKELEY L., https://www.law.berkeley.edu/research/bclt/bcltevents/2018annual-privacy-law-scholars-conference (last visited Sept. 22, 2019) [https://perma.cc/2FJ3-8WN5] (listing Joseph Calandrino and Kevin Moriarty as attending the May 30–31 conference in Washington, D.C.); Press Release, Fed. Trade Comm'n, FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets (Feb. 26, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology [https://perma.cc/6ZKJ-5H26] ("Agency dedicates resources exclusively towards monitoring competition in the tech industry and taking enforcement actions when warranted."). This Article was also workshopped at the Georgetown Technology Law and Policy Colloquium, and received input from a former FTC high-ranking official, ten months before the announcement of the task force. Since the Article was mostly researched, workshopped, and submitted before that task force's launch, it does not include an examination of that new group.

38. *See infra* notes 63–65 and accompanying text.

39. *See infra* Section IV.A.

40. *See infra* Section IV.B.

Congressional leaders have also weighed legislation for auditing algorithms in select contexts, such as for discrimination.[41] For these and related issues, it would be ideal for agency leaders, judges, and lawmakers, in deciding whether to monitor, to consider the context of the modern regulatory state's legal and normative framework for that authority.

If the monitoring framework is to be updated for the surveillance era, there is a risk in moving where prominent privacy warnings seem to naturally direct it—away from monitoring due to unease about regulators collecting customer data. Legitimate privacy concerns do not demand the complete avoidance of monitoring because they can be addressed through the design of monitoring programs and through legal constraints.[42] In fact, what the surveillance era may call for—at least to prevent some types of harms—is *more* government monitoring of businesses.[43] Among other reasons, monitoring can help regulators determine whether businesses are safeguarding customers' data.[44]

Clarifying the normative and legal framework for regulatory monitoring also helps sketch a blueprint for an improved administrative information architecture. Instead of restricting crime agencies and business regulators in the same way, as the APA and other statutes do, legislators should tailor restrictions to the divergent informational dynamics of each of those categories of agencies.[45] Greater attention to the fine distinctions between regulators and crime agencies, and the purposes of their information collection, would help reset the state informational framework to its constitutional roots by prioritizing personal privacy over business privacy.

The Article is structured as follows. Part I examines the historical record to identify the factors considered in congressional

---

41. James A. Allen, *The Color of Algorithms: An Analysis and Proposed Research Agenda for Deterring Algorithmic Redlining*, 46 FORDHAM URB. L.J. 219, 260 (2019) (discussing a congressional hearing on oversight of algorithms).

42. *See* Bamberger & Mulligan, *supra* note 15 (identifying mechanisms for increasing agencies' privacy accountability); Hans, *supra* note 15, at 34 (discussing the need for limitations in regulatory programs that collect data); *infra* Section III.B.

43. This assumes that the government continues to reflect democratic values, or that the monitor has appropriate constraints in place should that fail to be the case. Nor does it completely preclude private monitoring regimes, although purely private regimes may have limits. *See infra* Part II.C.

44. *See infra* Section III.A. Although he did not discuss business monitoring, the competing privacy interests between business owners and users is arguably an example of what David Pozen has described as a "privacy-privacy tradeoff." *Cf.* David E. Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221, 221 (2016) ("Whenever securing privacy on one margin compromises privacy on another margin, a privacy-privacy tradeoff arises."). By analogy, this Article develops a privacy-regulation tradeoff.

45. *See infra* Section III.B.

extension and judicial approval of regulatory monitoring authority. Part II begins a case study of platforms by applying the three factors weighing in favor of monitoring: a public interest in preventing harm, information asymmetries, and self-regulatory shortcomings. Part III explains the two main factors historically weighing against monitoring, privacy and burden, and considers how they are changing in the surveillance era. Part IV concludes by examining legal and theoretical implications. It analyzes the scope of the FTC's dormant statutory monitoring authority, and briefly considers possible action by other agencies, such as the FCC and the Equal Employment Opportunity Commission ("EEOC"). Both agency discretion and statutory design would benefit from a normative framework that more clearly demarcates the actors, targets, and content of monitoring from those of surveillance. The overarching goal is to contribute to an administrative structure that ensures regulators in the future, like crime agencies today, have the information they need to make informed decisions.

I. RATIONALE FOR REGULATORY MONITORING

Despite strong countervailing interests in privacy and autonomy at the founding of the country, regulators have steadily gained the authority to peer inside businesses to promote legal compliance. The legal literature lacks any holistic analysis of the considerations that legislators and judges weighed in elevating regulatory monitoring authority to a central role in policing firms. This Part begins to fill that gap by surveying the factors historically weighed in extending monitoring authority. The rest of the Article then develops this framework in the context of the platform economy and the surveillance state.[46]

A. Overview of Regulatory Monitoring

This Article is focused on administrative agencies' "systematic and routine" collection of nonpublic information, rather than one-off investigations.[47] The state has in recent decades increasingly relied on such "programmatic" information for enforcing criminal laws, ranging

46. Jack Balkin and Sanford Levinson conceived of the National Surveillance State as a new form of governance responding "to the particular needs of warfare, foreign policy, and domestic law enforcement in the twenty-first century." *See* Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489, 489 (2006). *But see* Orin S. Kerr, *The National Surveillance State: A Response to Balkin*, 93 MINN. L. REV. 2179, 2180 (2009) (arguing that the National Surveillance State is more about technological change than a new form of governance).

47. Slobogin, *supra* note 14, at 93.

from roadside checkpoints to call record databases.[48] Routine business monitoring also has steadily grown to become one of the regulatory state's core powers.[49]

At first glance, the work of front-line bureaucrats who monitor may seem mundane: poring over financial records to identify risky bank transactions, inspecting poultry for signs of contamination, or assessing the pollution controls in factories.[50] But like police officers, regulatory monitors make life-altering decisions about when and how the law will be enforced and against whom.[51] They are often scientists, economists, and engineers with the power to obligate companies to pay millions to their customers in redress, block hazardous food products from reaching Americans' dinner tables, or shut down offshore oil rigs.[52] Whereas legal scholars universally recognize that law enforcement officers wield considerable authority in federal criminal law, the role of their civil law counterparts—regulatory monitors—is overlooked.[53]

For present purposes, regulatory monitoring is the collection of information that the agency can force a business to provide even without suspecting a particular act of wrongdoing. The two main categories of monitoring are remote report collection and on-site visits. The scope of information accessible to on-site inspectors depends on their mandate. Food and Drug Administration ("FDA") and EPA inspectors, for instance, can access records related to their missions—food safety and the environment—but cannot examine records about profit.[54] Bank examiners, in contrast, can access almost any piece of data because their mission is broad.[55] These visits may occur with advanced notice or unannounced, as when oil inspectors drop in via

---

48. Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1042 (2016) ("While our Fourth Amendment framework is transactional, then, surveillance is increasingly *programmatic*."); *see also* Slobogin, *supra* note 14, at 93:

> Panvasive searches and seizures . . . seek to ferret out or deter *undetected wrongdoing* . . . rather than focus on a particular crime known to have already occurred; . . . they are purposefully *suspicionless* with respect to any particular individual, and thus will almost inevitably affect a significant number of people not involved in wrongdoing.

49. Van Loo, *supra* note 2, at 373 (describing the regulatory state's pervasive reliance on ongoing monitoring); *cf.* MICHAEL POWER, THE AUDIT EXPLOSION (1994) (describing the growth of audits by private and public actors in the United Kingdom).

50. *See* Van Loo, *supra* note 2, at 372–73.

51. *Id*. at 373.

52. *Id.* at 373–74.

53. *Id*.

54. *See* Toxic Substances Control Act, 15 U.S.C. § 2601 (2012); Federal Food, Drug, and Cosmetic Act § 372, 21 U.S.C. § 372 (2012).

55. *See* John D. Hawke, Jr., Comptroller of the Currency, Remarks Before a Conference on Credit Rating and Scoring Models (May 17, 2004), https://www.occ.treas.gov/news-issuances/speeches/2004/pub-speech-2004-36.pdf [https://perma.cc/M8UM-A547].

helicopter on Gulf of Mexico oil platforms to check safety and environmental compliance.[56] For some companies, such as the largest banks and nuclear facilities, regulators have resident monitors on site year-round.

Even agencies with on-site inspection authority typically supplement those efforts with heavy remote monitoring. These can occur through one-off requests to answer specific questions (such as asking to clarify a new technology used), whenever a specific event occurs (such as a proposed merger), or on a periodic basis (such as monthly reports on bank lending activities). Agencies also sometimes use legal authority to install remote-monitoring devices, such as sensors measuring equipment inside a manufacturing facility.[57] Once these reports or data sets are in place, analysts within the regulator conduct spot-check audits, algorithmically driven systemic reviews, or other checks to identify violations.

Monitors respond to violations in different ways depending on the agency. Banking monitors, called "examiners," typically have the independence to decide how to resolve the violation.[58] For instance, CFPB examiners have required banks to make multimillion dollar payments without an enforcement lawyer playing a substantial role.[59] Due to banks' fears of creating an antagonistic relationship, and the examiners' ability to pass a matter on to enforcement lawyers for formal legal proceedings, the examiners have substantial leverage in making informal demands.[60] The EPA, in contrast, has a more integrated approach. Once the EPA inspector—typically an engineer—identifies anything more than a minor violation, she works side by side with a lawyer to seek redress, even coauthoring court briefs.[61]

Of the nineteen large federal regulators of business, only four rely more heavily on lawyers than monitors.[62] Notably, the two agencies that are arguably the most important for overseeing the surveillance economy are among these four that do not rely heavily on monitoring: the FTC, which is the agency with the most regulatory authority over platforms, and the FCC, which oversees other important information

---

56. *See* Guy Hayes, *A Day in the Life of an Inspector*, BUREAU OF SAFETY & ENVTL. ENF'T, https://www.bsee.gov/newsroom/feature-stories/a-day-in-the-life-of-an-inspector (last visited Sept. 22, 2019) [https://perma.cc/QL2V-5A83].

57. *See* Daniel C. Esty, *Environmental Protection in the Information Age*, 79 N.Y.U. L. REV. 115, 156 (2004).

58. *See* Van Loo, *supra* note 2, at 413–14.

59. *Id*. at 414.

60. *Id*.

61. *Id*. at 434.

62. *See id*. at 382–83, 409–10 (finding low monitoring reliance at the FCC, FTC, EEOC, and National Labor Relations Board).

technology firms, such as telecommunications and cable companies.[63] Even without heavy reliance on monitoring, regulators may still access firms' information for investigations after wrongdoing is suspected, or in other limited contexts.[64] For instance, the FTC conducts one-off studies of a given industry or practice to decide whether it should act.[65] However, unlike most large regulators, the FTC and FCC do not rely for their enforcement actions on routinely compelling large firms to hand over information without particular suspicion of wrongdoing.[66]

Thus, monitoring authority is pervasive, and monitors—despite being overlooked in the literature and largely absent in the technology sector—are perhaps the single most influential law enforcement group in the regulatory state.[67] An account of why regulators monitor is overdue.

63. The CFPB also regulates fintech platforms. Rory Van Loo, *Technology Regulation by Default: Platforms, Privacy, and the CFPB,* 2 GEO. L. TECH. REV. 531 (2018).

64. *See* Van Loo, *supra* note 2, at 393–95.

65. *See* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 103 (2016) (describing the FTC's "structural case model").

66. As one measure of this, most large regulators devote more resources to monitors than to lawyers. *See supra* Table 1.

67. *See supra* Table 1.

TABLE 1: SHARE OF MONITORS AND LAWYERS WITHIN REGULATORY MONITOR AGENCIES

Monitor Employees as a Percentage of Combined Monitor and Lawyer Workforce[68]

Light Monitors <15%	**15-49%**	**50-85%**	**Heavy Monitors >85%**
FTC 3%	FCC 34%	FERC 62%	FDA 98%
EEOC 0%		EPA 60%	NCUA 97%
NLRB 0%		CFPB 54%	FSIS 95%
		SEC 53%	Fed. Res. 95%
			OSHA 93%
			NRC 93%
			FAA 93%
			FMCSA 93%
			OCC 93%
			MSHA 91%
			FDIC 86%

A. Why Do Regulators Monitor?

Courts and lawmakers weigh a number of factors in deciding whether monitoring is appropriate. Since privacy and criminal law scholarship has dominated the topic of administrative information collection, existing descriptive frameworks focus on Fourth Amendment constraints on searches.[69] Those analyses unearth many of the basic elements of a search scheme, which must be judged, according to the Supreme Court, "by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests."[70]

However, the analysis for courts of whether the state *can* monitor does not fully answer the question of *why* the state monitors. In practice, the Fourth Amendment provides minimal restrictions on regulatory collection of business information.[71] When courts invoke the

68. Table constructed from data in Van Loo, *supra* note 2. The acronyms not already mentioned are the Federal Aviation Administration, Federal Deposit Insurance Corporation, Federal Energy Regulatory Commission, Federal Motor Carrier Safety Administration, Federal Reserve, Food Safety & Inspection Service, Mine Safety & Health Administration, National Credit Union Administration, the Nuclear Regulatory Council, Occupational Safety and Health Administration, and the Office of the Comptroller of the Currency.

69. *See supra* notes 14–15 and accompanying text.

70. Delaware v. Prouse, 440 U.S. 648, 654 (1979).

71. Primus, *supra* note 14, at 255–56 (describing the broad judicial allowances of

Fourth Amendment to strike down monitoring, they find a particular implementation unconstitutional, rather than the agency's underlying authority.[72] As a result, the regulator can still exercise monitoring authority in a different manner, such as by more narrowly tailoring its actions or obtaining an administrative warrant. The Fourth Amendment also does not concern itself with regulators declining to monitor when they could.[73]

A caveat is in order. Lawmakers have numerous tools at their disposal. As an alternative to monitoring, for instance, lawmakers could rely on heavy fines and ex post deterrence.[74] These choices reflect a fundamental regulatory tradeoff between "police patrols" and "fire alarms."[75] Policy designers can devote resources to search routinely for problems—as police do when patrolling the streets—or can wait for someone to pull a fire alarm to alert the authorities.[76] In the case of regulating businesses, regulatory monitors are analogous to police patrols, and fire alarms to employee whistleblowers. At least in some contexts, there is evidence that an increase in regulatory monitoring is more effective than an increase in sanctions.[77] Nonetheless, a comparison of whether monitoring deters better than its many regulatory alternatives is beyond the scope of this Article and has yet to be answered satisfactorily despite decades of study.[78]

More attainable, and still relevant to studying deterrence, is an understanding of the basic factors that lawmakers weigh in deciding to

---

administrative searches under the Fourth Amendment).

72. *Cf.* City of Los Angeles v. Patel, 135 S. Ct. 2443, 2447–48 (2015) (striking down a requirement that hotels store guest records for 90 days); Marshall v. Barlow's, Inc., 436 U.S. 307, 320–21 (1978) (stating that a warrant could be obtained pursuant to a general administrative plan).

73. On nonmonitoring despite authority to do so, see, for example, *infra* Section IV.A.

74. *See, e.g.*, Nicholas R. Parrillo, *Federal Agency Guidance and the Power to Bind: An Empirical Study of Agencies and Industries*, 36 YALE J. ON REG. 165, 209–214 (2019) (discussing factors influencing compliance with agency guidance). Moreover, even in deciding on an ex post regime, lawmakers could choose to depend on administrative agencies or private parties to bring lawsuits, or both.

75. Mathew D. McCubbins & Thomas Schwartz, *Congressional Oversight Overlooked: Police Patrols Versus Fire Alarms*, 28 AM. J. POL. SCI. 165, 165–66 (1984).

76. *Id*. at 166.

77. *See, e.g.*, Michael P. Vandenbergh, *Beyond Elegance: A Testable Typology of Social Norms in Corporate Environmental Compliance*, 22 STAN. ENVTL. L.J. 55, 119 (2003) (concluding in the context of environmental law that "increases in monitoring lead to increases in compliance and performance, but increases in sanctions have limited effect").

78. *See, e.g.*, Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169, 176, 179 (1968) (emphasizing the likelihood of detection and the harshness of punishment in corporate compliance); George J. Stigler, *The Optimum Enforcement of Laws*, 78 J. POL. ECON. 526, 527 (1970) (developing a model on sanctions and the probability of being caught). Part of this has to do with broader challenges in quantifying the effects of regulation. *See, e.g.*, Richard L. Revesz, *Quantifying Regulatory Benefits*, 102 CALIF. L. REV. 1423, 1425–26 (2014).

extend monitoring authority.[79] Three primary indicators of the need for regulatory monitoring are a public interest in preventing harm, information asymmetries, and a lack of faith in self-regulation. The rest of this Part will explore these three factors and then turn to the countervailing considerations of privacy and burden.

1. Public Interest in Prevention

Courts have begun their analysis of whether to uphold monitoring legislation by considering the extent of the public interest.[80] For instance, in various cases they have emphasized the need to promote "public health and safety"[81] or protect the environment.[82] Like the underlying legislation granting monitoring authority, these cases regularly proceed without defining public interest or establishing how one would know whether a public interest exists. Given the breadth of situations in which courts have upheld monitoring authority, and the absence of a prominent example of courts blocking monitoring for failing the public interest requirement, the judicial standard for finding a public interest is low.[83]

The public interest provides a more meaningful filter in monitoring legislation. Two components are particularly important: the mobilization of public opinion and the inadequacy of ex post compensation. In practice, to mobilize public opinion, it has often taken a grave crisis or media outcry. Abraham Lincoln pushed for the first of today's large monitoring regulators, the Office of the Comptroller of the Currency ("OCC"), because of a crisis during the Civil War. Bank collapses from imprudent management outraged depositors who lost their savings and made it harder for the federal government to pay for military supplies and soldiers' wages.[84] In response, Congress passed the National Bank

---

79. Identifying factors weighed contributes to the question of deterrence by, for instance, highlighting variables to be tested empirically. Stated otherwise, to improve a framework, it helps to understand what it is.

80. *See, e.g.*, Camara v. Mun. Court of S.F., 387 U.S. 523, 534–35 (1967) (observing that "it is obviously necessary first to focus upon the governmental interest which allegedly justifies official intrusion upon the constitutionally protected interests of the private citizen").

81. *See*, *e.g.*, *id.* at 535 (concluding that in this case "[t]he primary governmental interest at stake is to prevent even the unintentional development of conditions which are hazardous to public health and safety").

