THE PROMISE AND PERILS
OF TECH WHISTLEBLOWING

Hannah Bloch-Wehba

ABSTRACT—Whistleblowers and leakers wield significant influence in technology law and policy. On topics ranging from cybersecurity to free speech, tech whistleblowers spur congressional hearings, motivate the introduction of legislation, and animate critical press coverage of tech firms. But while scholars and policymakers have long called for transparency and accountability in the tech sector, they have overlooked the significance of individual disclosures by industry insiders—workers, employees, and volunteers—who leak information that firms would prefer to keep private.

This Article offers an account of the rise and influence of tech whistleblowing. Radical information asymmetries pervade tech law and policy. Firms exercise near-complete control over corporate information, shielding their activities from oversight and scrutiny by regulators and the public. Secrecy, however, begets leaks, and leaks have become the de facto source of crucial information for lawmakers, regulators, and the public. Today, whistleblowing is an important part of broader efforts to bring accountability and transparency to the tech industry.

Yet existing frameworks for protecting whistleblowers are partial and haphazard. The law often permits firms to retaliate against internal critics, leakers, and organizers. The result is an informational environment shaped by selective disclosures on the part of tech whistleblowers and enormous discretion for tech firms that can choose whether and how to respond. Whistleblowing is therefore an incomplete, but still significant, source of information in the absence of meaningful, rigorous, and systematic transparency rules. In this Article, I make the case that broader protections for whistleblowing are a necessary component of systemic regulation of the tech sector.

AUTHOR—Associate Professor of Law, Texas A&M University School of Law; Affiliate Fellow, Yale Law School Information Society Project; Affiliate Fellow, NYU School of Law Policing Project. My thanks to Jenny Carroll, Vanessa Casado Perez, Rebecca Crootof, Evelyn Douek, Michael Z. Green, Thomas Kadri, Christopher Morten, Scott Mulligan, Gali Racabi, Neil Richards, Alicia Solow-Niederman, Nitasha Tiku, Nancy Welsh, and
Peter Yu for helpful conversations and insights about this project. This Article also benefited enormously from feedback during presentations at the 2022 Texas A&M faculty scholarship retreat, the 2023 Freedom of Expression Scholars Conference, and the 2023 Privacy Law Scholars Conference. I am grateful to the student editors of the Northwestern University Law Review, whose work greatly improved this piece. All errors are my own. Thank you to Christopher Reed, whose patience, love, and support make everything possible; Max and Rebecca Reed, who bring me boundless joy; and the Fort Worth Zoo, without whose facilities many productive Saturday mornings would have been out of reach. I am grateful to the Knight Foundation for its support for this project.

INTRODUCTION

Cambridge Analytica harvested Facebook user data.¹ Google planned to build a censored search engine for the Chinese market.² AT&T cooperated


with the National Security Agency’s warrantless wiretapping program.\textsuperscript{3} U.S. intelligence services extracted data directly from the servers of internet companies.\textsuperscript{4} Instagram was terrible for teen girls’ mental health.\textsuperscript{5} Facebook applied double standards to content moderation decisions that favored the famous and powerful.\textsuperscript{6} Twitter’s data security was garbage.\textsuperscript{7} Uber dodged its taxes.\textsuperscript{8}

We know about these controversies only because of unauthorized disclosures of information from organizational insiders—in short, because of leaks and whistleblowing.\textsuperscript{9} This Article identifies and explains the growing influence of whistleblowers in technology law and policy. Leakers and whistleblowers have become crucial sources of information for regulators, lawmakers, and the public seeking to understand technology companies and hold them accountable.\textsuperscript{10}

We depend on individual whistleblowers to provide key information about technology companies, products, and problems. Consider Erika Cheung, the Theranos employee who, in 2015, defied her nondisclosure agreement and sent an email to the Centers for Medicare and Medicaid Services about the flaws in the company’s finger-prick blood testing protocols.\textsuperscript{11} Soon afterward, John Carreyrou reported in the \textit{Wall Street Journalists} that the company was exempt from tax.\textsuperscript{12}

\begin{thebibliography}{10}
\bibitem{horwitz2021facebook} I return to offer a definition and distinction between “leaks” and “whistleblowing” in a few pages. \textit{See infra} Part I.
\bibitem{horwitz2021facebook} \textit{See infra} Part III.
\end{thebibliography}
Journal that Theranos had “struggled behind the scenes” to deliver on its promises of advancements in blood testing technology. The next day, inspectors from the Food and Drug Administration “showed up unannounced” at the company’s facilities and pressured the company to stop using its “nanotainers” and finger-prick methods. Then Safeway and Walgreens each announced they were cancelling planned partnerships with the company. Criminal investigations soon followed, and in December 2022, founder Elizabeth Holmes was sentenced to over a decade in prison for fraud.