82. *See, e.g.,* S. Yuba River Citizens League v. Nat'l Marine Fisheries Serv., 804 F. Supp. 2d 1045, 1061 (E.D. Cal. 2011).

83. *See, e.g.*, Donovan v. Dewey, 452 U.S. 594, 599 (1981) (explaining the federal interest in mine inspections partly through harms to interstate commerce); *Camara*, 387 U.S. at 535 (mentioning economic harms to property as justifying inspections).

84. *See* Eugene N. White, *Lessons from the History of Bank Examination and Supervision in the United States, 1863-2008*, *in* FINANCIAL MARKET REGULATION IN THE WAKE OF FINANCIAL CRISES: THE HISTORICAL EXPERIENCE, 15, 18 (Alfredo Gigliobianco & Gianni Toniolo eds., 2009).

Act of 1864, which established the OCC, authorized the on-site examination of bank affairs, and required monthly reports of their accounts to the agency.[85] At other times, muckrakers or advocates have raised awareness. For instance, Congress passed the Meat Inspection Act of 1906 after Upton Sinclair's *The Jungle* alarmed the public with graphic descriptions of filthy food production.[86]

The second element of a public interest in monitoring is the belief that waiting to act until after the harm has materialized would be insufficient because of an "irreparable harm."[87] Regulatory monitoring becomes more appealing if courts' ex post compensation is seen as inadequate once families have lost their homes due to risky bank behavior or beaches have become polluted by an oil spill.

2. Information Asymmetries

The less regulators know about a firm's activities, the more important it is to compel information production to determine whether intervention is needed. Courts have repeatedly cited the ease with which businesses can conceal violations and falsify information as a rationale for regulatory monitoring.[88] However, judges look unfavorably on monitoring when alternative sources of information are available.[89] In other words, monitoring is seen as a last resort, only to be used when alternative means of information collection, such as consumer complaints, are insufficient.[90]

---

85. National Banking Act of 1864, Pub. L. No. 103-325, 13 Stat. 99 (1864); *see also* Bank Activities and Operations, 69 Fed. Reg. 1895 (Jan. 13, 2004).

86. Meat Inspection Act, Pub. L. No. 59-242, 34 Stat. 1260 (1907) (codified at 21 U.S.C. §§ 601–695 (2012)); Roger Roots, *A Muckraker's Aftermath: The Jungle of Meat-Packing Regulation After a Century*, 27 WM. MITCHELL L. REV. 2413, 2413 (2001).

87. *S. Yuba River Citizens League*, 804 F. Supp. 2d at 1061 ("The court finds that inspections . . . required by the current sediment management plan are necessary to prevent irreparable harm . . . .").

88. *See*, *e.g.*, Liberty Coins, LLC v. Goodman, 880 F.3d 274, 285–86 (6th Cir. 2018) (summarizing the line of cases discussing the necessity requirement as based on the ease of falsification of the relevant information or ease of concealing violations).

89. *See, e.g.*, Appeal of FTC Line of Bus. Report Litig., 595 F.2d 685, 709 (D.C. Cir. 1978) (per curiam) (assessing the validity of the FTC's information collection by noting that "the information sought was not available to the FTC from another federal source"); *see also* New York v. Burger, 482 U.S. 691, 702–03 (1987) (finding that alternatives to warrantless inspections of business premises might not work as well).

90. *See* Camara v. Mun. Court of S.F., 387 U.S. 523, 537 (1967) (weighing whether "any other canvassing technique would achieve acceptable results"). The EPA, for instance, complements its factory inspections with remote devices measuring general pollution output in a given geography. *Air Data Basic Information*, EPA, https://www.epa.gov/outdoor-air-quality-data/air-data-basic-information (last visited Sept. 22, 2019) [https://perma.cc/A7JD-8JCZ] (noting that EPA data is collected both through "monitoring stations owned and operated mainly by state environmental agencies" and through emissions readings taken through factory inspections).

The congressional record surrounding the creation of the OCC shows a similar emphasis on information asymmetries. Lawmakers believed that "very full and very stringent" examination authority was necessary so that a bank could not "be conducted fraudulently or dishonestly without exposure."[91] Lawmakers consequently mandated a system based on government bureaucrats, called examiners, appearing unannounced at banks across the nation.[92]

The relevant information asymmetry is not only that between the business and the regulator, but also between the business and the public. In passing the Meat Inspection Act, lawmakers emphasized the public health interests in preventing sellers from causing "injury to the uninformed" and concern about what the slaughterhouses and meatpackers would do behind closed doors.[93] Nobel Prize–winning economics research has provided further theoretical and empirical support for concluding that information asymmetries are pervasive between businesses and that they create problems for regulators.[94]

3. Self-Regulatory Shortcomings

Sinclair's muckraking illustrates another factor pushing policymakers toward monitoring: the perception of inadequate self-regulation. The starting point in any industry has typically been that "the enlightened self-interest of an entrepreneur sufficed to guarantee the public safety."[95] In other words, once business managers are aware of the consequences—whether reputational or otherwise—of any bad acts, they can be trusted to take appropriate precautions. Events have repeatedly caused lawmakers to question that assumption.

For instance, bank managers regularly acted carelessly in using depositors' funds prior to the Civil War, despite laws punishing banker misconduct, and despite the risk of ruined reputations in the community.[96] More recently, food company managers knew that selling tainted products could harm their brands and yet numerous people died from salmonella in peanut butter, ice cream, and other packaged

91. CONG. GLOBE, 37th Cong., 3d Sess. 824 (1863).

92. White, *supra* note 84, at 21.

93. 40 CONG. REC. 1133 (1906) (statement of Mr. Heyburn).

94. *See, e.g.*, George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q. J. ECON. 488 (1970); Jean Tirole, *Market Failures and Public Policy*, NOBEL PRIZE 513–15 (Dec. 8, 2014), https://www.nobelprize.org/uploads/2018/06/tirole-lecture.pdf [https://perma.cc/3YFU-EZVT].

95. John G. Burke, *Bursting Boilers and the Federal Power*, 7 TECH. & CULTURE 2 (1966).

96. *See* White, *supra* note 84, at 20.

foods.[97] And oil company executives were aware that environmental disasters could devastate their business prior to the Deepwater Horizon oil spill, which cost BP tens of billions of dollars.[98]

Of course, as a practical matter, it is unrealistic to expect perfect compliance. And it is a matter of debate whether a crisis prompts Congress to act in ways it should have all along, or to overreact in the wake of disaster.[99] Nor is it necessarily clear the extent to which the self-regulatory fault lies solely with the business or with the larger legal environment. But empirical studies have found that regulatory monitoring improves self-regulation, at least in some industries.[100] One of the theoretical reasons why monitoring may be necessary beyond strong ex post deterrence is that people operate in a boundedly rational manner that makes them underestimate the likelihood of a bad event happening to them (and to the business they run), such as an oil spill or a bank failure.[101] Regardless of the empirical results, throughout history, policymakers have regularly concluded that firms neglected to adopt appropriate risk management practices even when the law already imposed ex post punishment.[102]

C. Traditional Limits on Monitoring: Privacy and Burden

This Section provides an overview of the two basic elements weighing against monitoring: privacy and burden. The discussion focuses on how lawmakers and judges have traditionally examined these considerations. As Part III will explain, these two factors are evolving in the face of increasingly digital businesses.

---

97. Debra M. Strauss, *An Analysis of the FDA Food Safety Modernization Act: Protection for Consumers and Boon for Business*, 66 FOOD & DRUG L.J. 353, 353–54 (2011).

98. *Cf.* David M. Uhlmann, *After the Spill Is Gone: The Gulf of Mexico, Environmental Crime, and the Criminal Law*, 109 MICH. L. REV. 1413, 1415 n.6, 1429 (2011) (discussing Deepwater Horizon in the context of prior penalties).

99. *See, e.g.*, David Kamin, *Legislating Crisis*, *in* THE TIMING OF LAWMAKING 34 (Frank Fagan & Saul Levmore eds., 2017).

100. *See, e.g.*, Jodi L. Short & Michael W. Toffel, *Making Self-Regulation More Than Merely Symbolic: The Critical Role of the Legal Environment*, 55 ADMIN. SCI. Q. 361, 361 (2010) ("We find that organizations are more likely to follow through on their commitments to self-regulate when they (and their competitors) are subject to heavy regulatory surveillance . . . .").

101. *See* Christine Jolls, *On Law Enforcement with Boundedly Rational Actors, in* THE LAW AND ECONOMICS OF IRRATIONAL BEHAVIOR 268, 268–286 (Francesco Parisi & Vernon L. Smith, eds., 2005) (discussing the challenges of deterrence with boundedly rational actors); Edward Rubin, *Can the Obama Administration Renew American Regulatory Policy?*, 65 U. MIAMI L. REV. 357, 393 (2011) (discussing the end of President Reagan's rational actor theory of government).

102. For a review of the legislation and regulatory responses following these incidents, see, for example, Van Loo, *supra* note 2.

1. Privacy

Historically, a primary source of resistance to regulatory monitoring was business owners' privacy interests.[103] This resistance can be seen in early legislative discussions. In the early 1800s, for instance, steamboat engineers consistently took their own lives and those of thousands of passengers by operating their boats while "ignorant, careless and usually drunk."[104] One congressman framed proposed inspection legislation as being about "[w]hether we shall permit a legalized, unquestioned, and peculiar class in the community to go on committing murder at will," but the bill still met with considerable resistance on the basis of "the sanctity of private property rights."[105]

The interest in protecting businesses from state searches was not as strong as that for personal matters. In *Oklahoma Press Publishing Co. v. Walling*, the Department of Labor sought to compel a media company to produce a broad array of books and records.[106] In rejecting the company's claim of a Fourth Amendment privacy violation, the Supreme Court observed, "[I]t has been settled that corporations are not entitled to all of the constitutional protections which private individuals have in these and related matters."[107] Additionally, Fourth Amendment jurisprudence omitted noncriminal searches until the twentieth century.[108]

Despite the lower level of privacy-related protections afforded to businesses, courts eventually added regulatory monitoring of businesses to the sphere of activities protected by the Constitution. In *Marshall v. Barlow's, Inc.*, the Supreme Court held that the Fourth Amendment protected a plumber from a suspicionless, warrantless Occupational Safety and Health Administration inspection of his site of business.[109] Business owners' privacy interests remain a factor that weighs against routine administrative monitoring of businesses. For

---

103. DOCUMENTS OF AMERICAN HISTORY 63, 143–49 (Henry Steele Commager, ed., 8th ed. 1968).

104. *See* Burke, *supra* note 95, at 11.

105. *Id.* at 21.

106. 327 U.S. 186, 189 (1946).

107. *Id.* at 205.

108. *See* Camara v. Mun. Court of S.F., 387 U.S. 523, 538 (1967) (requiring a warrant for health and safety inspections, and overturning *Frank v. Maryland*, 359 U.S. 360 (1959)).

109. *See* 436 U.S 307, 321 (1978) (observing that the enforcement needs must be weighed against the privacy guarantees of an inspection statute); *see also* See v. City of Seattle, 387 U.S. 541, 543 (1967) ("The businessman, like the occupant of a residence, has a constitutional right to go about his business free from unreasonable official entries upon his private commercial property.").

some courts, privacy includes maintaining sole possession of valuable data and retaining customers who might become disgruntled if their information were passed on to government officials.[110]

2. Burden

Another long-standing argument against monitoring has perhaps increased in importance in the modern era: burden. The business costs of designing and managing internal compliance systems, as well as taxpayer dollars used to fund a labor-intensive oversight force, can be substantial.[111]

In analyzing burden, the Supreme Court has considered whether the information requested is "limited in scope, relevant in purpose, and specific."[112] The state entity collecting the information is expected to minimize the burden in providing the information.[113] As a judicial matter, the burden analysis imposes "rather minimal limitations on administrative action."[114] A federal court did, however, strike down a city ordinance largely due to excess burden because it required Airbnb to hand over data, each month, about every host in New York.[115]

The possibility of excess burden weighed heavily against granting authority for early safety inspections.[116] Legislatures sometimes have attempted to specify that the scope of authorized monitoring is exceeded if "the information or records requested are unusually voluminous in nature."[117] Beyond concerns about preventing a regulatory "fishing expedition," lawmakers weigh arguments about

---

110. *See, e.g.*, Airbnb, Inc. v. City of New York, 373 F. Supp. 3d 467, 484 (S.D.N.Y. 2019) (dividing Airbnb's privacy interests into "competitive" in terms of keeping data from rivals, and "customer relations" in wanting to retain customers).

111. *See* Sean J. Griffith, *Corporate Governance in an Era of Compliance*, 57 WM. & MARY L. REV. 2075, 2102–03 (2016) ("Although figures vary widely depending upon company size, average compliance budgets are in the millions of dollars for multinational companies and for companies in regulated industries.").

112. See v. City of Seattle, 387 U.S. at 544; *see also* Donovan v. Lone Steer, Inc., 464 U.S. 408, 411, 415 (1984) (reiterating a similar standard for production of records).

113. *See* Appeal of FTC Line of Bus. Report Litig., 595 F.2d 685, 709 (D.C. Cir. 1978) (per curiam) (offering as one of the explanations for upholding the FTC's line of business reporting that "the Commission had sufficiently minimized the respondents' burden of compliance with the reporting requirement").

114. See v. City of Seattle, 387 U.S. at 545.

115. *Airbnb*, 373 F. Supp. 3d at 490–92.

116. *See* Burke, *supra* note 95, at 11 (discussing concerns about costs to business owners of inspecting steamboats).

117. 18 U.S.C. § 2703(d) (2012) ("A court . . . may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.").

efficiency due to the economic benefits that lower business costs can bring to society.[118]

In summary, core considerations weighing in favor of monitoring are (1) a compelling public interest, (2) information asymmetries, and (3) publicly salient failed self-regulation. These factors are present at least to some extent in some of the most prominent early extensions of monitoring authority. Pushing against those three considerations are (4) privacy and (5) the economic costs of monitoring. A more systematic study would be necessary to assess the relative influence and pervasiveness of each of these five factors across all historical instances of monitoring legislation. In theory, these five factors could also enable the type of cost-benefit analysis used throughout the administrative state for deciding whether to take a given course of regulatory action.[119] In the absence of any such systematic analysis, as the Supreme Court has explained, "Time and experience have forcefully taught that the power to inspect . . . is of indispensable importance . . . ."[120]

II. FACTORS IN FAVOR OF MONITORING PLATFORMS

The previous Part explained how monitoring of businesses is common among regulators and outlined the factors for and against monitoring. This Part begins to apply those factors to platforms run by large technology companies such as Google, Amazon, and Facebook. Although many scholars have analogized platform risks to those in heavily monitored industries such as pharmaceuticals,[121] oil,[122]

---

118. *Airbnb*, 373 F. Supp. 3d at 491.

119. On the use, importance, and challenges of cost-benefit analysis, see generally Michael A. Livermore & Richard L. Revesz, *Retaking Rationality Two Years Later*, 48 HOUS. L. REV. 1 (2011).

120. Camara v. Mun. Court of S.F., 387 U.S. 523, 537 (1967) (stating that there is "unanimous agreement" for routine periodic inspections of all structures to achieve effective compliance). Courts have consistently upheld agencies' ability to collect regulatory information. *See, e.g.*, Donovan v. Dewey, 452 U.S. 594, 602 (1981) (mines); United States v. Biswell, 406 U.S. 311, 313 (1972) (gun sales); Colonnade Catering Corp. v. United States, 397 U.S. 72, 77 (1970) (liquor sales).

121. Andrew Tutt, *An FDA for Algorithms*, 69 ADMIN. L. REV. 83, 122 (2017) ("Given the close analog between complex pharmaceuticals and sophisticated algorithms, leaving algorithms unregulated could lead to the same pattern of crisis and response.").

122. *See* Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1154 ("Just as oil made machines and factories run in the Industrial Age, Big Data makes the relevant machines run in the Algorithmic Society."); Julie E. Cohen, *The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy*, 31 PHIL. & TECH. 213, 215 (2017) (comparing the surveillance economy to raw material extraction from the public domain and to European sovereigns' financing of explorers, who by "naming and staking claim to hitherto undiscovered lands marked those lands as ownable resources and their contents as available for harvesting or capture"); Dennis D. Hirsch, *The Glass House Effect: Big Data, the New Oil, and the Power of Analogy*, 66 ME. L. REV. 373, 375 (2014) (noting that tankers spill oil, despoiling coastlines and waters, in a manner analogous to

transportation,[123] and finance,[124] those discussions are focused on other dimensions of the regulatory analogy and thus pay little if any attention to regulatory information collection.

The analysis of platforms serves several purposes. It provides a case study to flesh out the normative framework for monitoring. Moreover, the study of platforms provides a window into some of the dynamics facing monitoring in an increasingly digital world. Finally, the considerable influence of technology firms adds immediacy and practical importance to this case study as policymakers worldwide move toward regulatory oversight. If implemented, a monitoring program would initially enable learning to develop new regulatory standards and later provide a mechanism for adapting regulations to a fast-changing industry.[125] In terms of enforcement, monitoring would serve to help regulators identify platforms' violations of broad existing laws, such as general consumer protection and antitrust statutes,[126] as well as violations of any future platform-specific regulation.

A. Public Interest in Preventing a Harm

Scholars have identified numerous justifications for regulating portions of the platform economy. This Section looks at four of these: (1) privacy violations, (2) election engineering, (3) consumer harms, and (4) speech moderation. Many of these justifications fall under conventional rationales for monitoring—to correct a market failure or protect other core values.[127] Each is examined for whether it demonstrates a public interest in need of prevention—meaning that ex post court remedies, or waiting for the harm and punishing the wrongdoer afterwards, would prove inadequate.

---

how large companies like Target, Uber, and Equifax have allowed hackers access to hundreds of millions of credit cards, passwords, and social security numbers).

123. *See* Ganesh Sitaraman, *Regulating Tech Platforms: A Blueprint for Reform*, GREAT DEMOCRACY INITIATIVE 3, 5 (2018), https://greatdemocracyinitiative.org/wp-content/uploads/2018/03/Regulating-Tech-Platforms-final.pdf [https://perma.cc/NA2T-LQVQ] (analogizing tech platforms' antitrust challenges to railroads, public accommodations, and utilities).

124. *See, e.g.*, Nizan Geslevich Packin, *Too-Big-to-Fail 2.0? Digital Service Providers as Cyber-Social Systems*, 93 IND. L.J. 1211 (2018) (comparing digital service providers to major financial institutions); K. Sabeel Rahman, *The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept*, 39 CARDOZO L. REV. 1621 (2018) (analogizing platforms to finance and telecommunications).

125. On how monitoring informs policymaking, see Van Loo *supra* note 2.

126. *See infra* note 337 and accompanying text.

127. *See* OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, CIRCULAR A-4, REGULATORY ANALYSIS 4 (2003), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A4/a-4.pdf [https://perma.cc/F5EL-69C5] ("Correcting market failures is a reason for regulation . . . . Other possible justifications include improving the functioning of government, removing distributional unfairness, or promoting privacy and personal freedom.").

1. Privacy Harms to Individuals

Platforms can harm consumers, purposefully or accidentally, by allowing their data to reach third parties. Platforms purposefully sell personal data, or the advertising insights gained from analyzing such data, to third parties.[128] Facial recognition technologies can identify customers when they enter an establishment, and algorithms can search a customer's past transactions to determine whether a sales representative should approach.[129] Wearable devices, such as FitBit, collect health and behavior data for use by insurance companies setting monthly premiums, lenders establishing credit rates, and even employers deciding whether to hire.[130] While this data may benefit consumers by tailoring products, data sharing can also enable companies to charge consumers more by identifying consumers that are naïve or complacent.[131]

Firms' privacy practices also implicate nonmonetary values. Facebook recently came under criticism for allowing a data broker, Cambridge Analytica, to obtain millions of users' account information. Cambridge Analytica then used that data to promote election candidates. From a legal perspective, this conduct was problematic because Facebook's privacy disclosures did not make it clear that data would be used for such purposes.[132]

Privacy harms also occur when a firm fails to safeguard data. By infiltrating the systems of Uber, Yahoo, and other platforms, hackers have acquired hundreds of millions of people's names, social security numbers, birth dates, addresses, credit card information, and other personal information.[133]

Once data is stolen, it can be resold on the dark web, living on indefinitely in the hands of thieves.[134] Regardless of future government

---

128. *See, e.g.*, Calo & Rosenblat, *supra* note 12, at 1676.

129. *See* Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 355 (2015) ("We live in a world where every action we take can be observed, recorded, analyzed, and stored.").

130. *See* Alexandra Troiano, *Wearables and Personal Health Data Putting a Premium on Your Privacy*, 82 BROOK. L. REV. 1715, 1715 (2017).

131. *See infra* Section II.A.3 (discussing transactional harms).

132. Congress and the FTC have given firms broad legal leeway to use consumer data as they like—so long as they are candid about it. Morgan Hochheiser, *The Truth Behind Data Collection and Analysis*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 32, 35–37 (2015). The efficacy of this approach is considered in the discussion of self-regulation. *See infra* Section II.C.

133. *See, e.g.*, Tara Siegel Bernard et al., *Equifax Attack Exposes Data of 143 Million*, N.Y. TIMES, Sept. 8, 2017, at A1.

134. *See* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web,* 69 STAN. L. REV. 1075, 1090 (2017) ("Modern criminals use the dark web to carry out

intervention, hacking victims may need to take additional precautions. Impersonators have opened various accounts, left bills unpaid, and even committed crimes that later appear on innocent parties' records.[135] Some of these issues have taken the victims years, and many court battles, to resolve.[136] The stress of a criminal accusation cannot be undone—to the extent that "the process is the punishment,"[137] the ultimate arrest of the perpetrator would prove insufficient. Further, the victim is left in fear of it all happening again because the data could remain available to criminals.

Thus, platforms implicate an important public interest in privacy. And ex post remedies appear inadequate. Platforms' privacy implications therefore demonstrate the basic elements of a public interest in prevention.

2. Influencing Civic Behavior: Election Engineering

Several years after Jonathan Zittrain warned that Facebook could alter the outcome of "a hypothetical hotly contested future election,"[138] the Russian government attempted just that. From 2015 to 2016, computer scientists sponsored by the Russian government created social media accounts posing as Black Lives Matter supporters or the Tennessee Republican Party, gaining hundreds of thousands of followers.[139] They deployed bots, or autonomous programs that interact with computer systems, to create and spread messages.[140] By one count, these bots reached 126 million voters in an effort to spur support for Bernie Sanders and Donald Trump.[141]

Concerns about online platforms influencing elections find additional support in experimental research. One study examined whether the Facebook news feeds influenced voting behavior in the

---

technology-driven crimes, such as computer hacking, identity theft, credit card fraud, and intellectual property theft.").

135. *See, e.g.*, Randal C. Archibold, *A 17-Year Nightmare of Identity Theft Finally Results in Criminal Charges*, N.Y. TIMES, Apr. 13, 2007, at A10.

136. *See* Chris Jay Hoofnagle, *Internalizing Identity Theft*, 13 UCLA J.L. & TECH. 1 (2009); Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1244 (2003).

137. MALCOLM M. FEELEY, THE PROCESS IS THE PUNISHMENT: HANDLING CASES IN A LOWER CRIMINAL COURT (1979).

138. Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. FORUM 335, 336 (2014).

139. Apuzzo & LaFraniere, *supra* note 8.

140. Mike Isaac & Daisuke Wakabayashi, *Broad Reach of Campaign by Russians Is Disclosed*, N.Y. TIMES, Oct. 31, 2017, at B1.

141. *Id.*

2010 congressional elections.[142] The researchers inserted graphics with voting booth locations and friends' "I Voted" buttons in some users' feeds, while withholding such graphics from others.[143] The results suggest that about 340,000 people voted nationwide as a result of the interventions. Those results seem modest compared to the study's sixty million participants, but recall that ten years earlier, the 2000 presidential election was decided by 537 votes.[144] It is further possible that alternative intervention designs could produce a greater impact, particularly if messages are targeted at certain political groups.[145] The study thus demonstrates the potential for an election to be "quietly engineered" using platforms.[146]

There is no clearly sufficient remedy when election tampering becomes observable after the fact. A repeat election would surely prove contentious and would risk undermining stability and public faith in elections.[147] Additionally, it might take months or years to reveal the manipulation, as it did with Russian tampering.[148] Influences on civic behavior thus likely satisfy the requirement of a public interest worth preventing.

3. Transactional Harms

Platforms drive diverse economic activities. Search engines such as Expedia help people decide what to buy and for how much. Bitcoin exchanges and financial apps like Venmo enable transactions to occur through new payment systems. Consumers are beginning to outsource shopping and finance to digital butlers, or robo-advisers, which find the best deals and purchase products when the consumer simply clicks "approve."[149] Although they bring great benefits, these emerging

142. Robert M. Bond et al., *A 61-Million-Person Experiment in Social Influence and Political Mobilization*, 489 NATURE 295, 295 (2012).

143. *Id.*

144. *Id.*

145. *See* Zittrain, *supra* note 138, at 336–39.

146. *See id.* at 339 (referring back to the hypothetical election).

147. *See* Jeffrey A. Karp et al., *Dial 'F' for Fraud: Explaining Citizens' Suspicions About Elections*, 53 ELECTORAL STUD. 11, 17 (2018) (explaining that doubts regarding the "integrity and security" of the election process and management can "erode citizen's trust" in political actors, the government and democracy).

148. *See* Scott Shane & Mark Mazzetti, *The Plot to Subvert an Election: Unraveling the Russia Story So Far*, N.Y. TIMES (Sept. 20, 2018), https://www.nytimes.com/interactive/2018/09/20/us/politics/russia-interference-election-trump-clinton.html [https://perma.cc/Y3AT-845A] (providing a timeline which illustrates that the federal investigation into Russian tampering did not begin until months after Trump won the 2016 presidential election).

149. *See generally* Michal S. Gal & Niva Elkin-Koren, *Algorithmic Consumers*, 30 HARV. J.L. & TECH. 309 (2017).

intermediaries can skew information in ways that cause costly mistakes.

Consumer harms can, in the extreme, lead to physical injuries. For example, investigative journalists uncovered in 2017 that TripAdvisor had removed posts that talked about crimes committed in hotels.[150] Many guests had, for instance, posted about being assaulted and robbed at a vacation resort in Riviera Maya, Mexico, but had their posts deleted.[151] Subsequent travelers chose to go to the same resort after reading TripAdvisor's redacted reviews, only to become victims of those same crimes.[152] Because unfavorable reviews would deter hotels from advertising on the site, TripAdvisor may have had incentives to delete reviews alleging assault.[153] Regardless of the motives, when business practices jeopardize personal safety, legal design principles generally prefer ongoing monitoring.[154]

Other platform-facilitated transactions result in discrimination and monetary harms. Repeated studies found that Airbnb hosts are more likely to cancel reservations from guests thought to be racial minorities.[155] Investigations faulted Amazon and Facebook for deceiving consumers, including many children, into paying hundreds or thousands of dollars through in-app purchases, which allow a video game player to purchase additional abilities or time with a quick click.[156] Facebook employees referred to such practices as "friendly fraud," and called children racking up thousands of dollars in fees "whales," a term used by casinos to refer to heavy gamblers.[157]

---

150. Raquel Rutledge & Andrew Mollica, *Misery in Mexico: Tourists Say TripAdvisor Blocked Warnings*, MILWAUKEE J. SENTINEL, Nov. 1, 2017, at A1.

151. *Id.*

152. *Id.*

153. *Id.*

154. This can be seen in safety-related agencies that overwhelmingly rely on monitoring, such as the FAA, FDA, and OHSA. *See generally* Van Loo, *supra* note 2.

155. *See* Press Release, Dep't of Fair Emp't & Hous., Department Of Fair Employment And Housing Reaches Agreement With Former Airbnb Host Who Cancelled Reservation Texting "One word says it all. Asian." (July 13, 2017), https://www.dfeh.ca.gov/wp-content/uploads/sites/32/2017/07/2017-07-13-Suh-Airbnb-Press-Release.pdf [https://perma.cc/4Y38-PT9F] [hereinafter Airbnb Agreement]; *infra* notes 197–200 and accompanying text. Platforms may also facilitate other forms of discrimination, such as that based on age. *See* Ifeoma Ajunwa, *Age Discrimination by Platforms*, 40 BERKELEY J. EMP. & LAB. L. 1, 1 (2019).

156. *See* F.T.C. v. Amazon.com, Inc., No. C14-1038-JCC, 2016 WL10654030, at *11 (W.D. Wash. July 22, 2016) (holding Amazon accountable for third-party app developers' charges through its app store and on Kindle products); I.B. *ex rel.* Fife v. Facebook, Inc., 905 F. Supp. 2d 989, 996 (N.D. Cal. 2012) (class action regarding in-app purchases made by minors on Facebook).

157. *See* Order Granting in Part and Denying in Part Motion for Leave to Intervene and to Unseal Judicial Documents at Ex. K, Bohannon v. Facebook, Inc., No. 12-cv-01894-BLF (N.D. Cal. Jan. 24, 2019), ECF 193-6 ("Friendly Fraud – what it is, why it's challenging, and why you shouldn't try to block it."); Facebook's Opposition to The Center for Investigative Reporting Inc.'s

At a more subtle level, search results generated for a product on Amazon, eBay, or other sites can subtly cause consumers to pay more simply by making it harder to find the best deal or offering confusing product specifications, through a tweak to the search algorithm.[158] Those practices have come to light in part because academics have occasionally obtained unusual access to internal company data.[159] From a theoretical perspective, a growing number of antitrust scholars have argued that the monopoly power of online platforms may be used to bankrupt competitors and ultimately lead to higher consumer prices and less innovation.[160]

Assuming the harm will eventually become known and quantified, consumer protection laws have often viewed ex post remedies as sufficient for monetary harms.[161] Unlike with death or physical injury, the breaching party can, in theory, pay money afterwards or perform specific acts to put the other party in the position she would have been in had the harm never occurred. In ex post transactional regimes, regulators tend to rely more on direct-to-consumer disclosures, in which the business is required to provide clarifying information to consumers, such as the price per unit on grocery shelves.[162] Similarly, the law handles many antitrust violations, such as price fixing, through ex post remedies.[163] The regulator, mostly the FTC at the federal level, does not routinely collect nonpublic information in these transactional contexts.[164]

But lawmakers have concluded that ongoing monitoring is best for some types of transactional harms. In consumer protection, banking

---

Motion for Leave to Intervene and to Unseal Judicial Documents at Ex. OO, Bohannon v. Facebook, Inc., No. 12-cv-01894-BLF (N.D. Cal. Oct. 8, 2018), ECF 179-3 ("Would you refund this whale ticket?").

158. Glenn Ellison & Sara Fisher Ellison, *Search, Obfuscation, and Price Elasticities on the Internet*, 77 ECONOMETRICA 427, 428–29 (2009); Michael Dinerstein et al., *Consumer Price Search and Platform Design in Internet Commerce* 2 (Nat'l Bureau of Econ. Research, Working Paper No. 20415, 2014), http://www.nber.org/papers/w20415.pdf [https://perma.cc/WS33-77T4].

159. *See* Ellison & Ellison, *supra* note 158, at 433 (relying on a company's decision to share nonpublic cost and sales data); Dinerstein et al., *supra* note 158, at 2 (same).

160. *See* ARIEL EZRACHI & MAURICE E. STUCKE, VIRTUAL COMPETITION: THE PROMISE AND PERILS OF THE ALGORITHM-DRIVEN ECONOMY 11–13 (2016); Kenneth A. Bamberger & Orly Lobel, *Platform Market Power*, 32 BERKELEY TECH. L.J. 1051, 1051 (2017); Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 716–17 (2017); John M. Newman, *Antitrust in Digital Markets*, 72 VAND. L. REV. 1497 (2019); John M. Newman, *Antitrust in Zero-Price Markets: Foundations*, 164 U. PA. L. REV. 149, 151 (2015); John M. Newman, *The Myth of Free*, 86 GEO. WASH. L. REV. 513, 515 (2018).

161. *See* Omri Ben-Shahar, *Consumer Protection Without Law*, 33 REGULATION 26, 27 (2010).

162. *See, e.g.*, Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 653–55 (2011) (discussing examples of such disclosure regimes).

163. *See, e.g.*, Khan, *supra* note 160, at 722–25.

164. *See supra* Section I.A (providing an overview of monitoring across regulators); *infra* Section IV.A (discussing the FTC's regulatory approach).

regulators such as the CFPB routinely visit and collect reports from banks in search of unfair and deceptive acts or discriminatory lending.[165] In antitrust, companies must submit sizeable mergers to authorities for approval, rather than completing the merger and letting authorities or competitors sue afterwards.[166] And the New York Stock Exchange ("NYSE"), a private company, must obtain regulatory approval before changing the rules for trading stocks—in part because of its monopolistic nature, which may increase harms such as undetected self-dealing and compromised access to the market.[167]

Some platforms arguably present comparable shortcomings with respect to ex post remedies. Amazon has gatekeeper and network structures, along with difficult-to-observe consumer harms, that raise regulatory challenges similar to stock exchanges.[168] A pure ex post approach poses notable challenges, illustrated by the European Commission's twelve-year process to fine Google $2 billion—the largest monetary penalty in antitrust history—for crushing once-promising startups.[169] Given that digital industries provide first-mover advantages and network effects,[170] a startup has a small window of opportunity to compete that may have closed by the time regulators or courts have obtained the information needed to intervene ex post.

Overall, the heterogeneity of harms makes it difficult to classify platforms' transactional conduct broadly as being better regulated by monitoring or ex post litigation. From an institutional perspective, however, at least some large online platform harms—such as removing safety-related information, causing significant financial harms, and stifling startup businesses—reflect those that have driven policymakers to identify a public interest in preventing the harm using monitoring.

4. Speech Harms

Online platforms such as Instagram, Facebook, Twitter, and YouTube direct the flow of communications among users and must decide what information to allow on their platforms. Some editing of content implicates state accountability. For example, in 2016, an

165. *See infra* note 189 and accompanying text.

166. 15 U.S.C. § 18 (2012).

167. Gordon v. N.Y. Stock Exch., Inc., 422 U.S. 659, 665 (1975).

168. *See* Rory Van Loo, *Rise of the Digital Regulator*, 66 DUKE L.J. 1267, 1319–20 (2017) (analogizing oversight of online platforms to oversight of the NYSE). On the network effects of platforms, see, for example, EZRACHI & STUCKE, *supra* note 160, at 231.

169. Commission Fines Google, *supra* note 10.

170. EZRACHI & STUCKE, *supra* note 160, at 231.

onlooker recorded a police officer shooting Alton Sterling, who was being held to the ground by other officers. In another incident, the girlfriend of Philando Castile filmed the aftermath of his fatal shooting during a traffic stop.[171] These videos' widespread circulation prompted nationwide protests, Department of Justice investigations, and police department reforms, including more widespread body camera requirements.[172] But the movement came close to being technologically blocked. Shortly after the Castile video was posted, Facebook moderators removed it for being too graphic. They reposted it twenty minutes later with a viewer discretion warning,[173] but had the platform gone with its initial decision to take the content down, it could have amounted to a significant speech harm.

Platforms also curate content directed at individuals or groups. Since their early years, Facebook and Twitter have sought to remove harmful content including racist comments and other hateful speech.[174] Yet scholars have argued that these measures have not gone far enough to address revenge porn, cyber harassment, and "troll armies" designed to intimidate critics into silence.[175]

Internet intermediaries have great discretion as moderators because the Communications Decency Act protects them from liability for users' content.[176] For instance, in *Zeran v. America Online, Inc.*, the plaintiff sought damages because AOL failed to remove defamatory posts from its message boards.[177] The court held AOL immune from such suits under the Act, paving the way for broad website operator discretion as to whether and how to curate content.[178]

Moreover, platforms' filtering role has recently intensified. For many years, Twitter moderators allowed white supremacists to use the site but would remove any post deemed offensive.[179] In December of

171. Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1600 (2018).

172. *Id.*

173. *Id.* at 1600–01.

174. *Id.* at 1625–26.

175. *See, e.g.*, Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 62, 66–67 (2009); Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 349 (2014); Tim Wu, *Is the First Amendment Obsolete?*, 117 MICH. L. REV. 547, 548 (2018).

176. *See* 47 U.S.C. § 230(c) (2012).

177. 129 F.3d 327, 330 (4th Cir. 1997).

178. *Id*. at 330–32. *But see* Spy Phone Labs LLC v. Google, Inc., No. 15-cv-03756-KAW, 2016 WL 6025469, at *1, *6–7 (N.D. Cal. Oct. 14, 2016) (denying in part a motion to dismiss based on the Communications Decency Act because of allegations of bad faith).