Though made by individuals, whistleblower disclosures are systematically significant: they drive market-based responses, inform public discourse, and prompt policymakers to react. But while tech whistleblowers play an increasingly prominent role, they have yet to receive sustained scholarly treatment. My core claim is that whistleblowing is playing an

---


16 See infra Parts II–III.

17 For scholarly discussion of whistleblower protections, see Sonia K. Katyal, Private Accountability in the Age of Artificial Intelligence, 66 UCLA L. REV. 54, 126–27 (2019), which points toward whistleblower protections as a potential answer to overexpansive trade secrecy. Outside of legal scholarship, examples are also limited but include Rebekah Larsen, ‘Information Pressures’ and the Facebook Files: Navigating Questions Around Leaked Platform Data, 10 DIGIT. JOURNALISM 1591, 1599 (2022), which advocates for greater transparency around how academic researchers approach and work with leaked data, and Philip Di Salvo, Leaking Black Boxes: Whistleblowing and Big Tech Invisibility, FIRST MONDAY (Dec. 2022), https://doi.org/10.5210/fm.v27i12.12670 [https://perma.cc/SJR7-5AMZ], which provides descriptive case studies of recent instances of whistleblowing by Facebook and Google employees. In the popular press, see Erin Woo, A Tech Whistle-Blower Helps Others Speak Out, N.Y. TIMES (Nov. 24, 2021), https://www.nytimes.com/2021/11/24/technology/pinterest-whistle-blower-ifeoma-ozoma.html [https://perma.cc/2H8F-5MP7], which describes California’s bill to add protections for whistleblowers of discrimination in the workplace; Shirin Ghaffary, Big Tech’s Employees Are One of the Biggest Checks on Its Power, Vox (Dec. 29, 2021), https://www.vox.com/recode/22048750/whistleblower-facebook-google-apple-employees [https://perma.cc/VB9B-U3MR], which discusses the
increasingly significant, though underappreciated, role in checking excessive secrecy in tech, alerting the government and the public about potential wrongdoing, and highlighting areas of concern for policy action and development.\textsuperscript{18}

By highlighting the significance of whistleblowing, I make three key contributions. First, I explain how the technology sector’s resistance to transparency and oversight has, perhaps counterintuitively, encouraged leaking and whistleblowing. I attribute the rise of whistleblowing to two related dynamics that have impeded the flow of information about technology. First, whistleblowing has grown in importance and influence because the regulatory state has struggled to formulate systemic rules for governing emerging technologies.\textsuperscript{19} An information-intensive economy generates substantial challenges for a regulatory state oriented toward industrial production.\textsuperscript{20} Existing regulatory models, which “presumed well-defined industries, ascertainable markets and choices, and relatively discrete harms amenable to clear description and targeted response,” have struggled to address emerging informational modes of production.\textsuperscript{21} With the erosion of those presumptions, questions remain about how exactly the regulatory state should adapt in the face of technological changes that have,
to date, skirted meaningful oversight.22 Emerging models of collaborative governance, public–private partnerships, and other managerial structures of legal compliance carry with them the potential for co-optation and abuse.23 Effective regulation and enforcement under conditions of information asymmetry and complexity require new modes of oversight and extensive access to information.24

Compounding regulatory inaction, technology firms have employed a welter of different legal privileges and obligations to consolidate and promote corporate control of information.25 Using trade secrecy, contractual arrangements, company policies, and even privacy and computer crime law, tech companies have laid claim to expansive informational control—inhbiting regulation, enforcement, and public discourse as a result.26 Firms enforce and protect their informational prerogatives in no small part by

---

22 See, e.g., COHEN, supra note 20, at 172 (stating that an information-intensive economy makes it harder to determine what “should trigger compliance obligations, enforcement actions, and other forms of regulatory oversight”); Andrew Tutt, An FDA for Algorithms, 69 ADMIN. L. REV. 83, 90–91 (2017) (proposing the establishment of a federal regulatory agency to address challenges posed by the proliferation of machine-learning algorithms); Margot E. Kaminski, Binary Governance: Lessons from the GDPR’s Approach to Algorithmic Accountability, 92 S. CAL. L. REV. 1529, 1531–35 (2019) (providing an overview of rationales for regulating algorithmic decision-making and proposing a two-pronged approach that accounts for individual due process and the need for systemic regulation based on collaborative governance); Alicia Solow-Niederman, Administering Artificial Intelligence, 93 S. CAL. L. REV. 633, 643 (2020) (“[T]echnical decisions about algorithms are not only mediating public safety, but also encoding values, without any uniform oversight, normative requirements, or public accountability.”); Morten & Kapczynski, supra note 20, at 497 (“Yet existing tools for an independent assessment of clinical trial data are inadequate. What remains missing is an effective legal and regulatory framework for the release of this data within the United States.”); Andrew D. Selbst, An Institutional View of Algorithmic Impact Assessments, 35 HARV. J.L. & TECH. 117, 190–91 (2021) (arguing that algorithmic impact assessment regulations are a key for public oversight of algorithms, but that a careful balance between flexibility and accountability must be struck for regulation to be effective).

23 COHEN, supra note 20, at 187 (“[C]oregulatory processes . . . have produced significant devolution of regulatory authority to the private sector.”); Hannah Bloch-Webba, Algorithmic Governance from the Bottom Up, 48 BYU L. REV. 89, 82 (2022) (“The introduction of algorithms into political contexts fraught with power disparities has enhanced the power of the private sector but not meaningfully boosted the power of marginalized individuals or groups.”).


25 See infra Section II.B.

26 See infra Section II.B; see also Menell, supra note 24, at 23 (“In a broad range of scenarios, access to information has proved critical to the capacity of government to protect its citizenry and maintain a properly functioning society.”).
clamping down on worker speech and expression.\textsuperscript{27} In an atmosphere of tight informational control, leaks and whistleblowing play a critical “safety valve” role.\textsuperscript{28}

The Article’s second contribution is its analysis of how existing whistleblower protections shape and channel what we learn about technology firms. Despite the political, legal, and social influence of tech whistleblowers, existing legal protections rooted in sectoral regulation are haphazard and incomplete.\textsuperscript{29} Patchwork laws shield those who disclose information in certain domains from retaliation while others are left out in the cold.\textsuperscript{30} These partial protections mean that the public is more likely to learn of some kinds of wrongdoing than others.

I show that, in the absence of tech-specific legislation, tech workers have increasingly turned to two alternative sources for protection of public speech about their employers: securities law and labor law.\textsuperscript{31} The Securities and Exchange Commission (SEC) whistleblower program offers appealing monetary incentives for those who come forward with evidence of securities fraud or other wrongdoing.\textsuperscript{32} The National Labor Relations Act (NLRA), for its part, protects worker speech when it is part of “concerted activit[y] for . . . mutual aid or protection.”\textsuperscript{33} As tech workers seek more power and control over decision-making in the workplace, the worker movement has become increasingly bound up with worker speech about corporate practices.\textsuperscript{34}

Third, the Article assesses the pitfalls of relying exclusively on whistleblowing and offers a potential remedy. Whistleblower disclosures (whether made through formal legal channels under existing protections or to journalists without legal sanction) are necessarily partial and incomplete.\textsuperscript{35} The tech industry’s valorization of secrecy further raises the personal,
reputational, and professional costs of blowing the whistle and no doubt deters many individuals from coming forward. These costs illustrate a structural problem: whistleblowing puts the burden on individuals to alleviate systemic informational problems.

For decades, scholars and policymakers across many areas have understood that whistleblowing has a vital role to play in contexts of information asymmetry and technical complexity. Today, however, lawmakers simultaneously depend on tech whistleblowers to inform the public while ignoring their need for protection. While I leave most institutional design considerations for another day, I propose two concrete interventions that would broaden whistleblower protections and ensure that information critical to tech oversight and accountability reaches the appropriate parties. First, state and federal lawmakers should include whistleblower protections in proposed legislation reforming oversight of technology firms, platforms, algorithms, artificial intelligence (AI), and the like. Second, Congress should amend the Federal Trade Commission Act of 1914 to ensure that individuals who blow the whistle regarding unfair or deceptive trade practices are protected.

Understanding the role and influence of whistleblowers and industry insiders is important now amid ongoing debates about the optimal way to promote accountability and transparency in the tech industry. Federal, state, and local lawmakers are considering a range of mechanisms intended to foster accountability for AI and automated decision systems, including impact assessments, algorithmic registers, and auditing mandates. Lawmakers have also introduced and enacted legislation intended to promote the transparency of large online platforms through disclosure mandates and

---

36 See infra Section III.B.
38 See infra Section IV.A.
39 See infra Section IV.D.2.
researcher access requirements. Federal regulators are considering how best to exercise oversight of autonomous vehicles and discriminatory AI. In the context of these ongoing debates, this Article highlights the inadequacies of the existing regulatory regime and proposes reforms that would facilitate future disclosures of information.