179. Twitter also withheld official "verification." Thomas Kadri, *Speech vs. Speakers*, SLATE (Jan. 18, 2018, 12:56 PM), https://slate.com/technology/2018/01/twitters-new-rules-blur-the-line-between-extremists-speakers-and-their-speech.html [https://perma.cc/2HWP-BNZF].

2017, however, the company began to suspend many accounts based on the account holder's *offline* persona, a move dubbed "#TwitterPurge."[180] In early 2018, Facebook announced that it would play an editorial role in deciding which news was sufficiently high quality to reach users, rather than solely letting the number of clicks decide.[181]

Although online platforms are private domains, the moderation of online content has free speech implications. When private actors perform a public function, such as by operating corporate towns, some courts have deemed them functionally equivalent to public actors.[182] But courts are reluctant to find public functions, and in analogous contexts, such as shopping malls and public television channels, the Supreme Court has made clear that a private entity does not necessarily perform a public function merely because it holds a forum open to the public.[183]

A recent Court ruling underscores the free speech tension in content moderation. In *Packingham v. North Carolina*, the Court struck down a state statute barring sex offenders from participating in social networks.[184] The Court observed that to prevent "access to social media altogether is to prevent the user from engaging in the legitimate exercise of First Amendment rights."[185] Because the state—not the platform itself—blocked access in this case, it is unclear what remaining ability the state has to regulate platforms' own restrictions on access and content.[186]

In the pre-digital era, the harm of having one's speech blocked or being subject to harassment could not necessarily be undone. Nonetheless, the law has predominantly relied on ex post judicial remedies, such as fines and injunctions, to regulate harassment.[187]

---

180. *Id.*

181. *See* Deepa Seetharaman, *Facebook to Rank News Sources*, WALL ST. J., Jan. 20, 2018, at B1 ("The most 'broadly trusted' publications—those trusted and recognized by a large cross-section of Facebook users—would get a boost in the news feed, while those that users rate low on trust would be penalized.").

182. *See* Marsh v. Alabama, 326 U.S. 501, 502–503, 510 (1945) (holding that a Jehovah's Witness had First Amendment rights while distributing literature on the sidewalk of a privately owned town).

183. Manhattan Cmty. Access Corp. v. Halleck, 139 S. Ct. 1921 (2019); Hudgens v. NLRB, 424 U.S. 507, 519 (1976); Amalgamated Food Emps. Union Local 590 v. Logan Valley Plaza, Inc., 391 U.S. 308, 318–19 (1968), *abrogated by Hudgens*, 424 U.S. at 518–19.

184. 137 S. Ct. 1730, 1737–38 (2017).

185. *Id.* at 1737.

186. *Cf.* Danielle Keats Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep,* 93 NOTRE DAME L. REV. 1035, 1062 (2018) ("[T]ech companies should adopt special policies and procedures to protect against governmental overreach.").

187. Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2340 (2014). Entry restrictions, such as demonstration licenses, have also been used. *See id.* at 2299.

Fully evaluating the wisdom of that emphasis is beyond the scope of this Article, but it is possible that the reliance on ex post measures is partly explained by the impracticability of monitoring all potential harassment in real time. Offline harassment can occur during a completely private interaction, whereas harassment that happens on platforms introduces a third party—the information technology. Therefore, monitoring could be more plausible in the digital context. Facebook, for example, has developed tools to identify harassment, including tracking IP addresses to recognize when blocked users open a new account in order to message the same person who blocked them.[188]

Overall, the strength of the public interest factor varies by the four categories of harm discussed above. Harms such as privacy and election meddling are in need of heightened prevention. Some transactional harms and speech harms have stronger countervailing considerations, such as the possibility of ex post monetary compensation and a preference for not stamping out speech in advance. But many transactional harms merit prevention, and even some speech harms might justify monitoring of the platform's practices. A holistic view of platforms suggests that they meet the basic threshold of implicating public harms worthy of prevention.

B. Information Asymmetries

The second major reason regulators might monitor an industry—information asymmetries—is potentially heightened for online platforms given their limited observability as compared to other monitored industries. Absent a monitoring regime, the government is dependent on how observable a harm is by either those harmed or some third party, such as journalists. However, the more consumers cannot see what is happening to others, and the more complex the underlying decisionmaking process, the more difficult it is for individuals to monitor a company's behavior. One reason why the CFPB regularly examines bank records for personal financial harms, even small fees, is that consumers will not necessarily know they are harmed and would have difficulty knowing whether someone else with the same credit score got a different deal.[189]

188. Antigone Davis, *New Tools to Prevent Harassment*, FACEBOOK NEWSROOM (Dec. 19, 2017), https://newsroom.fb.com/news/2017/12/new-tools-to-prevent-harassment [https://perma.cc/3QJT-VYLS].

189. *See* Van Loo, *supra* note 12, at 1372–73.

Platforms demonstrate incredible complexity through their individualized black-box interfaces.[190] Yet the visibility of platform harms varies by category. Consumers cannot easily observe security precautions and privacy because, by its nature, a company does not share such information publicly.[191] For many instances of identity theft, victims may learn of the harm once they receive a bill for unauthorized purchases or observe an unexplained depletion in their bank account. But consumers will not necessarily know when their data has been hacked. It took years before the public learned of millions of compromised accounts at Yahoo and Uber.[192] Indeed, companies have taken steps to hide such security incidents. Uber paid a ransom to keep the breach quiet.[193]

Nor is the selling or use of personal data easily observable. Consumers may never know that they were routed to a less helpful call center, charged more for a loan, or had their data sold to a third-party data broker such as Cambridge Analytica. Companies are not required to disclose to customers that others paid lower prices.[194]

While elections, transactional consumer harms, and some categories of speech harms may have observable elements, these harms are predominantly opaque. They are marginally more observable than privacy harms in that voters can report questionable election messages in social media feeds, posters can see the number of retweets or video views to infer silencing, and small businesses can run Google searches to learn if they have been delisted.[195] Sometimes platforms even notify users that their post has been removed, or could be required to do so by substantive law.[196] Explicit discrimination can be observed by the victim, as when an Airbnb host cancelled a California mountain cabin rental minutes before the guest arrived by texting, "One word says it all. Asian."[197]

---

190. Oren Bracha & Frank Pasquale, *Federal Search Commission – Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149, 1178 (2008) (discussing the black-box nature of search engines); Van Loo, *supra* note 168, at 1270–72 (describing the nonsalience of digital harms).

191. Chris Jay Hoofnagle, *Assessing the Federal Trade Commission's Privacy Assessments*, IEEE SECURITY & PRIVACY, Mar.-Apr. 2016, at 58, 58.

192. Knutson & McMillan, *supra* note 9.

193. *See, e.g.*, Isaac et al., *supra* note 9.

194. *See* PASQUALE, *supra* note 33, at 163–64 (analyzing the opacity of companies' decisions).

195. For instance, some of Google's small-business competitors suddenly saw their revenues drop precipitously, prompting them to lodge complaints with antitrust regulators. *See* Commission Fines Google, *supra* note 10.

196. *See, e.g.*, Rutledge & Mollica, *supra* note 150 (noting that TripAdvisor issues messages after deleting posts, citing "various reasons for the deletions").

197. Airbnb Agreement, *supra* note 155.

The challenge with many means of observation is that "companies fastidiously study consumers and, increasingly, personalize every aspect of the consumer experience."[198] If an Airbnb host denies an individual's request for lodging, it is unclear whether other consumers of different races received preferential treatment. However, insight is possible with the right information and access. One field experiment used fake accounts and over six thousand messages to determine that on average, hosts were sixteen percent less likely to accept reservations from distinctly African-American names, even when every other aspect of the guest's profile was identical.[199] Airbnb swiftly blocked the academics' accounts, and platforms have even more sophisticated techniques to identify fake accounts.[200] Other researchers seeking to understand related problems, such as why Google shows lower-paying job ads to women than to men, have faced similar barriers of access to the relevant nonpublic information.[201] As a result, relying on the cooperation of platforms to share necessary information will not necessarily suffice to identify and understand harms.

Any two social media feeds may differ greatly based on the users' digital profiles, including makeup of followers and past clicks.[202] The products or election advertisements users see may also vary. Any given person has limited knowledge of other user experiences, since most only have access to their single feed. Consequently, Instagram moderators may deprioritize or bury a post in users' feeds without the poster knowing. Facebook voluntarily announced its platform's ability to influence elections, although it could have withheld that private information.[203] Essentially, platforms can effectively silence tweets, tailor election news, or aid sellers in selectively charging higher advertised prices, all while obscuring that conduct from affected individuals.

It would be a complex undertaking for the harmed party to identify and track the many subtle ways that any two feeds differ in

198. Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 995 (2014).

199. Benjamin Edelman et al., *Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment*, AM. ECON. J., Apr. 2017, at 1, 1–2.

200. *See id.* at 4.

201. *See* Amit Datta, Anupam Datta, Jael Makagon, Deirdre K. Mulligan & Michael Carl Tschantz, *Discrimination in Online Advertising: A Multidisciplinary Inquiry*, 81 PROC. MACHINE LEARNING RES. 1, 14 (2018).

202. Roger McNamee, *How to Fix Facebook—Before It Fixes Us*, WASH. MONTHLY (Jan./Feb./Mar. 2018), https://washingtonmonthly.com/magazine/january-february-march-2018/how-to-fix-facebook-before-it-fixes-us/ [https://perma.cc/CS87-QP4P].

203. Kevin Roose, *What Has Facebook Learned Since the 2016 Election?*, N.Y. TIMES, Oct. 12, 2017, at B3 (interviewing Facebook's Chief Security Officer, who stated that Facebook undertook research into behavioral influence of its own volition).

terms of the ordering, timing, and composition of items displayed. Analyzing millions of feeds would require a sophisticated analysis with unprecedented access to many individuals' personal accounts.[204] Individuals and small businesses, in particular, would likely be unable to monitor effectively.

Even if users observed that their business was deprioritized or that an advertisement was tailored, they would not necessarily know why. Platforms use complex, continually changing algorithms to produce web search results and social feed content.[205] Users would likely be unable to determine whether they were losing out in the search results based on the competitive merits or due to the gatekeeper's desire to lessen competition.

These information asymmetries reflect those in other monitored industries. Like social media feeds, consumer financial products are tailored to the individual.[206] A borrower generally cannot attribute higher mortgage rates to illegal factors, such as race, or may be unable to understand the fine print terms that impose hidden fees.

Additionally, by some accounts, companies such as Google and Apple have taken corporate secretiveness to new levels in an effort to prevent competitors from copying innovations.[207] They use nondisclosure and nondisparagement agreements liberally, and develop tools for hiding information.[208] One Uber software program identified transportation regulators; when they opened the app, Uber would create a "ghost screen" displaying fake drivers. After the regulator requested a ride, the cars would disappear from the screen, giving the impression that cars were no longer available.[209] Platforms can thus deploy legal and technological tools not only to limit public information access, but also to tailor user experiences such that one external observer's inferences would be irrelevant to another's. Given the intensely secretive culture and inscrutability of digital technologies,

204. Of course, data for some accounts is publicly available, but Facebook would be able to control which accounts are subject to manipulation and whether that data is available publicly.

205. *See* Bracha & Pasquale, *supra* note 190, at 1168.

206. *See, e.g.*, Rory Van Loo, *Digital Market Perfection*, 117 MICH. L. REV. 815, 835 (2019).

207. *See, e.g.*, James Grimmelmann, *The Virtues of Moderation*, 17 YALE J.L. & TECH. 42, 67 (2015) (describing Google's secretiveness); Tom C. W. Lin, *Executive Trade Secrets*, 87 NOTRE DAME L. REV. 911, 914 (2012) (describing Apple's secretiveness).

208. *See, e.g.*, SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 56–57 (2019).

209. Mike Isaac, *Uber Uses Tech to Deceive Authorities Worldwide*, N.Y. TIMES, Mar. 3, 2017, at A1.

there may be no other industry with greater public-private information asymmetries than online platforms.[210]

C. Self-Regulation

Historically, monitoring legislation has followed prominent legal violations by businesses—presumably based on the conclusion that the prior reliance on self-regulation was faulty or at least politically unacceptable.[211] By that basic measure, the platform economy, like more heavily regulated industries, has failed the test of self-regulation.[212] Indeed, an industry built in part by skirting the law and evading regulators, with a prominent motto of "move fast and break things,"[213] is an unlikely candidate for self-regulation. But before jumping to the alternative of a full regulatory monitoring regime, it is necessary to consider not only the effectiveness of monitoring, but also the different versions of industry self-regulation as embraced in the literature or utilized by the FTC: public disclosure and private third-party monitoring.

1. Private Monitoring and Transparency

Observers have proposed private monitoring regimes or making information publicly available, thereby letting markets or private actors hold businesses accountable.[214] One version of this is mandated disclosures to the end user. Also, by faulting Facebook for being unclear with users about what would happen to their data, the FTC pushes the platform to disclose risks and harms.[215] Well-designed disclosures can help, but they have traditionally performed poorly because hardly anyone reads the fine print of contracts.[216] Even if people did, they likely

---

210. *Cf.* Cohen, *supra* note 7, at 190 ("The platform-based environment . . . is characterized by both information abundance and endemic information asymmetry.").

211. *See* Van Loo, *supra* note 2, at 384–95.

212. *See supra* notes 8–10 and accompanying text.

213. Elizabeth Pollman & Jordan M. Barry, *Regulatory Entrepreneurship*, 90 S. CAL. L. REV. 383, 446 (2017).

214. *See, e.g.*, Ryan Bubb & Richard H. Pildes, *How Behavioral Economics Trims Its Sails and Why*, 127 HARV. L. REV. 1593, 1597 n.10 (2014) (summarizing the political appeal of mandated disclosures); Alan Schwartz & Louis L. Wilde, *Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis*, 127 U. PA. L. REV. 630, 631 (1979) (arguing that in deciding whether market regulations are warranted, the most important criterion is whether "imperfect information has produced noncompetitive prices and terms").

215. *See* Decision and Order, Facebook, Inc., F.T.C. File No. 0923184, No. C-4365 (F.T.C. July 27, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf [https://perma.cc/2JW9-HPY6].

216. Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1, 1 (2014).

would not understand the contents, and even simpler prominent disclosures often fail to realize their intended purpose.[217]

Disclosures might also target public or third-party experts, which would require platforms to make some part of their underlying code publicly available.[218] Private parties would then periodically observe platforms in a kind of crowd-sourced monitoring. Disclosure-based regulation is one of the most widely supported interventions, both among policymakers and legal scholars, because it preserves freedom of choice.[219] However, without other legal reforms and careful design, such disclosures have limits because voluntary third-party experts—including reputation websites—may lack resources or motivation.[220] Additionally, under any public disclosure regime, competitors would acquire any information released, meaning that such information would need to be more limited.[221] As a result, after a company has transgressed, its settlement agreement with a public entity often requires the hiring of a private third-party monitor to assess compliance.[222]

The FTC applied both mandated disclosures and private monitoring when it learned that Google and Facebook had violated privacy policies in 2011 and 2012. Facebook had allowed its users to keep their information private, but repeatedly made that information public.[223] The consent orders required the companies to pay for third-party "assessments" of their compliance, with heightened privacy policies outlined in the settlement.[224]

Facebook's assessor, PricewaterhouseCoopers, upon reviewing Facebook's online policy and direct assertions, submitted annual reports to the FTC verifying that Facebook was in full compliance and

---

217. *Id.*; Ben-Shahar & Schneider, *supra* note 162, at 665.

218. *See, e.g.*, PASQUALE, *supra* note 33, at 150–51 (discussing transparency in context of firms that use personal data); Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 419–22 (2014) (arguing that transparency of private companies is increasingly important in the big data age).

219. Bubb & Pildes, *supra* note 214, at 1597 n.10.

220. Sofia Ranchordás, *Online Reputation and the Regulation of Information Asymmetries in the Platform Economy*, 5 CRITICAL ANALYSIS L. 127, 129–34 (2018)

221. *See* PASQUALE, *supra* note 33, at 163–64 (discussing balance between trade secrets and monitoring of internet search engines).

222. Cristie Ford & David Hess, *Can Corporate Monitorships Improve Corporate Compliance?*, 34 J. CORP. L. 679, 680 (2009); Vikramaditya Khanna & Timothy L. Dickinson, *The Corporate Monitor: The New Corporate Czar?*, 105 MICH. L. REV. 1713, 1714 (2007); Veronica Root, *The Monitor-"Client" Relationship*, 100 VA. L. REV. 523, 524 (2014). Companies also voluntarily undertake monitoring in response to public regulation. Michael P. Vandenbergh, *The Private Life of Public Law*, 105 COLUM. L. REV. 2029, 2038 (2005).

223. *See* Facebook, Inc., F.T.C. File No. 092-3184, 2011 WL 6092532, at *3 (F.T.C. Nov. 29, 2011) (Agreement Containing Consent Order).

224. *Id.* at *5.

taking the necessary precautions to safeguard user data.[225] Subsequently, evidence emerged that Facebook failed to protect privacy in accordance with its published policies, most prominently when one of its apps helped transfer millions of users' data to Cambridge Analytica for psychological profiling during the 2016 presidential election.[226] It is worth noting that Google and Facebook were able to comply with their third-party assessments by simply making assertions to the third party about their privacy policies, a process that falls short of a full audit.[227] Thus, the performance of these regimes does not reflect how a more empowered third-party auditor would have performed.

Perhaps a truly independent private third party could provide that benefit.[228] Regulators other than the FTC have deployed more powerful private auditors with "unrestricted access" to the regulated entity's documents.[229] In theory, these private monitors could provide many of the benefits of public monitors, and indeed scholars have often proposed private rather than public monitoring of platforms.[230] Private monitors have the advantage of using fewer public resources and avoiding governmental acquisition of private information.

Another common reason for preferring a disclosure-oriented or private third-party regime is that either regime would use monitors with more sophistication and resources than bureaucrats.[231] After all, government agencies pay considerably less than Silicon Valley firms.[232]

---

225. *See* Nicholas Confessore, *Audit Approved of Facebook Policies*, N.Y. TIMES, Apr. 19, 2018, at A18 (discussing the compliance audits and noting that Facebook determined which policies that PricewaterhouseCoopers (now known as PwC) reviewed). *See generally* Hoofnagle, *supra* note 191, at 58 (distinguishing FTC assessments from audits).

226. *See, e.g.*, Philip M. Napoli, *What If More Speech Is No Longer the Solution? First Amendment Theory Meets Fake News and the Filter Bubble*, 70 FED. COMM. L.J. 55, 75–76 (2018).