The Article proceeds in four Parts. Part I offers a brief note of clarification about the distinction between “leakers” and “whistleblowers.” Part II sets out the legal and political dynamics that foster information asymmetries and hamper oversight of the technology sector. Part III shows how tech whistleblowers use legal protections to disclose crucial information about a range of practices and problems. Part III also shows that, for many whistleblowers, protections are elusive, putting workers at serious risk if they decide to blow the whistle. Part IV puts whistleblowing in context: whistleblowers are a crucial component of systemic reform and oversight of the tech sector. But the current system of de facto reliance on individual whistleblowers is underinclusive and perhaps undemocratic. Broadening existing protections would help to address the problems of haphazard disclosure created by the current framework.

I. DEFining TECH WHISTLEBLOWING

Both “whistleblower” and “leaker” are “loaded term[s]” with significant connotations for public understanding. Throughout this Article, I primarily use the term “whistleblower” instead of “leaker” to emphasize that my focus here is on those who disclose information to promote the public interest and accountability, rather than (for example) to steal secrets for competitive gain. I use this term even though, as the rest of the Article shows, those who blow the whistle often do so outside of the “proper channels” and without the protection of the law.

---

45 Menell, supra note 24, at 8.
46 See infra Part III.

1511
There is no meaningful consensus, let alone a legal rule, that distinguishes a whistleblower from a leaker.\textsuperscript{47} One typical way of drawing the distinction is based on the recipient of the disclosure.\textsuperscript{48} Black’s Law Dictionary defines a whistleblower as a worker who “reports employer wrongdoing to a governmental or law-enforcement agency.”\textsuperscript{49} But this definition excludes individuals who blow the whistle using internal channels within the employer’s organization.\textsuperscript{50} It also excludes unauthorized disclosures to the media or the broader public.\textsuperscript{51} A still broader definition abandons the focus on illegal conduct and covers “organization members’ disclosure of illegal, immoral, or illegitimate practices under the control of their employers, to parties who may be able to effect action.”\textsuperscript{52}

Relatedly, some distinguish between whistleblowers and leakers based on whether disclosure was authorized or mandated by law. One broad definition of whistleblowing suggests that the individual wants to “reveal malfeasance” using existing legal mechanisms.\textsuperscript{53} A leak, by contrast, is often defined as an “anonymous unauthorized disclosure of confidential information,” typically from within a government agency to the media.\textsuperscript{54} As opposed to whistleblowing, leaking connotes the absence of legal protection: leakers cannot, or do not, go through the “proper channels.”\textsuperscript{55}

Existing legal channels for whistleblowing are set forth in specific statutes that offer particular substantive and procedural protections. For instance, under the Whistleblower Protection Act of 1989, any federal

\textsuperscript{48} UYS, supra note 44, at 33.
\textsuperscript{49} Whistleblower, BLACK’S LAW DICTIONARY (11th ed. 2019).
\textsuperscript{50} Elizabeth C. Tippett, The Promise of Compelled Whistleblowing: What the Corporate Governance Provisions of Sarbanes Oxley Mean for Employment Law, 11 EMP. RTS. & EMP. POL’Y J. 1, 4 n.26 (2007); Lobel, supra note 30, at 446.
\textsuperscript{52} Marcia P. Miceli & Janet P. Near, Characteristics of Organizational Climate and Perceived Wrongdoing Associated with Whistle-Blowing Decisions, 38 PERS. PSYCH. 525, 525 (1985).
\textsuperscript{53} Pozen, supra note 28, at 534 n.111; see also Benkler, supra note 47, at 285 n.24 (arguing that the term whistleblowing “threaten[s] to cabin the debate to what would be legal under the existing whistleblower protection regime”).
\textsuperscript{54} Margaret B. Kwock, Leaking and Legitimacy, 48 U.C. DAVIS L. REV. 1387, 1394–95 (2014).
employee who discloses “gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety” to Congress, a Special Counsel, or an Inspector General is protected from retaliation. Federal whistleblower protections grew out of late-1970s civil service reforms that tried to improve the “performance” and flexibility of the government amid rising distrust and demands for a more efficient and responsive bureaucracy. Public-sector whistleblowing is, essentially, about promoting efficiency and accountability.