227. *See* Megan Gray, Understanding and Improving Privacy Audits under FTC Orders (May 5, 2018) (unpublished manuscript), https://ssrn.com/abstract=3165143 [https://perma.cc/KDZ5-4ZPW].

228. *See* G.S. Hans, Note, *Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for A New Era*, 19 MICH. TELECOMM. & TECH. L. REV. 163, 191 (2012) ("Much will depend on the vigor and effectiveness of the privacy audits and the FTC's response.").

229. Root, *supra* note 222, at 584; *see* Khanna & Dickinson, *supra* note 222, at 1732.

230. *See, e.g.*, Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. REV. (forthcoming 2019) (manuscript at 4–5), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3351404&download=yes [https://perma.cc/354Y-M6DE].

231. *Cf.* Vladeck, *supra* note 25, at 514 (2016) (concluding that regulatory auditing of algorithms "would pose an enormous challenge to regulators, who . . . may not have the expertise required to design and carry out a sufficiently robust audit").

232. P'SHIP FOR PUB. SERV. & BOOZ ALLEN HAMILTON, CYBER IN-SECURITY II: CLOSING THE FEDERAL TALENT GAP 25 (2015), https://ourpublicservice.org/wp-content/uploads/2018/09/Cyber_In-Security_II Closing_the_Federal_Talent_Gap-2015.04.13.pdf [https://perma.cc/CU46-58BM] (calculating that senior-level software engineers could make $33,000 more in the private sector than in the federal government and entry-level engineers could make more than $14,000 more).

Moreover, bureaucrats often have protected employment status, which has led critics to argue that regulators cannot easily update their workforce with training or more technologically savvy employees.[233] Many believe that a third-party regulatory regime would make it less likely that "the government will remain several steps behind."[234] In light of these advantages and the political obstacles to government regulation, wholly private monitoring could offer a sensible policy option.

Nonetheless, private monitors also have several shortcomings. A company hired to monitor has incentives to please the customer paying the bills—which is typically the regulated entity.[235] A secretive industry is also unmotivated to share its inner workings with another business or the public.[236] Considering these factors and the empirically supported successes of government monitoring in other industries, it is likely that regulatory monitoring of platforms—or at least publicly accountable private monitors—would offer the best option as long as the government reflects democratic values.

2. Regulatory Monitoring Design and Effectiveness

One challenge for the typical analysis is that an incident of failed self-regulation does not mean that a direct monitoring regime would have done better. Companies still engage in substantial wrongdoing in heavily monitored industries. Despite having OCC and CFPB examiners on-site year-round, Wells Fargo employees opened millions of unauthorized accounts in customers' names for years until the publication of a *Los Angeles Times* exposé.[237] Any platform-monitoring regime, even helped by the most sophisticated of private-sector analysts, would have limits.[238] Despite these uncertainties, empirical studies of government inspections across different jurisdictions and

233. Frank Ostroff, *Change Management in Government*, HARV. BUS. REV., May 2006, at 141 (critiquing federal agencies for having inflexible workplaces that inhibit innovation and prioritize the avoidance of failure over promotion of exceptional performance).

234. EZRACHI & STUCKE, *supra* note 160, at 231.

235. The agency usually has at least veto power over the choice. *See* Khanna & Dickinson, *supra* note 222, at 1723. On the related inadequate incentives of stock exchanges to monitor, as well as liability strategies to address such inadequacies, see Yesha Yadav, *Oversight Failures in Securities Markets*, 104 CORNELL L. REV. (forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2754786 [https://perma.cc/FDX4-LPJY].

236. *See supra* Section II.B (discussing platforms' secretive cultures).

237. James Rufus Koren, *Wells Fargo Not the Only Bank to Have Created Unauthorized Accounts—But Regulator Won't Identify Others*, L.A. TIMES (June 8, 2018), http://www.latimes.com/business/la-fi-unauthorized-accounts-occ-20180608-story.html [https://perma.cc/MGE6-KUMH].

238. Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633, 638 (2017) (discussing limitations of auditing algorithms).

timeframes suggest that governmental monitoring increases compliance.[239]

Critics' points about a sophistication imbalance between government and private monitors have merit, but as a basis for resistance to government monitoring, the argument reflects a misconception about the operation of monitoring regimes. From a functional perspective, regulatory monitors utilize three main categories of information collection: direct observations, explanations, and self-regulatory processes. Direct observations would mean examining the activities, such as looking at how the factory machines operate, or perhaps monitoring various outputs, such as chemical discharge into air and ocean waters.[240] The next level would require the business to explain how those specific operations function, perhaps mandating an analysis performed by the business. Instead, many monitors focus on the third category: self-regulatory processes. For example, government inspectors ensure that offshore oil platforms install and use mandatory safety devices that prevent explosion by shutting down drilling if the machinery temperature rises too high.[241] They also look at whether training programs and internal procedures position employees to mitigate and respond to emergencies.[242]

To apply a similar regime to digital platforms, a regulator would ask the platform to identify which internal organizational processes filter out foreign political ads, protect against hackers, or prevent racially discriminatory behavior. The monitor would ideally be technologically savvy, but even one without a strong technology background would be capable of analyzing organizational processes to determine whether firms were asking the right questions and measuring the right outputs. Some outputs would also be discernible to monitors since most platforms have live feeds or other means of communicating to management what is happening.[243]

Dialogue would further allow government monitors to better comprehend complex algorithms. Regulatory monitors do not simply examine in silence, but as part of a dialectic process. Bank employees sometimes need to break down a complex new financial instrument so that the Federal Reserve examiner understands whether it violates the law or poses a new risk.[244] Environmental inspectors "rely on industry

239. *See supra* notes 100–102 and accompanying text.

240. *See, e.g.*, Uhlmann, *supra* note 98, 1426–27.

241. *See* Hayes, *supra* note 56.

242. 40 C.F.R. § 112.21 (2018).

243. *See generally* Klonick, *supra* note 171 (discussing internal moderators' roles).

244. *See* PETER CONTI-BROWN, THE POWER AND INDEPENDENCE OF THE FEDERAL RESERVE 165 (2015) (describing the complexity facing bank supervision).

representatives to explain the technology at a facility."[245] Similarly, regulatory monitors could question platform coders or ask to see the internal reports that those coders produced. In the context of privacy, for instance, regulators could ask platforms to provide privacy impact assessments. They might also routinely ask the regulator to provide any updates to privacy practices within the prior six months, such as any new types of data collected or any new third parties that are receiving user data.

To be clear, even after adopting these approaches, monitors of platforms may still have more blind spots than do monitors in other industries. But perfect regulatory understanding is not the standard. Instead, regulatory comprehension is better seen as existing along a spectrum. Without ex ante monitoring authority, regulators currently operate with minimal algorithmic knowledge. If monitoring increased that comprehension from five to fifty percent, regulators would lack total comprehension, but that increase would be a meaningful advancement. If a disclosure regime would move public oversight from five to ten percent comprehension, but with less burden and more political support, that is an alternative to be weighed—or an additional measure that could create a pluralistic public-private monitoring regime.[246]

It is impossible to know precisely how far any particular regime would move a regulator along the comprehension spectrum. Nor does space allow for determining which items from the menu of monitoring options would work best for platforms—auditing raw complaints or assessing compliance systems, conducting on-site examinations, requiring remote report submissions, or other tactics. Indeed, the answer will vary by the type of harm and platform. But regulatory monitoring would certainly add a significant degree of knowledge to the current state of substantial real-time ignorance in the face of fast-shifting platforms.

III. FACTORS WEIGHING AGAINST MONITORING PLATFORMS

The previous Part showed how the three criteria in favor of monitoring are met at a basic level, at least regarding some harms and platforms. That brings the analysis to two main considerations

245. NAT'L COMM'N ON THE BP DEEPWATER HORIZON OIL SPILL & OFFSHORE DRILLING, DEEP WATER: THE GULF OIL DISASTER AND THE FUTURE OF OFFSHORE DRILLING 28–30, 77 (2011), https://www.sintef.no/globalassets/project/hfc/documents/gpo-oilcommission.pdf [https://perma.cc/8QQ7-Z7SQ].

246. *See, e.g.*, Hannah Bloch-Wehba, *Global Platform Governance: Private Power in the Shadow of the State*, 72 SMU L. REV. 27, 30 (2019) (connecting public and private ordering options).

historically weighing against monitoring: privacy and burden. Each factor is complicated with respect to online platforms given their role in surveillance and their core product being information itself.

A. Business Owners' Privacy

Historically, privacy weighed against monitoring due to the importance of the business owner's reasonable expectation of privacy.[247] However, business owners' privacy expectations have not restricted monitoring in other industries, including the routine collection of sensitive profit data for antitrust scrutiny.[248] Is there any reason to think that business owners' privacy interests carry extra weight for platforms? It helps to approach that question by looking at "the privacy interests of the people involved" rather than the privacy interests of the entity.[249]

Perhaps the best argument is the enhanced role of intellectual property, a key legal tool deployed in platforms' secretive cultures.[250] A regulator that leaked valuable trade secrets would, in a sense, violate the business owners' privacy interests.[251] Although trade secrets and sensitive competitive information are exempt from the Freedom of Information Act,[252] businesses have exploited the Act to access FTC information, demonstrating commercial motivation to exploit monitoring data.[253] Heightened secrecy can, however, be seen in other industries, such as finance, where investment strategies and business acquisitions are closely guarded.[254] Any platform-monitoring regime 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.[255]

It is otherwise difficult to see how the type of information collected for regulatory oversight would meaningfully threaten business owners' privacy. That information would be related to the technologies deployed and the company's interactions with users,

247. *Supra* Section I.C.1.

248. *See supra* Section I.A.

249. *See* Elizabeth Pollman, *A Corporate Right to Privacy*, 99 MINN. L. REV. 27, 33 (2014).

250. *See* sources cited *supra* note 207 and accompanying text.

251. *See* Airbnb, Inc. v. City of New York, 373 F. Supp. 3d 467, 484 (S.D.N.Y. 2019). 252. 5 U.S.C. § 552(b)(1)–(9) (2012).

253. Margaret B. Kwoka, *FOIA, Inc.*, 65 DUKE L.J. 1361, 1405 (2016) (finding that thirty-four percent of FTC requests were from commercial entities).

254. *See, e.g.*, Lin, *supra* note 207, at 911.

255. *See, e.g.*, David Zaring, *Administration by Treasury*, 95 MINN. L. REV. 187, 208–10 (2010) (detailing the highly confidential nature of bank examinations).

rather than about the business owners' personal lives.[256] Early constitutional privacy protections of business records resulted from Fifth Amendment concerns about sole proprietors, and the Court declined to extend those protections to corporations.[257] The Court's Fourth Amendment jurisprudence leaves open the question of whether the collective entity should have privacy protections, but arguably "most corporations in most circumstances should not have a constitutional right to privacy."[258] Thus, to the extent the business owners are themselves users of the company's technologies, the business owners' personal privacy dovetails with the privacy of the platforms' users.

B. Users' Privacy

Privacy offers another increasingly important argument against monitoring: in collecting information from businesses, regulators may collect sensitive consumer data. As a starting point for the normative analysis, customers' privacy has not prevented regulatory monitoring of sensitive personal information in other industries. The SEC, CFPB, and FDA, not to mention the Census Bureau and Internal Revenue Service, collect a broad range of sensitive financial, medical, and household data.[259] However, platforms have a far greater quantity of personal data than businesses did when Congress extended monitoring authority in other industries. Commentators and the public now have a heightened concern about surveillance. Should these concerns change the analysis for platforms, or perhaps for regulatory monitoring more generally?

Surveillance is a general term that focuses on the collection of personal information.[260] It implicates regulatory monitoring in part because government agencies have often used platforms to surveil individuals—leading one commentator to depict the modern era as one of "liquid surveillance."[261] Technology firms have given the state

256. For more on the type of information collected, see *infra* Section IV.C.

257. *See* Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 841–44 (2005) (reviewing Fifth Amendment privacy origins).

258. Pollman, *supra* note 249, at 32.

259. Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205, 219–21 (2015) (surveying sensitive information collected by numerous government entities under force of law).

260. *See, e.g.*, LYON, *supra* note 18, at 14; Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1937 (2013).

261. *See* Balkin, *supra* note 187, at 2297 (2014) ("The technologies and associated institutions and practices that people rely on to communicate with each other are the same technologies and associated institutions and practices that governments employ for speech regulation and surveil-

visibility into people's associates and interests from social media behavior, spending habits from credit card statements, and a growing array of other details from smart-home device data.[262] Surveillance could thus pose a problem for regulatory monitoring because the very transfer of information from technology companies to the government is associated with an overbearing bureaucracy violating an important right.[263]

To weigh the real privacy risks of regulatory monitoring, it is instructive to draw two distinctions between regulatory monitoring and state surveillance. One distinction relates to the type of entity that is collecting the information. The other concerns the nature of the information collected.

1. Organizational Distinction: Crime Agencies Versus Regulators

From an entity perspective, business regulators should be analyzed separately from crime agencies. Conflating these two types of entities is problematic because they have different institutional cultures regarding information collection. Crime agencies have regularly exceeded the bounds of public comfort with information collection. To provide a few examples: in 1968, the Supreme Court held in a prominent case, *Katz v. United States*, that federal agents had violated the Fourth Amendment by wiretapping a public pay phone without obtaining a warrant, and the case garnered significant attention;[264] later, President Richard Nixon used federal law enforcement agencies to spy on political rivals and activist groups;[265] and more recently, former Central Intelligence Agency ("CIA") analyst Edward Snowden leaked classified documents revealing that the NSA had conducted a warrantless search of electronic communication

lance."); Richards, *supra* note 260, at 1940 ("It might seem curious to think of information gathering by private entities as 'surveillance' . . . [b]ut in a postmodern age of 'liquid surveillance,' the two phenomena are deeply intertwined.").

262. Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 588 (2017); Kim & Telman, *supra* note 25, at 725–26; Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1090–91 (2002). Palantir alone has helped the Central Intelligence Agency ("CIA"), FBI, NSA, and ICE detect drug distribution rings, profile people for airport searches, and identify criminal suspects. Sarah Brayne, *Big Data Surveillance: The Case of Policing*, 82 AM. SOC. REV. 977, 985, 993–95 (2017).

263. *See infra* Section IV.C.

264. 389 U.S. 347, 353 (1967).

265. Wylie Stecklow, *The Curious and Questionable History of FISA: From Richard Nixon and George W. Bush to Edward Snowden*, FED. LAW. Jul. 2016, at 59, http://www.fedbar.org/Image-Library/Sections-and-Divisions/Civil-Rights/The-Curious-and-Questionable-History-of-FISA.aspx [https://perma.cc/EBP4-WKXS].

databases that included metadata from almost every U.S. citizen.[266] Public anger at these and other programs has led to a "patchwork of limits from disparate sources" now regulating access to various personal data sources, such as social media postings and "digital records of an individual's movements."[267]

Whereas Congress has regularly constrained crime agency surveillance, it has repeatedly done the opposite with regulators, concluding that regulators underutilized the authority they already had.[268] For instance, the FDA already had the ability to inspect food manufacturers when, in 2010, an estimated 1,939 people became seriously ill from salmonella in peanut butter, ice cream, spinach, and other products.[269] Congress responded to the outcry with legislation stating that the FDA "shall increase the frequency of inspection of all facilities," and requiring at least one inspection every three years for high-risk manufacturers.[270] Similarly, federal authorities gained the power to inspect underground mines in 1941, but an explosion ten years later in Illinois that killed 119 miners prompted Congress to mandate

266. *See, e.g.*, Slobogin, *supra* note 14, at 107. That bulk collection had resulted from agencies' aggressive application of section 215 of the USA Patriot Act, which did not on its face appear to authorize such collection of Americans' telephone records. USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287–88 (codified as amended at 50 U.S.C. §§ 1861–62 (2012)). The legislation ended the NSA's bulk collection of Americans' phone call metadata. *See* 50 U.S.C. § 1861(b)–(c) (2012).

267. Berman, *supra* note 262, at 581–82; *see, e.g.*, 50 U.S.C. § 1861(b)–(c) (limiting bulk collection of data); Barry Friedman & Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281, 285 (2016) (referring to public anger). *Katz* prompted Congress later that year to pass the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 211–25 (1968) (codified as amended at 18 U.S.C. §§ 2510–2522 (2012)). *See* Nicholas J. Whilt, *The Foreign Intelligence Surveillance Act: Protecting the Civil Liberties That Make Defense of Our Nation Worthwhile*, 35 SW. U. L. REV. 361, 371 (2006) (mentioning the influence of *Katz* on legislation). Congress responded to President Nixon, and related concerns, with the Foreign Intelligence Surveillance Act of 1978 ("FISA") as the "exclusive means by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted." 18 U.S.C. § 2511(f) (2012); *see* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified in scattered sections of 50 U.S.C.); Stecklow, *supra* note 265, at 59 (describing FISA as a "Nixon Legacy," "born in the aftermath of unlawful behavior of the executive branch of government").

268. One notable exception to this is the Paperwork Reduction Act, but that applies to agencies beyond business regulators, including those engaged in national security, and restricts information collected from individuals as well as businesses. Some categories of business monitoring, such as inspections, are exempt, as are some categories of crime agency information collection, such as those in the midst of an investigation. 44 U.S.C. § 3518(c)(1)(A), (C) (2012) (exempting the collection of information for federal criminal investigations, prosecutions of particular criminal matters, and certain FTC civil processes).

269. Strauss, *supra* note 97.

270. Food Safety Modernization Act, Pub. L. No. 111-353, § 201, 124 Stat. 3885, 3923–24 (2011) (codified as amended at 21 U.S.C. § 350j(a) (2012)).

an annual inspection of each underground coal mine.[271] Congress has imposed similar minimum annual monitoring of oil and gas platforms,[272] underground mines,[273] large banks,[274] credit rating agencies,[275] and nuclear plants.[276] Notably, crime agency statutes do not contain such minimum surveillance stipulations.[277] In short, as public choice theory suggests, regulators tend to undercollect information.[278] As a result, policymakers considering regulatory monitoring should have less organizational concern about overzealous government officials violating individuals' privacy—including for any program involving regulatory monitoring of platforms.

What about the possibility that business regulators would hand over personal information to crime agencies? The distinction between crime agencies and business regulators would matter less if business regulators shared all of the personal information collected with crime agencies. Regulators do sometimes share information with other law enforcement agencies for prosecuting criminal matters related to their mission. For instance, the FTC's mission of protecting consumers implicates criminal fraud. When the agency identifies businesses engaging in fraud, it hands the matter over to the agency with the ability to prosecute criminal matters in court.[279] Statutes often dictate these links between regulators and crime agencies.