Private-sector whistleblower law, by contrast, is rooted not in hostility to government but rather in affinity to law enforcement and regulatory need. In order to incentivize insiders to come forward, many formal whistleblower provisions focus on protecting individuals who blow the whistle on illegal activity or are involved in legal proceedings against their employers under specific sectoral statutes that regulate substantive harm. These statutes recognize the regulatory demand for insider information, particularly in light of technological, economic, and political shifts toward increasing complexity within firms and decreasing capacity within administrative agencies. Another view of private-sector whistleblowing sees it primarily as an exception to the at-will employment rule and a mechanism of redressing power disparities between labor and management.

A second way of distinguishing whistleblowers from leakers involves the content of the disclosure. A minimal definition of whistleblowing covers individuals who disclose illegal activity for which an organization is responsible. But broader definitions might include disclosures of “morally wrong” or “unethical” behavior. A still broader definition of whistleblower would include “disclosures about disagreements with corporate policy.” Complicating matters further, legal scholars have distinguished between

---

60 See infra notes 157–160 and accompanying text.
61 See id.
62 See id.
63 Id. at 28.
different types of leaks based on motivation, source, and scale of disclosure.\textsuperscript{64} Indeed, scholars of state secrecy have examined what Professor Margaret Kwoka calls “whistleblower leaks” and what Professor Yochai Benkler calls “accountability leaks”—unauthorized disclosures that are intended to reveal abuses or malfeasance.\textsuperscript{65}

In this Article, I am focused primarily on individuals who disclose illegal, unethical, or otherwise wrongful behavior by organizations, regardless of whether they use legal channels to do so. I explore disclosures made in the public interest rather than those made chiefly for personal or political gain. Whether disclosures are motivated by disagreement with policy does not concern me for two reasons. First, sometimes policy-motivated disclosures reveal legal wrongdoing.\textsuperscript{66} Second, the legal structures shielding whistleblowers do not distinguish based on the motivation for disclosure.\textsuperscript{67} Nor does my definition hinge on whether disclosures are authorized or shielded by law. As the Article shows, existing protections often fall short of protecting whistleblowing. But that does not diminish the value of whistleblower disclosures or convert whistleblowers into purely self-interested actors. Instead, as the next Part shows, whistleblowing (regardless of legal protection) plays a crucial role in facilitating the flow of information between firms, regulators, lawmakers, and the public.

II. THE CAUSES AND EFFECTS OF TECH SECRECY

To put tech whistleblowing in a broader context, this Part begins by synthesizing the voluminous literature showing that tech law and policy are shaped by radical information asymmetries. These asymmetries stem from many sources, including regulatory inertia; broad claims of corporate secrecy; and restrictions that constrain how workers, journalists, researchers, and the public learn about and discuss issues of public concern. Meanwhile, critical questions about free expression, privacy, data security, AI, and more are being resolved primarily within the same firms that are eluding regulation. If “information is the ‘lifeblood’ of effective governance,” the current prospects for effectively governing tech look dim.\textsuperscript{68}

\textsuperscript{64} Kwoka, supra note 54, at 1395.
\textsuperscript{65} Id. at 1387; Benkler, supra note 47, at 303 (proposing a defense for “accountability leaks . . . that expose substantial instances of illegality or gross incompetence or error in certain classes of particularly important matters associated with the activities of the national security system”).
\textsuperscript{66} See infra Section III.A.1 (discussing Frances Haugen).
\textsuperscript{67} See infra Part III.
A. Regulators Adrift

Information asymmetries arise in part from regulatory failings. For the most part, the United States has followed a “permissive approach” to tech regulation, driven by both laissez-faire ideology and an overall optimism about technological innovation. That permissive approach, in turn, has fostered the concentration of resources in the private sector and has allowed Silicon Valley to significantly “outpace” public investment in both the development and regulation of technology. As Professor Alicia Solow-Niederman points out, one result is a form of de facto private governance through digital technology that directly affects human behavior, individual rights, and freedom. In no small part because of this hands-off approach, concerns are growing that the government is now ill-equipped to understand technology and to intervene when necessary to protect the public. In order to effectively regulate emerging technologies, regulators must acquire new kinds of information and expertise. Consider, for example, artificial intelligence and machine learning (AI/ML). AI/ML is rapidly reshaping finance, health care, transportation, and employment, among many other domains. A straightforward regulatory approach might be to require the disclosure of source code. But disclosure is a “deceptively simple solution to the problem of algorithmic transparency.” On a technical level, the complexity of AI/ML is likely to make disclosures meaningless because algorithms might be adjusted and incorporate new data over time.

---

70 See Solow-Niederman, supra note 22, at 644.
71 Id. at 684.
72 See, e.g., Ryan Calo & Alex Rosenblat, The Taking Economy: Uber, Information, and Power, 117 COLUM. L. REV. 1623, 1671 (2017) (“[R]egulators will need to develop a better understanding of the technology and business practices of sharing economy firms in order to uncover the entire range of offending practices.”); Van Loo, supra note 68, at 1566 (“[R]egulators often lack visibility into business activities.”); Solow-Niederman, supra note 22, at 638 (“[G]eneralist policymakers are likely to lack the expertise or resources to make informed governance choices about highly technical digital code.”).
73 Julie E. Cohen & Ari Ezra Waldman, Framing Regulatory Managerialism as an Object of Study and Strategic Displacement, 86 LAW & CONTEMP. PROBS., at i, ii (2023) (“Regulators shackled by the assumptions of legacy regulatory models have been unable to develop new models, and legacy models’ evident inadequacies have reinforced the seeming inevitability of the managerial turn.”).
76 Solow-Niederman, supra note 22, at 639 (“This dynamism contrasts markedly with static regulatory objects that may be more amenable to prescriptive controls.”).
models are also often both “inscrutable and nonintuitive,” calling the value of disclosure into further question. On an institutional level, scholars such as Andrew Tutt and Solow-Niederman have questioned whether bureaucrats with sector-specific expertise will be able to effectively govern AI/ML.

Regardless of any particular regulatory choice, AI/ML exemplifies a basic problem raised by attempts to govern informationally intensive activity: information asymmetry. If the rise of AI/ML has not yet spurred new regulatory approaches, it has at least led observers to appreciate the significant “information disparities between developers on the one hand, and policymakers and the public on the other.” Any regulatory strategy for AI/ML needs to account for the information asymmetries that have hamstrung regulators and plagued scholars. As Professor Andrew Selbst concisely put it in his study of algorithmic impact assessments, “right now there is just a lot we don’t know.” Even outside of the regulation of AI/ML itself, regulators often lack key information to be able to understand “routine” products with highly technical components. But information asymmetries do not arise organically: as discussed below, these asymmetries are the product of legal entitlements.

B. The Legal Architecture of Informational Control

The law compounds information asymmetries by allocating significant informational control to firms. Collectively, the legal mechanisms I describe below—commercial secrecy, control of worker speech, and obstacles to public and journalistic access—reflect the prevailing default rule of firm control over corporate information. Corporate control of information presents regulatory obstacles, to be sure, but it also has much further reaching effects, dampening public discourse and legal change.

1. Commercial Secrecy

To begin, firms use expansive arguments about trade secrecy and commercial confidentiality to insulate themselves from oversight by regulators. In environmental law, for example, Professors Charles Tait Graves and Sonia Katyal identify how chemical manufacturers leverage

---

78 Tutt, supra note 22, at 114; Solow-Niederman, supra note 22, at 638–39.
79 Selbst, supra note 22, at 125.
80 Selbst & Barocas, supra note 77, at 1089 (“Scholarly and policy debates about regulating a world controlled by algorithms have been mired in difficult questions about how to observe, access, audit, or understand those algorithms.”).
81 Selbst, supra note 22, at 127.
82 Van Loo, supra note 24, at 406.
broad trade secrecy claims to withhold information about health effects from the Environmental Protection Agency. As Graves and Katyal point out in the context of hydraulic fracking, “it is often difficult to disentangle assertions of trade secrecy from an underlying resistance to regulation and lack of regulatory oversight.”

As the foregoing example shows, the phenomenon of regulatory obstruction is by no means unique to Silicon Valley. But tech companies have embraced a culture of secrecy and have aggressively exploited trade secrecy and corporate confidentiality beyond ordinary expectations. Underscoring the breadth of these claimed protections, tech firms have cited corporate secrecy, for example, to resist regulatory oversight of potential pay discrimination. In 2014, Google was selected for a “compliance review” after it was awarded a federal contract. The Office of Federal Contract Compliance Programs (OFCCP) sought data about compensation and potential gender-based pay disparities in conducting its review. When OFCCP sought more data in the course of its investigation, Google resisted, arguing that it should not be required to produce “confidential data.”

As Professor Amy Kapczynski has argued, faith in the power of trade secrecy has become naturalized in legal scholarship and policy circles, where the imperative to protect corporate secrecy is almost a baseline assumption. At the same time, reporting requirements, compliance monitoring, algorithmic enforcement, and standard-setting have become increasingly important “regulatory modalities” for constraining informationally intensive industries, but they often lack direct or effective accountability mechanisms. In tech law, these new modalities often underpin new kinds of cooperation between state and private actors. It remains unclear, however, whether public agencies have the capacity, ability, or knowledge necessary to “look under the hood” to examine tech firms’ algorithms, policies, or practices.