Beyond such mandated interagency sharing, the information transfer is limited by several factors. Most importantly, various statutes curtail how agencies can disclose information. The Privacy Act provides general limitations on an agency's ability to disclose individuals' records to other governmental agencies, except under enumerated exceptions.[280] The Act also limits access within the agency,

---

271. Alexa E. Welzien, *MSHA's Pattern of Violations Authority: Reviving an Untapped Resource of Enforcement Power*, 79 GEO. WASH. L. REV. 1613, 1617 (2011).

272. 43 U.S.C. § 1348(c) (2012).

273. Federal Mine Safety and Health Amendments Act of 1977, Pub. L. No. 95-164, 91 Stat. 1290 (requiring four annual inspections for all underground mines).

274. 12 U.S.C. § 1820(d)(1) (2012) ("The appropriate Federal banking agency shall, not less than once during each 12-month period, conduct a full-scope, on-site examination of each insured depository institution.").

275. Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 932(a)(8), 124 Stat. 1376–2223 (2011) (codified at 15 U.S.C. § 78o-7(p) (2012)).

276. Atomic Energy Act of 1946, Pub. L. No. 79-585, § 10(6)(c), 60 Stat. 755 (mandating varying inspection frequencies for nuclear plants).

277. For instance, the Stored Communications Act and the Foreign Intelligence Surveillance Act do not impose minimums. *See* 18 U.S.C. §§ 2702–03 (2012); 50 U.S.C. §§ 1801–11 (2012).

278. On public choice theory predicting that regulators would more plausibly have an anti-regulation tendency, see Bagley & Revesz, *supra* note 32, at 1262.

279. *See Criminal Liaison Unit*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/criminal-liaison-unit (last visited Sept. 22, 2019) [https://perma.cc/N8RH-KBFN].

280. 5 U.S.C. § 552a(b) (2012).

allowing access only to those "who have a need for the record in the performance of their duties."[281] Many industry-specific statutes go further, such as requiring disclosure to the individual whose medical records were requested or prohibiting any use of those records "for any purpose other than the litigation or proceeding for which such information was requested."[282] Some of these statutes make it a criminal offense for government officials to disclose information collected.

Two institutional factors further mitigate the concerns about handing over information. First, when regulators collect sensitive information, the monitoring group would be expected to establish firewalls. From an institutional perspective, agency divisions tend to be selective about what they share even when others in the same agency, such as enforcement attorneys, desire unfettered access.[283] Even when they are supposed to work together and coordinate to prevent disasters, agencies have resisted coordinating functions.[284] Since regulators' employees would risk themselves breaking the law by inappropriately sharing personal information, the sharing of personal information should be seen as having significant motivational barriers. These and other sources of "internal administrative law"[285] help to deter regulators from routinely passing information to crime agencies.

Finally, crime agencies do not need regulators' help to obtain access to extensive personal data. Through the maligned third-party doctrine, the Court has held that when people voluntarily share information with a third party, they usually have no reasonable

281. *Id.* § 552a(b)(1).

282. 45 C.F.R. § 164.512(e)(v)(A) (2018) (covering medical records under the Health Insurance Portability and Accountability Act); *see also* 20 U.S.C. § 1232g(b)(1)(J) (2012) (limiting access to education records).

283. *See* Jody Freeman & Jim Rossi, *Agency Coordination in Shared Regulatory Space*, 125 HARV. L. REV. 1131, 1148 (2012) (analyzing the balkanized nature of federal agencies and noting that "information sharing and coordination remain significant challenges to the effective operation of the fragmented regime"); Van Loo, *supra* note 2, at 397–98 (discussing how monitors guard nonpublic information closely, partly to encourage business cooperation).

284. *See* FIN. STABILITY BD. & INT'L MONETARY FUND, THE FINANCIAL CRISIS AND INFORMATION GAPS 18–20 (2009), https://www.imf.org/external/np/g20/pdf/102909.pdf [https://perma.cc/TK2Y-6PPP] (explaining how insufficient information sharing contributed to the financial crisis of 2008); David A. Hyman & William E. Kovacic, *Why Who Does What Matters: Governmental Design and Agency Performance*, 82 GEO. WASH. L. REV. 1446, 1455 (2014) (describing the ongoing "turf war" between the FBI and the CIA). Nonetheless, agencies pervasively coordinate functions, and sometimes share information informally. *See* Freeman & Rossi, *supra* note 283, at 1156.

285. Gillian E. Metzger & Kevin M. Stack, *Internal Administrative Law*, 115 MICH. L. REV. 1239 (2017).

expectation of privacy in such information.[286] Consequently, the Constitution provides minimal limits on crime agencies' access to user data from platforms even without a warrant.[287] The FBI, CIA, and other agencies have hired leading private-sector data brokers, such as Palantir, to amass and analyze large amounts of private data.[288] Therefore, regulatory monitoring implicates users' privacy less than does crime surveillance due to agency cultural differences, crime agencies' independent information access, and existing privacy laws that restrict regulators' ability to hand over information.

2. Information Distinction: Personal Versus Organizational

Those concerned about potential monitoring harms to users' privacy must also consider the type of information sought. One categorization is vital for monitoring in the digital era—whether the information collected is personal or organizational.[289] That distinction is important because popular alarm about surveillance stems from the collection of personal—not business—data.

There is no doubt that for some platform harms, data from user accounts would be vital. To determine whether an algorithm was discriminating improperly, for instance, the monitor would need some mechanism for at least inferring characteristics about users, such as race.[290] Again, it bears emphasis that federal agencies face considerable political and legal pressures to safeguard personal data. Although the

---

286. *See*, *e.g.*, Smith v. Maryland, 442 U.S. 735, 745–46 (1979). The Court recently weakened the doctrine in a case that excluded cell phone location data. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) ("In light of the deeply revealing nature of [cell-site location information], its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."). On the widespread criticism and debates surrounding the third-party doctrine, see, for example, Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1239 (2009).

287. *See, e.g.*, United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (citing voluntary sharing of information with Yahoo as grounds for allowing government use of such data); Slobogin, *supra* note 257, at 809 (discussing widespread government access to personal records using subpoenas).

288. *See* discussion *supra* note 262 and accompanying text.

289. Christopher Slobogin has emphasized the importance of this distinction between personal and business records in the context of government investigation of crimes. Slobogin, *supra* note 257, at 808–09.

290. On data being used for discrimination, and legal responses, see, for example, Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 719 (2016); Christopher K. Odinet, *The New Data of Student Debt*, 92 S. CALIF. L. REV. (forthcoming 2019) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3349478&download=yes [https://perma.cc/4MLG-VRD2]; Anya Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, IOWA L. REV. (forthcoming 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3347959&download=yes [https://perma.cc/Z2UB-ZMLJ]; Rory Van Loo, *The Corporation as Courthouse*, 33 YALE J. REG. 547, 579–80 (2016).

Fourth Amendment overall provides minimal restrictions on regulatory information collection, it would be more likely to restrain regulators collecting personal information than business information.[291] Various statutes have restricted government agencies above that floor. The Privacy Act, for example, imposes criminal penalties on government employees for improper use of personal data.[292] The Stored Communications Act restricts government access to emails.[293] And the Federal Information Security Modernization Act of 2014 requires annual independent information security evaluations of agencies, performed by the Inspector General.[294]

Accordingly, regulators take precautions in handling personal data, such as firewalls and encryption. Furthermore, for some harms requiring access to user accounts, it may be possible to provide the data to the regulator in de-identified form, such as by replacing the name with a randomly generated number. Government agencies, like private businesses, have at times failed in their efforts to protect privacy, and anonymization has limits.[295] But it is worth recognizing that de-identification can reduce the risks of regulatory analysis of some personal data when it is collected.[296]

Of course, government entities, like businesses, are vulnerable to hacks and leaks.[297] However, the legal constraints on agencies arguably go further than laws constraining private businesses, as the

---

291. As the Supreme Court explained in *Camara v. Municipal Court of San Francisco*, the "basic purpose of [the Fourth] Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." 387 U.S. 523, 528 (1967). Exactly what makes a search personal is undefined and "established by general social norms." Robbins v. California, 453 U.S. 420, 428 (1981).

292. 5 U.S.C. § 552a (2012).

293. 18 U.S.C. § 2702(a) (2012).

294. Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, § 2(a), 128 Stat. 3082 (2014) (to be codified at 44 U.S.C. § 3555(a)–(b)) (specifying that for agencies with an Inspector General, the Inspector General will lead the annual evaluation). Federal agencies must also conduct privacy impact assessments for information systems that use personally identifiable information. E-Government Act of 2002, 44 U.S.C. § 3501 (2012).

295. *See, e.g.*, Hans, *supra* note 15, at 2 ("Too much individual data is being collected, stored, and sometimes disclosed without anyone asking or answering some very important questions."). If implemented poorly, anonymized data can reveal too much. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1719 (2010); Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703 (2016).

296. The challenges can largely be determined in advance for a given data set, and for difficult-to-anonymize categories of data, there are solutions that still allow for robust monitoring. Ohm provides five factors to weigh in deciding whether data can be anonymized. *See* Ohm, *supra* note 295, at 1765–68.

297. On government data breaches, and related concerns about agency data collection, see, for example, Kimberly A. Houser & Debra Sanders, *The Use of Big Data Analytics by the IRS: Efficient Solutions or the End of Privacy as We Know It?*, 19 VAND. J. ENT. & TECH. L. 817, 866 (2017); Adam B. Thimmesch, *Tax Privacy?*, 90 TEMP. L. REV. 375, 389 (2018).

Privacy Act only applies to government entities. Thus, while precautions must be taken and the risks involved in collecting personal data obviously must be considered, in weighing those risks it is important to recognize that regulators already have a legal structure in place for handling personal information.

Additionally, unlike crime agencies—which need users' identities to assess their personal targets—regulators are looking for wrongdoing by the business.[298] Above all, regulators need business information, not personal information. They can analyze companies' internal policies and procedures, or even examine the code behind various algorithms, without obtaining any user data. In theory, they could ask the business to conduct a particular quantitative analysis about, say, the number of fee complaints that Facebook received using the word "child," without the regulator ever receiving any information about a particular user. In practice, regulators go to great lengths to minimize the collection of personally identifiable information, given their lesser need for it and the controversies surrounding it.[299]

Finally, it is worth noting that the normative analysis of privacy in the monitoring framework may be flipped for platforms. In most historical extensions of monitoring, whether in banking, the environment, or health, agencies received extensive monitoring authority despite privacy concerns weighing only against monitoring.[300] In contrast, today one of the main goals of any regulatory monitoring regime for platforms would presumably be to ensure those companies are respecting users' privacy.[301] Thus, even if the regulator collected personal information for that purpose, the privacy risks created by the regulator would need to be weighed against the privacy benefits of the additional regulatory oversight. However, since regulators could audit a platform's privacy systems without collecting personal data, the

298. Regulators are enforcing mostly civil laws against businesses, meaning that tracing users to conduct is largely irrelevant. This is particularly true for transactional and privacy-related harms. *See supra* Section II.A. Speech harms, as mentioned above, provide a weaker case for monitoring than other categories, but even those harms could be monitored without collecting identifiable data, as the goal would be to categorize blocked speech, which could be determined by examining the platforms' internal rules alone. If the regulator wanted particular examples, it could ask for the user conduct or words that led to ostracizing a given user, without obtaining the user's identity. *See supra* Section II.A.4. Speech harms and election engineering would, however, come closer to implicating criminal wrongs, and thus any program would need to weigh the value of identifying wrongdoers and the threats to privacy in the collection of such information. If the communications were already publicly available on a social media platform, there would be fewer privacy concerns.

299. *Infra* Section IV.C (summarizing political pressures on regulators regarding personal information).

300. *See supra* Section I.C.1.

301. *See supra* Section II.A.1.

privacy analysis should overall weigh *more* in favor of regulatory monitoring in the surveillance age than it did in prior eras.

To be clear, agency officials could potentially misuse regulatory information acquired about businesses and individuals—or an unscrupulous executive could seek to leverage it to persecute political opponents. Those issues are, however, more about design of the regulatory monitoring—and indeed about appropriate constraints on government power—than about whether to extend the authority in the first place.[302] Legal and organizational safeguards are crucial for any regulatory monitoring program. The main point here is that avoiding regulatory monitoring of platforms altogether due to anxiety about individual privacy would be inconsistent with a broader perspective on regulatory monitoring, privacy, and the administrative state.

C. Regulatory Burden

How should the costs of compliance be weighed in the case of platforms? There is little that can be said with certainty about the monetary costs of monitoring platforms because no such program exists. Three potential sources of burden lie in stifling innovation, increasing the costs that the platform incurs in providing information to the regulator, and spending public resources collecting and processing the information.

One possibility is that monitoring could chill innovation by making the innovator nervous about trying something new, out of fear of being punished for the unknown. Or monitoring could deter new entrants because of the costs of complying with heavy oversight, thereby deterring the entrance of new ideas.[303] While it may be true that "[w]e couldn't kill the Internet if we tried,"[304] the issue is largely theoretical because the interplay between regulation and innovation is poorly understood as an empirical matter.[305] Also, the potential for stifling innovation is a broader point about regulating business in general, as a similar concern could be raised about other enforcement

---

302. Although I return to the question of designing monitoring programs in Section IV.C, *infra*, that topic is sufficiently capacious to require a separate project.

303. *See, e.g.*, David McGowan, *Innovation, Uncertainty, and Stability in Antitrust Law*, 16 BERKELEY TECH. L.J. 729, 765–70 (2001).

304. Paul Ohm, *We Couldn't Kill the Internet If We Tried*, 130 HARV. L. REV. FORUM 79, 85 (2016). Another possibility is a chilling effect in which users do not want to provide their data to firms out of fear that the government will attain it. *See* Niva Elkin-Koren & Michal Gal, *The Chilling Effect of Governance-By-Data on Data Markets*, 86 U. CHI. L. REV. 403, 407 (2019).

305. Keith N. Hylton, *A Unified Framework for Competition Policy and Innovation Policy*, 22 TEX. INTELL. PROP. L.J. 163, 164 (2014) (discussing how competition policy often omits innovation considerations).

mechanisms, such as ex post litigation. Society has so far rejected suppression of innovation as an argument against regulation, given the prevalence of regulation in the economy, but the narrative may hold greater weight for platforms, given the industry's entrepreneurial ethos.[306]

A more tangible cost is the expenditure of resources to transfer information.[307] Those costs could be substantial and should be factored in to any proposed oversight regime. In undertaking such a prospective analysis, it would be valuable to leverage the empirical studies of the costs of monitoring in other industries. The challenge with doing that, however, is that overall compliance costs are driven by the extent of the substantive regulation in addition to the costs of monitoring. Since far fewer substantive laws govern platforms than, say, banks, platforms would presumably have less information to transfer—and thus a lower monitoring burden.[308]

For the estimates to be comprehensive, they should include the potential savings that studies have found from governmental monitoring. These savings include benefits to shareholders, who may not be able to sufficiently monitor the risks taken by a firm's managers, as well as the avoidance of compliance costs that the firm would have otherwise undertaken.[309] Counterintuitively, since platforms already spend a considerable amount of money on data security, it is possible that a centralized regulator providing monitoring services across an entire industry could reduce some platform costs by providing economies of scale—or add shareholder value by providing more reliable monitoring of risks.[310]

Platforms might even interface with monitors more efficiently than have businesses in other industries. Monitoring is, after all, about transferring information. One of platforms' core specialties is collecting and transferring information in a highly automated manner. Thus, platforms' monitoring burden may be significantly less than for companies whose core operations are far from information technology.

---

306. *See, e.g.*, Cass R. Sunstein, *Interpreting Statutes in the Regulatory State*, 103 HARV. L. REV. 405, 409 (1989) (discussing the expanding role of regulation since the new deal).

307. *See, e.g.*, J.B. Ruhl & James Salzman, *Mozart and the Red Queen: The Problem of Regulatory Accretion in the Administrative State*, 91 GEO. L.J. 757, 799–800 (2003).

308. The amount of information that would need to be transferred per law is also relevant to this equation.

309. *See, e.g.*, Emilio Bisetti, The Value of Regulators as Monitors: Evidence from Banking (June 12, 2019) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3081537 [https://perma.cc/67Z9-WQ3J] (finding that reduction of Federal Reserve monitoring of banks increased firms' internal compliance costs and lowered shareholder value).

310. The gains to shareholders would need to be weighed against any value destroyed by monitoring.

D. Summary of Factors for Monitoring Online Platforms

Among the four types of public interest discussed—privacy, civic engagement, transactional integrity, and speech—the strength of the case for monitoring varies. The case for monitoring speech harms, for instance, is weaker than for monitoring election engineering.[311] Nonetheless, the main normative historical drivers of monitoring are largely present in online platforms: harms worth preventing, insufficient public information, and a track record of failed self-regulation.

The factors that might weigh against monitoring platforms are, if anything, potentially weaker than in other monitored industries. Platforms can transfer information to regulators at a lower cost, since data is their core product. While the issue of privacy has certainly become more complex in the digital era due to users' privacy interests, at the very least, concerns about users' privacy should not prevent regulators from collecting *only* business information, rather than personal information. For most types of harm, an informative monitoring program is possible without a regulator ever collecting personal data and instead focusing on information about the platform and its processes.

However, where personal data collection is necessary to protect users, there are precedents in other industries for legally and organizationally constraining agencies that collect highly sensitive information. Ultimately, citing personal data as a reason against regulatory monitoring of platforms would be a red herring. Rather, privacy arguably strengthens the case for monitoring platforms since large business owners' privacy interests are minimally affected. Moreover, those minimal interests must be balanced against the privacy interests of millions of platform users in having regulatory oversight of how platforms use their data.

Legitimate privacy concerns, as well as the need to protect trade secrets and minimize regulatory burden, underscore how any monitoring regime should be designed—with appropriate accountability and burden-minimizing processes in place. Those details would need to be worked out in a way that is sensitive to the specific platform and harm. The main point here is that if policymakers were to weigh the principal factors as they have in oil, pharmaceuticals, food

311. Nonetheless, compared to the alternative of leaving it entirely to platforms, there is still a normative and historical case for monitoring content moderation. *See supra* Kyle Langvardt, *Regulating Online Content Moderation*, 106 GEO. L.J. 1353, 1353 (2018); Section II.A.4.

safety, and most other major industries, they would find normative foundations for monitoring platforms.