---

84 Id. at 1359.
87 COHEN, supra note 20, at 189–91.
88 Solow-Niederman, supra note 22, at 681.
89 See, e.g., FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 165 (2015) (arguing that it was unclear whether the Federal Trade Commission had the necessary tools to adequately investigate allegations of “search bias”).
The problems of tech secrecy go beyond the regulatory state, however. Again, commercial secrecy claims are partly responsible, and some of the dynamics driving regulatory inertia also exacerbate information deficits for the public. Continuing with the example of equity in the tech workplace, tech firms have leveraged trade secrecy claims to prevent workforce diversity data from becoming public. In 2011, CNN filed dozens of Freedom of Information Act requests for tech firm workforce diversity data held by the Department of Labor and Equal Employment Opportunity Commission. In response, many firms filed objections to the requests, asserting that disclosure of the diversity data would cause “competitive harm.”

Trade secrecy claims also obstruct public access to critically important information relevant to health, safety, public discourse, and public governance. As Kapczynski has shown, corporations have made broad constitutional claims that regulatory disclosure mandates are “takings.” In response, states have “neuter[ed]” their statutes so that they can compel disclosure to regulators, conditioned on a promise to keep that information confidential. As described below, tech firms also use contract and a bevy of other legal doctrines to buttress claims of trade secrecy and further restrict information flow. The result: firms’ broad claims to secrecy are reified in legal structures that bless corporate opaqueness.

2. Restrictions on Worker Speech

Corporations preserve control of information by taking that control away from workers. The principle of at-will employment means that “employers may generally terminate workers for what they say” or for any reason at all. Because constitutional guarantees of freedom of expression

---

91 Id.
92 See, e.g., Morten & Kapczynski, *supra* note 20, at 495 (providing an example of trade secrecy obstructing access to COVID-19 vaccine trial information); Allison Durkin, Patricia Anne Sta Maria, Brandon Willmore & Amy Kapczynski, *Addressing the Risks That Trade Secret Protections Pose for Health and Rights*, 23 Health & Hum. RTS. J. 129, 130 (2021) (“[T]rade secrecy can also impede access to information that is needed to ensure quality, affordable medicines, thereby burdening the public’s right to health and its right to enjoy the benefits of scientific progress and its applications.”).
93 Kapczynski, *supra* note 86, at 1379.
94 Id. at 1426.
do not generally protect private-sector workers from employment practices that limit their speech, firms are generally free to constrain worker disclosures (within the limits discussed in Part III below).97

Limitations on worker speech rights flow from the doctrine of “managerial prerogative,” which scholars have described as a “powerful prevailing ideology,” “starting assumption,” “background norm,” and “the default governance rule in the workplace.”98 To put it succinctly, management has the right to control both the firm and the firm’s employees.99 In the context of speech rights, as Professor Gali Racabi has described it, managerial prerogative effectively operates to curtail worker speech by redefining it as the proper subject of employer control and thus as the employer’s own speech.100 Because the employer can “exercise . . . control over what the employer itself has commissioned or created,” the individual worker has no “right” to speak.101

In theory, contractual agreements between workers and employers can “overcom[e] the employer prerogative default” and give workers additional speech protections.102 In practice, however, contracts and internal policies are more often used to further restrict worker speech. Among a variety of contractual mechanisms restricting information-sharing, the nondisclosure agreement (NDA) has become the best-known, perhaps in part because it is so endemic: one report estimates that between a third and a half of all U.S. workers are bound by an NDA.103 While NDAs are used across a variety of