IV. IMPLICATIONS FOR REGULATORY MONITORING

The case study of platforms most immediately suggests that policymakers should consider building new monitoring programs for the increasingly digital economy. It also shows how the information collection framework developed in a pre-digital era is in need of refinement. Most importantly, in the surveillance age, policymakers must balance a more complex set of privacy interests.

A. FTC Monitoring of Platforms

What steps would be necessary for regulatory monitoring of platforms? No single agency would have jurisdiction over all of the categories of public interest discussed above, but the FTC has authority to enforce two of them: privacy and transactional harms.[312] Yet the agency currently operates on a largely ex post model that has failed in the past to assess whether online platforms are taking necessary steps to safeguard user data.[313] Their antitrust enforcement processes also allow platforms to establish themselves during critical periods of competition, after which it would likely be impractical to undo the harm.[314] While legislation and other agencies may be necessary for monitoring other types of platform harm such as election engineering and speech moderation, this Section examines the FTC's relatively straightforward path to monitoring the surveillance economy.

Because the FTC has generally not engaged in monitoring except in narrow contexts where explicitly required by statute, its legal authority to develop a monitoring regime of platforms is in many regards unsettled. But under section 6(a) of its originating statute, the agency has the power "[t]o gather and compile information concerning, and to investigate from time to time the organization, business,

312. *See* Federal Trade Commission Act of 1914, 15 U.S.C. § 45 (2012); Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801, 6805 (2012). On the FTC's privacy enforcement, see, for example, Chris Jay Hoofnagle, *FTC Regulation of Cybersecurity and Surveillance*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 708, 708, 722–23 (David Gray & Stephen Henderson eds., 2017) (observing also that "regulation of the private-sector has effects on the government as surveillant"); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585 (2014).

313. *See supra* notes 223–225 and accompanying text.

314. *Cf.* Chris Jay Hoofnagle, *The Federal Trade Commission's Inner Privacy Struggle*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 179 (Evan Selinger et al.) (2018) ("The delay involved in FTC processes gives respondents time to establish their platform and shut out competitors.").

conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce."[315] It also has the authority to require regular submission of reports, which it used in 1975 to request cost and sales data from 450 of the largest U.S. manufacturing firms.[316] Cost and sales data is particularly sensitive and closely guarded information, which explains why about 180 of the companies filed motions to quash.[317] In upholding the program, the U.S. Court of Appeals for the D.C. Circuit noted that the FTC's statute "provides a clear basis of authority for the Commission to issue orders requiring corporations to submit informational reports to the FTC."[318] Subsequent legislative reforms to the FTC's authority have preserved its main monitoring tools.[319]

In 1980, Congress passed the Paperwork Reduction Act ("PRA"), which requires Office of Management and Budget ("OMB") approval for certain information collection activities.[320] But OMB approval is only required for information collection from ten or more entities, meaning that the FTC could at least collect information from the most important nine platforms or through one-off requests.[321] Moreover, as an independent agency, the FTC has the statutory option of overruling any OMB rejection.[322] For these and other reasons, the Act is more of a legal barrier to the type of industry-wide information collection used in rulemaking—but has not generally prevented regulatory monitoring.[323] Indeed, the FTC even recently used 6(b) authority to collect sensitive

---

315. FTC Act, Pub. L. No. 63-203, § 6(a), 38 Stat. 717 (1914) (codified at 15 U.S.C. § 46(a) (2012)).

316. Appeal of FTC Line of Bus. Report Litig., 595 F.2d 685, 690 (D.C. Cir. 1978) (per curium).

317. *Id.* at 692.

318. *Id.* at 693. This observation arose even though no parties questioned the FTC's authority. *Id.* The court also noted that the FTC's order was "clearly investigatory in nature." *Id.* at 696.

319. The FTC Improvements Act of 1980 directed the agency to use civil investigative demands ("CID"s) instead of subpoenas for investigating unfair and deceptive acts, though not for competition. Federal Trade Commission Improvements Act of 1980, Pub. L. No. 96-252, 94 Stat. 374 (1980) (codified at 15 U.S.C. § 57b-1 (2012)). The CID is broader in scope, but the tools are functionally the same and separate from the regular report collection function. *See A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMM'N (Apr. 2019), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/WK5A-87J6].

320. Pub L. No. 96-511, 94 Stat. 2812 (1980) (codified at 44 U.S.C. §§ 3501–3521 (2012)).

321. 5 C.F.R. § 1320.3(c)(4) (2018).

322. 44 U.S.C. §§ 3502(5), 3507(f) (2012). Of course, that move by the FTC may be politically untenable. The full extent of independence from review by the Office of Information and Regulatory Affairs ("OIRA") is debated and evolving. *See* Nina A. Mendelson & Jonathan B. Wiener, *Responding to Agency Avoidance of OIRA*, 37 HARV. J.L. & PUB. POL'Y 447, 506–07 (2014).

323. *See* 44 U.S.C. § 3502(5) (2012) (listing independent agencies covered by the Act, such as banking regulators, the Federal Communications Commission, and the Occupational Safety and Health Review Commission); Van Loo, *supra* note 2, at 408–12 (describing monitoring by same agencies).

information from large companies for a one-off study, after satisfying the PRA requirements.[324]

Consider, also, how FTC monitoring might be viewed in the context of the surveillance state. The Drug Enforcement Administration ("DEA") has surveilled individuals extensively despite an originating statute granting only the ability to "investigate" suspects.[325] The FBI has conducted far-reaching personal surveillance with an enabling statute that mentions only the authority to "detect" crimes.[326] The FTC's explicit authorizations to "gather and compile" and "investigate from time to time" more clearly indicate monitoring authority than do the originating statutes of the DEA and FBI. Viewed against the backdrop of expansive DEA and FBI surveillance under vaguer originating authorities, the FTC's ability to build a monitoring program is even stronger—particularly since it would be collecting information from businesses, rather than individuals.[327]

Supreme Court decisions provide further support for FTC monitoring authority. The Court has concluded that the FTC's organic statute provides "ample power" to require reports, as well as to send investigators to examine a company's books.[328] More broadly, regulatory requests for business records do not require a warrant, or even allegations of a particular violation, as long as the requests are not unreasonable and relate to "general or statistical investigations."[329] Thus, the FTC's enabling statute and direct case history, along with courts' treatment of other regulators and crime agencies, indicate that the commissioners can construct a vigorous platform-monitoring program if they so choose.

Monitoring requires personnel, so the FTC would need to either obtain new allocations or reassign existing employees. Limited

---

324. FED. TRADE COMM'N, PATENT ASSERTION ENTITY ACTIVITY 37–38 (2016), https://www.ftc.gov/system/files/documents/reports/patent-assertion-entity-activity-ftc-study/p131203_patent_assertion_entity_activity_an_ftc_study_0.pdf [https://perma.cc/F7S3-8LZT] (compelling companies, after meeting PRA requirements and using 6(b) authority, to provide nonpublic information to study patent competition).

325. *See* Reorganization Plan No. 2 of 1973, Pub. L. No. 93-253, 88 Stat. 50 (1974) (codified at 5 U.S.C. app. § 1 (2012)).

326. *See* 28 U.S.C. §§ 531, 533 (2012). The FBI has not sought to justify its surveillance under this detection clause and has instead looked to the unconvincing residual authority of the All Writs Act—which is also available to the FTC. *See* Judiciary Act of 1789, ch. 20, § 14, 1 Stat. 73, 81–82 (codified as amended at 28 U.S.C. § 1651 (2012)); Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 126 (2018) (noting frequent use by FBI).

327. *See supra* Section III.B.2.

328. United States v. Morton Salt Co., 338 U.S. 632, 649 (1950).

329. Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 208–09 (1946); *see also* McLane Co. v. EEOC, 137 S. Ct. 1159 (2017) (noting that the EEOC should be given access to any material that *might* be relevant to the investigation).

resources undermine detection.[330] Nonetheless, the agency's current workforce could support a meaningful level of monitoring. The CFPB runs a substantial monitoring apparatus with over 400 examiners, compared to about 350 attorneys.[331] The FTC has an insignificant number of monitors and over 700 attorneys.[332] Platforms would require fewer monitors than financial institutions, because the latter are some of the most heavily regulated businesses, requiring the CFPB to monitor over one hundred large banks, thousands of payday lenders, and many other categories of financial institutions for compliance with dense laws.[333] Devoting even one hundred FTC employees to monitoring would allow meaningful examinations, especially if focused on the ten largest platforms.[334] At the very least, the FTC's leaders should actively decide whether it is worth diverting resources from their other activities to monitoring platforms, rather than assume no other option exists. The FTC's recent move to create a twenty-person task force to "monitor" platforms for antitrust violations demonstrates the plausibility of such resource reallocations.[335] However, for the FTC to develop a monitoring program more in line with that of most other large regulators, the agency would need to devote more resources; expand its monitoring to cover other areas of its mission, such as privacy and consumer protection more broadly; and make it a routine practice to compel businesses to produce information rather than doing so only in a more ex post manner once a particular issue has clearly become a problem.

What the FTC would do with such information is not the subject of this Article. Still, despite more limited civil penalty and rulemaking authority than some other agencies,[336] the FTC has wide-ranging consumer protection and antitrust authority designed to evolve with markets.[337] It would be able to take significant action to address some of the privacy and transactional harms discussed above.

---

330. *See, e.g.*, Hoofnagle, *supra* note 314, at 170.

331. Van Loo, *supra* note 2, at App. A.

332. *Id.*

333. *See, e.g.*, Rory Van Loo, *Making Innovation More Competitive: The Case of Fintech*, 65 UCLA L. REV. 232, 237, 271–75 (2018) (summarizing the CFPB's authority).

334. Moving employees to monitoring would require a cost-benefit analysis of the relative importance of those employees' other tasks. Given the prominence of platforms in the modern economy, the harms presented by platforms should compare well.

335. *See* sources cited *supra* note 37 and accompanying text.

336. During a deregulatory period of the 1980s, Congress curtailed the agency's ability to impose civil penalties and write rules, making the FTC in this regard weaker than, say, the CFPB. Federal Trade Commission Improvements Act of 1980, Pub. L. No. 96-252, 94 Stat. 374 (codified at 15 U.S.C. § 57b-1 (2012)).

337. Its mandate to regulate unfair and deceptive acts is purposefully broad, designed to change on an "evolutionary basis" alongside markets. Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 982 (D.C. Cir. 1985). Additionally, the prospect of a federal regulator bringing public lawsuits,

However, a monitoring program need not involve aggressive prosecutions. Ex post legal investigations typically result in a formal enforcement action after major wrongdoing has occurred. In contrast, monitoring fits well with the modern emphasis on collaborative governance—that is, working with firms to solve problems rather than adopting a punitive approach at the first signs of wrongdoing.[338] By identifying issues early on before they have become systemic, the FTC would be better situated to steer firms away from problematic practices before major liabilities materialize.

Nor does a monitoring regime need to involve extensive information collection. As explained above, the FTC could still learn a great deal without analyzing source code or collecting large troves of detailed information. The FTC could, for example, examine whether companies have appropriate privacy practices by requesting existing internal summary reports and explanations from employees.[339] After the FTC initially learned more about how a given platform operated, and as substantive platform regulations developed, it would have a better sense of what types of questions to ask to identify ways that the platform could avoid causing harm.

In some instances, existing internal reports and insights would not exist, in which case the FTC or Congress would need to take additional steps, such as imposing "audit trails" on platforms to ensure they record the reasoning and facts related to their decisions.[340] Other tools, such as ordering companies to conduct technical systems tests, may be needed.[341] Private third-party monitors could also complement FTC monitoring—although the FTC has less ability to impose private monitoring industry wide than it does to exercise its own authority to collect information.[342] Finally, it would be valuable to determine what types of information are necessary to achieve particular goals and the

---

even if those actions would have limited monetary impact, would hold some sway in motivating a large platform to comply with requests.

338. *See* Van Loo, *supra* note 2, at 397–98.

339. *See supra* Section II.C.

340. *See* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1305 (2008) (discussing audit trails for government entities' automated decisions); Crawford & Schultz, *supra* note 12, at 121–24 (applying Citron's proposal to the private sector).

341. *See* Hoofnagle, *supra* note 191, at 7.

342. The FTC currently deploys third-party private monitoring through settlement agreements and for limited periods of time, which is different from the kind of ongoing monitoring discussed here. *See supra* Section II.C. There may be efficiency advantages to some forms of private monitoring. *Cf.* Emily S. Bremer, *Private Complements to Public Governance*, 81 MO. L. REV. 1115, 1117 (2016) (discussing the institutional tradeoffs between private and public governance). Another issue is whether the FTC's ability to collect information from time to time covers on-site examinations of platforms. Assuming that it does not, a remote monitoring program would also help the agency determine whether to request such authority.

extent to which personal, rather than purely business, information is needed to determine compliance with a given law.[343] These and many other platform governance features have been explored elsewhere.[344]

The necessity of working out further details about the shape and scope of FTC monitoring, and political pressures weighing against FTC assertiveness,[345] should not obscure a more fundamental point. There is a strong basis for concluding that the FTC already has the mandate, without new legislation, to build a substantial monitoring program. Used as a complement to other tools, such as ex post litigation and consumer complaints, monitoring could contribute to a more robust oversight architecture for the most surprisingly unregulated entities in the information age.

B. The FCC, EEOC, and State Regulators

Most of this Article has focused on online platforms, a regulatory sphere most relevant to the FTC. But a variety of other companies can leverage technologies to engage in "digital market manipulation."[346] The monitoring framework, and its emerging tension with surveillance, thus implicates other regulators.

First, the FCC has extensive unused monitoring authority over cable and telecommunications firms.[347] Comcast, Verizon, AT&T, and similar companies arguably have greater ability to surveil than does Facebook, because they can access all transferred data.[348] Cable and telecommunication companies can also sell that data to third parties, thus cashing in on the incredible revenues from "big data, the new oil."[349] A policy norm that prioritizes individuals' privacy over that of

343. *See* discussion *supra* note 289 and accompanying text.

344. *See* sources cited *supra* note 12; *see also* Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 18 (2017); Tutt, *supra* note 121.

345. Congress has previously reduced the agency's powers and funding in response to a period of vigorous FTC enforcement. *See, e.g.*, Hans, *supra* note 228, at 168. Those dynamics may make its leaders hesitant to use their full remaining authority.

346. Calo, *supra* note 198, at 999; *see also* Shaun B. Spencer, *The Problem of Online Manipulation*, U. ILL. L. REV. (forthcoming 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3341653&download=yes [https://perma.cc/N438-YAJU].

347. *See* Van Loo, *supra* note 2, at 387 n.111 (explaining the FCC's originating authority).

348. Salome Viljoen, *Facebook's Surveillance is Nothing Compared with Comcast, AT&T and Verizon*, GUARDIAN (Apr. 6, 2018), https://www.theguardian.com/commentisfree/2018/apr/06/delete-facebook-live-us-still-share-data [https://perma.cc/R8PY-DSQS]. Thanks to recent legislative reforms, internet providers have great freedom to collect, analyze, and share essentially all of the browsing data that flows through them. S.J. Res. 34, 115th Cong. (2017) (enacted).

349. *See, e.g.*, Hirsch, *supra* note 122, at 374.

businesses would lend support to the FCC monitoring how these firms handle such massive data access.

Additionally, the EEOC provides an example of an agency operating beyond the technology sector. Its originating statute, the 1964 Civil Rights Act, granted the authority to systematically collect salary data from employers about pay to identify racial, gender, or other discriminatory pay practices.[350] But the EEOC did not write rules to collect such data systematically until 2012.[351] Moreover, although the agency now collects considerable data in a routine manner from large companies nationwide, it devotes only a handful of employees to analyzing such data, relying primarily on employee complaints to open over ninety-nine percent of investigations.[352] Granted, analyzing systematic employment data raises difficult questions about causality and poses the risk of false accusations.[353] But given that the agency now collects large amounts of data, many of the costs to privacy and compliance have already been overcome. In light of the difficulty one employee may have in ascertaining pay differences, discriminatory pay seems to be an area in need of rigorous cost-benefit analysis to determine whether it merits greater use of regulatory monitoring.

Finally, state and local regulators also undertake considerable monitoring. City inspectors grade restaurants, and county authorities oversee cable companies.[354] State and local regulatory monitors have limits because multinational companies' wrongdoing, particularly when data is involved, typically transcends local government borders. Also, courts consistently allow federal crime agencies to access state regulatory information.[355] Still, in some instances it may make sense for local regulatory authorities to monitor business activities, especially in the absence of action by federal regulators. Indeed, it was a local agency that initiated action in some of the biggest corporate prosecutions in recent years, such as the Los Angeles city lawsuit against Wells Fargo for creating fake accounts in customers' names.[356]

---

350. Civil Rights Act of 1964, Pub. L. No. 88-352, § 709, 78 Stat. 241, 262–64.

351. 29 C.F.R. § 1602.7 (2018).

352. U.S. EQUAL EMP'T. OPPORTUNITY COMM'N, FISCAL YEAR 2016 PERFORMANCE AND ACCOUNTABILITY REPORT 93 (2016), https://www.cbp.gov/sites/default/files/assets/documents/2017-Mar/FY-2016-CBP-PAR-508C.pdf [https://perma.cc/7NUM-SRP7].

353. For a discussion of the problem of big-data-driven disparate impact, and different ways to address the problem, see Barocas & Selbst, *supra* note 290, at 719; see also Pauline T. Kim, *Auditing Algorithms for Discrimination*, 166 U. PA. L. REV. ONLINE 189, 194 (2017).

354. *See, e.g.*, Ho, *supra* note 13, at 607–08.

355. *See* Mikos, *supra* note 18, at 105, 152 (showing that courts allow federal agencies to access state regulatory information, albeit with Fifth Amendment and other limitations).

356. *See, e.g.*, James Rufus Koren. *Why L.A. City Atty. Mike Feuer Knew the Wells Fargo Scandal Was Going to Blow Up*, L.A. TIMES, Sept. 28, 2016, at B1.

And though the FTC has not audited Airbnb for racial discrimination by hosts, the state of California Department of Fair Employment and Housing has used its legal authority to conduct tests.[357]

It is difficult to know, from the outside, why any particular agency leader may have opted not to monitor—or whether that possibility was even considered. But regulators' historical track record gives little confidence that repeated decisions to refrain from monitoring were made on the merits, and instead indicates that those decisions may be explained by industry capture or institutional inertia.[358] Ideally, legislators and agency leaders would take a fresh look at whether they should exercise regulatory monitoring—their primary means for understanding businesses—wherever that tool currently lies dormant.

C. Moving Monitoring Out of the Shadow of Surveillance

Whether the goal is to build a new technology meta-agency that monitors platforms, to require Facebook and Twitter to submit real-time election advertising reports to the Federal Election Commission, or for the FTC commissioners to use the authority they already have, policymakers must undertake a normative and legal analysis about the appropriate exercise of administrative information collection. That inquiry is more difficult because regulatory monitoring is, as a matter of law and popular imagination, part of the surveillance state.

In a world in which "everything has software,"[359] large portions of the regulatory state that collect information from businesses could now be incorrectly seen as engaging in personal surveillance. Part of the problem is the pervasive monolithic portrayal of government information collection. Scholars and judges often describe both business regulators and crime agencies as being engaged in surveillance.[360] The challenge with a close association between the two is that observers, including Supreme Court Justices, frequently reference an Orwellian *1984* dystopia in their discussions of crime data surveillance.[361] Indeed,

---

357. Voluntary Agreement at 16–17, Dep't of Fair Emp. and Hous. of Calif. v. Airbnb, Inc., Nos. 574743-231889, 574743-231624, (Apr. 19, 2017), https://www.dfeh.ca.gov/wp-content/uploads/sites/32/2017/06/04-19-17-Airbnb-DFEH-Agreement-Signed-DFEH-1-1.pdf [https://perma.cc/46UY-F4VP] (outlining terms of testing).

358. *See supra* Section III.B.1.

359. Paul Ohm & Blake Reid, *Regulating Software When Everything Has Software*, 84 GEO. WASH. L. REV. 1672, 1688–89 (2016).

360. *See* sources cited *supra* note 21 and accompanying text.

361. *See, e.g.*, Margaret Hu, *Orwell's* 1984 *and a Fourth Amendment Cybersurveillance Non-intrusion Test*, 92 WASH. L. REV. 1819, 1832–33, 1870 (2017) (surveying frequent judicial and scholarly references to Orwell's *1984*); *see also* Richards, *supra* note 260, at 1934 ("From the Fourth

concerns about a totalitarian state pervade broader advocacy for privacy.[362] Nor is the association with totalitarianism limited to crime agencies—television commercials, op-eds, and social media depict regulators such as the FTC, CFPB, and EEOC as "Big Brother."[363]

These pervasive references to a single state scrutinizing our lives likely carry weight with the public. Apple CEO Tim Cook even appealed to such suspicions when the FBI attempted to gain access to terrorism suspects' phones following the shooting deaths of fourteen people at a San Bernardino, California work party in 2016.[364] In an open letter, Cook warned that the FBI's demands would "undermine the very freedoms and liberty our government is meant to protect."[365] Cook went on to state the implications of granting the FBI's request:

> The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge.[366]

Note that Cook's message uses the singular term, "the government," but mentions health records and financial data—information collected by business regulators—alongside video and sound recordings of personal space, which are more relevant to crime agencies.[367]

It is also noteworthy that terrorist attacks are one of the strongest justifications for surveillance.[368] The CEO of a major consumer company would appeal to consumers' anxiety about privacy to ward off a government agency obtaining information about terrorist activities only if he—based, presumably, on the considerable research

---

Amendment to George Orwell's *Nineteen Eighty-Four* . . . our law and culture are full of warnings about state scrutiny of our lives.").

362. Whitman, *supra* note 15, at 1153 ("It is the rare privacy advocate who resists citing Orwell when describing these dangers.").

363. *See, e.g.*, Camille Olson, *Big Brother Is Still Watching—and It Doesn't Know Why*, HILL (Sept. 28, 2016, 11:30 AM), http://thehill.com/blogs/congress-blog/labor/298203-big-brother-is-still-watching-and-it-doesnt-know-why [https://perma.cc/PAE5-HS47] (critiquing the EEOC's salary-data collection while making the observation that "Big Brother is still watching"); Rachel Witkowski & Rob Blackwell, *Why that Orwellian Anti-CFPB Ad Could Backfire*, AM. BANKER (Nov. 10, 2015, 8:45 PM), https://www.americanbanker.com/news/why-that-orwellian-anti-cfpb-ad-could-backfire [https://perma.cc/84EQ-DC3N]; discussion *infra* notes 374–375 and accompanying text (comparing the FTC to Big Brother). Private entities are sometimes included in these metaphors, which have expanded to portray myriad Little Brothers. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1397 (2001).

364. *See* Rozenshtein, *supra* note 326, at 102–03.

365. Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), https://www.apple.com/customer-letter [https://perma.cc/239E-XF2N].

366. *Id.*

367. *See supra* notes 189–206 and accompanying text.

368. *Cf.* Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 729–30, 732 (S.D.N.Y. 2013) ("After the September 11th attacks, Congress expanded the Government's authority to obtain additional records.").

insights available to him about customers—believed that such rhetoric persuades a substantial portion of the public. Indeed, despite those salient government interests in obtaining access to suspected terrorists' phones, about forty-five percent of people supported Apple's refusal to help the FBI.[369]

It is difficult to know the impact of these blurred lines on regulatory monitoring policy. But the muddling of the concept of state surveillance may enable political actors with a deregulatory agenda to leverage privacy concerns on a broader basis. For instance, when Mick Mulvaney became the interim director of the CFPB in 2017, one of his first moves was to freeze a significant amount of information collection out of concerns that the CFPB could endanger consumers' privacy.[370] The effect of the data collection freeze was to significantly hinder the agency's core regulatory activities.[371]

To be clear, Mulvaney may have been responding to the legitimate privacy concerns that exist whenever an agency collects personal information, and did reinstate some information collection processes after the Inspector General found that the CFPB had not endangered consumers' privacy.[372] But Mulvaney was a strong opponent of the CFPB. He had previously called the agency a "sick, sad" joke, had introduced legislation to terminate the CFPB in his previous role as a congressman, and, even after being appointed interim director, continued to reiterate that the agency should not exist.[373] Regardless of Mulvaney's motives in freezing data collection, the incident highlights the potential tension between regulation and privacy.

Additional signs suggest regulators are wary that monitoring will make them vulnerable to being publicly associated with surveillance. For instance, in 2009 the FTC called for online endorsers

---

369. *CBS News Poll: Americans Split on Unlocking San Bernardino Shooter's iPhone*, CBS NEWS (Mar. 18, 2016, 8:24 PM), https://www.cbsnews.com/news/cbs-news-poll-americans-split-on-unlocking-san-bernardino-shooters-iphone [https://perma.cc/77VS-3ZLJ].

370. John Heltman, *Warren Grills CFPB Head Over Data Collection Freeze*, AM. BANKER, (Jan. 8, 2018, 3:09 PM), https://www.americanbanker.com/news/warren-grills-cfpb-head-over-data-collection-freeze [https://perma.cc/D8EP-TQZ2].

371. *Id.*

372. OFFICE OF INSPECTOR GEN., 2018 AUDIT OF THE BUREAU'S INFORMATION SECURITY PROGRAM 1 (2018), https://oig.federalreserve.gov/reports/bureau-information-security-program-oct2018.pdf [https://perma.cc/E57W-24GU].

373. *See* David A. Hyman & William E. Kovacic, *Implementing Privacy Policy: Who Should Do What?*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1117, 1140 (2019); Kelsey Ramirez, *CFPB Acting Director Mulvaney Says He Still Believes Bureau Shouldn't Exist*, HOUSINGWIRE (Apr. 11, 2018), https://www.housingwire.com/articles/43077-cfpb-acting-director-mulvaney-says-he-still-believes-bureau-shouldnt-exist [https://perma.cc/V7RS-EJ9J].

of products to disclose any gifts or payments they received.[374] Following online commentaries comparing the agency to Big Brother, an FTC official issued a statement saying, "We are not going to be patrolling the blogosphere."[375] Given that public perception has historically played an important role in driving Congress to authorize monitoring,[376] a core enforcement activity could face additional obstacles in the surveillance era.

Greater clarity in discussing and analyzing regulatory monitoring is thus important for regulating businesses in the surveillance era. This Article has highlighted, at a top level, two main sources of confusion. The first is the question about which agency is acting, with the most important challenge being the conflation of crime and regulatory agencies. The second is the type of information sought, especially whether it is business or personal.[377] These distinctions complement existing efforts to move toward more accountable and transparent algorithms.[378]

A few further preliminary observations on this basic taxonomy and its application are in order. One of its main functions is to facilitate a more refined normative analysis. Each type of information collection would still be weighed in terms of the traditional normative factors, such as information asymmetries.[379] Within that analysis, however, the regular collection of business information, without any personal data, would face a lower privacy barrier than would the other categories.

It bears emphasis that neither a taxonomy nor a normative framework for exercising information collection should hew too closely to Fourth Amendment jurisprudence. To be sure, a real-world state privacy hierarchy would ideally reflect the constitutional prioritization of personal over business privacy.[380] But the Fourth Amendment allows agencies to subpoena even sensitive personal records, such as bank

374. *FTC Reassures Bloggers—Big Brother Isn't Watching*, BLOG LEGALTIMES (Oct. 14, 2009), http://legaltimes.typepad.com/blt/2009/10/ftc-.html [https://perma.cc/7F9P-2WMS].

375. *Id.*

376. *See supra* Section I.B.

377. *Cf.* Slobogin, *supra* note 257, at 841 (drawing on Fifth Amendment cases to conclude that in subpoena law "the distinction between personal and impersonal records is a crucial one").

378. *See,* e.g., Citron & Pasquale, *supra* note 12, at 18; Desai & Kroll, *supra* note 12, at 6–23; David Lehr & Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn About Machine Learning*, 51 U.C. DAVIS L. REV. 653, 655 (2017); Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085, 1087 (2018). The project of ensuring governmental algorithms are transparent and accountable is a separate but related project. *See, e.g.*, Cary Coglianese & David Lehr, *Transparency and Algorithmic Governance*, 71 ADMIN. L. REV. 1, 4 (2019); Tal Z. Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503, 1563–64.

379. *See supra* Part I.

380. *See supra* note 290 and accompanying text.

account statements, held by businesses—and confusingly calls them "business records."[381] Fourth Amendment jurisprudence thus has little to offer from a prescriptive standpoint or in terms of linguistic precision.

What would it mean to write laws with this privacy hierarchy in mind? A prominent legislative example of a failure to differentiate regulatory monitoring from crime surveillance comes from what has been called the constitution of the administrative state: the APA. Section 555(c) of the APA specifies that any "requirement of a report, inspection, or other investigative act or demand may not be issued, made, or enforced except as authorized by law."[382] Drafters intended the APA to govern both crime agencies and regulators,[383] and the official legislative notes on section 555 show that they wanted to address personal privacy.[384] Given that personal privacy is violated mostly by crime agencies associated with the Fourth Amendment and government overreach,[385] lawmakers drafting a statute covering all agencies would understandably err on the side of constraints.

Despite being drafted with a goal of constraining crime agencies' information collection, the APA is rarely applied to crime agencies.[386] Thus, through the APA lawmakers imposed an additional hurdle for regulatory monitoring that did not exist for crime agencies. Although in court the APA has not posed a significant obstacle to the FTC and other regulators' exercise of monitoring,[387] agencies decide on courses of action to minimize the chance of being judicially overturned.[388] By

---

381. United States v. Miller, 425 U.S. 435, 446 (1976) (finding no privacy exception for financial records).

382. Administrative Procedure Act, 5 U.S.C. § 555(c) (2012).

383. Puerto Rico v. United States, 490 F.3d 50, 60 (1st Cir. 2007) (noting "the existence of the APA as a means for reviewing the FBI's actions"); Kenneth Culp Davis, *An Approach to Legal Control of the Police*, 52 TEX. L. REV. 703, 708 (1974) (explaining drafters' intent for the APA to apply to crime agencies).

384. H.R. REP. NO. 79-1980, pt. 4, at 264 (1946) ("Investigations may not disturb or disrupt personal privacy . . . .").

385. *See supra* Section III.B.1.

386. *See, e.g.*, Rachel E. Barkow, *Separation of Powers and the Criminal Law*, 58 STAN. L. REV. 989, 989 (2006) ("[U]nlike the administrative law context, where agencies must adhere to the structural and procedural protections of the Administrative Procedure Act and their decisions are subject to judicial review and political oversight, the government faces almost no institutional checks when it proceeds in criminal matters."); Slobogin, *supra* note 14, at 122 ("The fact that police are exempt [from administrative law] appears to be an inadvertent byproduct of judicial constitutional activism and our federalist structure rather than a considered policy development.").

387. *See supra* Section IV.A (reviewing judicial authorization of FTC monitoring).

388. Although agency avoidance of potential review is difficult to document, it often inferred in the literature. *See, e.g.*, Mendelson & Wiener, *supra* note 322, at 472 (discussing common assumptions that agencies avoid OIRA review and describing the difficulty in knowing diverse agency responses); Jennifer Nou, *Agency Self-Insulation Under Presidential Review*, 126 HARV. L. REV. 1755, 1756–57 (2013) (describing agencies' reluctance to have their decisions overturned by courts).

failing to differentiate the information collection nuances of the administrative state, lawmakers may have, through the APA, inadvertently had a chilling effect on business regulators regarding information collection.

The information default in administrative statutes such as the APA would ideally reflect the different privacy implications and historical tendencies of the specific type of agency. The APA might, for instance, be amended to change its default rule to allow a regulator to collect information from businesses necessary to carry out its mission. Congress could then limit that default for any given agency or in particular contexts, such as through the Paperwork Reduction Act.[389] Indeed, the APA may be best interpreted as allowing broad regulatory monitoring as long as an agency's organic statute mentions basic information collection authority—since that is how crime agencies' authority has been interpreted.[390]

In designing monitoring statutes, there would be further value in adjusting for the type of information collected. Lawmakers and judges might, for instance, give less weight to the business owners' interests in withholding anonymized personal data from regulators if that business is already routinely sharing similar nonanonymized data with crime agencies. Crime agencies would, in a sense, provide a floor for what business regulators could collect. More important than any particular reform, a reoriented normative framework for monitoring should more explicitly fit each type of information collection, rather than subsuming regulatory monitoring into the constraint-oriented crime surveillance framework.

None of this speaks to valid concerns about business regulators taking adequate precautions with any data collected, including passing information on to crime agencies[391] Information-sharing concerns are relevant to the question of deciding whether to support a monitoring proposal because policymakers, scholars, and the public must have confidence in advance that appropriate safeguards are possible. In addition to the existing constraints discussed above, one layer of additional protection would be statutorily prohibiting the regulator from collecting personal data, such as accessing the contents of Gmail

389. *See supra* note 320 and accompanying text (discussing the Paperwork Reduction Act).

390. *See supra* notes 325–327 and accompanying text.

391. A tradeoff exists between performance and engineering standards. Performance standards are broader guidelines and best practices that are harder to monitor but provide more flexibility in identifying wrongdoing. Engineering standards are more precise, facilitating both compliance by the business and monitoring by the regulator, but allow less flexibility to police new harms. *See, e.g.*, Cary Coglianese & Jennifer Nash, *The Law of the Test: Performance-Based Regulation and Diesel Emissions Control*, 34 YALE J. ON REG. 33, 39 (2017).

messages, except where necessary for the nature of the law.[392] Instead, the regulator may be allowed to collect information about Google's policies, such as how its algorithms analyze, store, and share those emails, and perhaps the anonymized consumer complaints that Google has received.[393]

Another layer of protection for individuals' privacy would come from mandating firewalls for sharing information both within the agency and externally. Banking regulators provide one such model, in which examiners closely safeguard the raw data they collect.[394] The Office of the Inspector General could then ensure that regulators are following mandated data security precautions, as it did with the CFPB.[395] Although business regulators are already hesitant to collect sensitive information and reluctant to share it, these limits built into legislation would limit risks further.[396]

Once it is recognized that regulators can collect valuable information from businesses without undermining privacy, the issue of monitoring platforms can be analyzed more rigorously. Empirical work on the cost-benefit analysis of monitoring, including a comparison to ex post fines, would advance that project considerably. A crucial initial step is to weigh the tradeoffs on their merits, rather than dismiss monitoring out of a fear that collecting data from Amazon, Google, Facebook, or other businesses is a step on the path to totalitarianism.

CONCLUSION

Although the linkage between regulatory monitoring and personal surveillance is inevitable, these two administrative mechanisms need greater distinction and coherence. If information is the lifeblood of good governance, an increasingly muddled monitoring

392. *See supra* Section II.C.2 (discussing monitoring design and effectiveness). Some privacy statutes already make this distinction, albeit imperfectly. *See, e.g.*, 18 U.S.C. § 2702(a) (2012) (restricting access to the contents of personal emails). Some protections, such as for discrimination based on names identified with race, may require personally identifiable information to be collected. In those cases, the purpose and nature of the information would be spelled out by statute, and the need to protect the victims should be balanced against those victims' privacy interests.

393. All that data either implicates no individual user or could be anonymized before being handed over to the government.

394. *See* Gramm-Leach-Bliley Act, 15 U.S.C. § 6801(a) (2012) ("It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."); Drake Mann, Christopher L. Travis & Don Lloyd Cook, *Data Security and Privacy: More Than I.T.*, 50 ARK. LAW. 14, 15 (2015) ("[T]he banking sector may have the most mature regulation of all information security regulatory regimes.").

395. OFFICE OF INSPECTOR GEN., *supra* note 372, at 1 (2018).

396. *See supra* notes 283 to 285 and accompanying text.

framework constricts a key artery of the administrative state. Privacy, as it is currently understood and advocated, offers a pretext for deregulation.

Nowhere is state information incoherence starker than in the nonmonitoring of the platform economy. The very firms that have enabled the state to circumvent restrictive surveillance laws are themselves unusually shielded from observation, even as many other industries are required to provide troves of data for regulatory examination. As a result, key regulators, most notably the FTC, do not have the information needed to analyze arguably the most important firms in the modern economy—the gatekeepers of information in the information age. Paradoxically, more ongoing private information collection by the government—in other words, activity that could easily be confused with surveillance and often is—might in fact be necessary to contain harmful surveillance of individuals.

Faced with an increasingly opaque and continually changing business landscape, some of the most important administrative agencies in the information age are sitting on dormant "power to get information from those who best can give it and who are most interested in not doing so."[397] Regulators would be better situated to exercise that authority with monitoring moved out of the shadow of surveillance.

397. United States v. Morton Salt Co., 338 U.S. 632, 642 (1950).