---

97 Pauline T. Kim, Market Norms and Constitutional Values in the Government Workplace, 94 N.C. L. REV. 601, 610 (2016) (“Because the state action doctrine limits constitutional restraints to government actors, constitutional protections for speech and privacy have little direct application to private employers.”).
98 Id. at 615; Cynthia L. Estlund, Free Speech and Due Process in the Workplace, 71 IND. L.J. 101, 110 n.25 (1995); Gali Racabi, Abolish the Employer Prerogative, Unleash Work Law, 43 BERKELEY J. EMP. & LAB. L. 79, 82 (2022).
99 Elizabeth Dale, Employee Speech & Management Rights: A Counterintuitive Reading of Garcetti v. Ceballos, 29 BERKELEY J. EMP. & LAB. L. 175, 214 (2008) (noting that management’s control is nonetheless constrained by internal restraints such as workplace custom, external constraints such as laws, and public policy).
100 Racabi, supra note 98, at 95.
101 Id. at 95 (quoting Garcetti v. Ceballos, 547 U.S. 410, 421–22 (2006)).
102 Id. at 98. For example, employment contracts can create both procedural and substantive protections against disciplining or dismissing a worker who exercises their expressive rights. These kinds of procedural protections are often present in contracts for tenured and tenure-track faculty, who have substantial freedom in research and teaching, although much rarer for the majority of academic faculty members who are not on the tenure track. Bridget R. Nugent & Julee T. Flood, Rescuing Academic Freedom from Garcetti v. Ceballos: An Evaluation of Current Case Law and a Proposal for the Protection of Core Academic, Administrative, and Advisory Speech, 40 J.C. & U.L. 115, 145–46 (2014).
103 RACHEL ARNOW-RICHMAN, GRETCHEN CARLSON, ORLY LOBEL, JULIE ROGISKY, JODI SHORT & EVAN STARR, SUPPORTING MARKET ACCOUNTABILITY, WORKPLACE EQUITY, AND FAIR
industries and sectors, the technology sector appears to use them particularly broadly. Many tech companies require every visitor to their offices to sign an NDA as a condition of physical entry. NDAs are often part of the terms of a software license. Indeed, NDAs are so common that one legal tech firm introduced a standard template, reasoning that “the sheer volume of [nondisclosure] contracts that [the firm was] processing and the cost, time and effort involved was clearly disproportionate to the value they were adding or bringing, to anyone.”

Firms use NDAs to control employee speech. Of course, firms contractually bind employees not to disclose trade secrets. But NDAs can also reach far beyond bona fide trade secrets to prevent employees from speaking about a broad range of information. As Professor Lauren Rogal has written, employee NDAs can also cover “confidential or proprietary information,” defined far more broadly than trade secrecy protections. Rogal describes how Theranos, the blood testing startup that imploded after revelations of widespread fraud, aggressively used broad NDAs to prevent employees from speaking publicly. NDAs also operate alongside other policies and contractual restrictions that inhibit worker speech and mobility, including nonsolicitation agreements and noncompete agreements.

Because employees who enter into NDAs are broadly understood to have “voluntarily” agreed to remain silent, the dominant doctrinal approach has emphasized the primacy of freedom of contract over the potential

---


106 About Us, ONeNDA, https://onenda.org/about [https://perma.cc/EKT6-CA35].


109 See, e.g., Denson v. Donald J. Trump for President, Inc., 530 F. Supp. 3d 412, 432–33 (S.D.N.Y. 2021) (finding that a restrictive confidentiality agreement covering virtually “unlimited” information was unenforceable).

110 Rogal, supra note 11, at 1687–88.

111 Id. at 1668.

112 Lobel, supra note 107, at 786 (“NDAs, noncompetes, innovation assignment clauses, mandatory arbitration, and secrecy policies remove the tongues of employees, inventors, creators, and entrepreneurs, prohibiting them from speaking up against the institution and from using their potential to impact the path of an industry.”).
chilling effect of silencing. But contractual secrecy requirements have also given firms substantial leverage over workers. Indeed, the law gives firms “enormous latitude to designate information as confidential.” NDAs and other contractual restrictions in corporate policies, handbooks, and the like constrain employees’ “use of knowledge, skill, and information acquired during employment” and empower the firms that employ them to control that knowledge and the terms of its disclosure. It is not uncommon, for instance, for technology firms to have internal policies that severely restrict workers from speaking to journalists and reporters. Former Pinterest employee Ifeoma Ozoma violated her NDA to disclose the company’s pay disparities and racially discriminatory practices.

In addition to NDAs, firms use both internal and external communications policies to govern how employees interact and share information. Firms also use other “modalities of regulation” for restricting access to corporate information—namely, technical restrictions. Firms have complex, ever-changing corporate policies and technical restrictions.

113 Gordon, supra note 105, at 1114; Hoffman & Lampmann, supra note 108, at 209 (“[O]ur society values autonomy more than contractual fairness.”).
114 Sarah Roberts, Behind the Screen: Content Moderation in the Shadows of Social Media 25–26 (2019) (describing how NDAs, job insecurity, and term-limited status exacerbate the poor working conditions of commercial content moderators for large social media platforms).
115 Arnow-Richman et al., supra note 103, at 2.
118 Woo, supra note 17.
For example, firms constrain calendar access and limit the kinds of topics that can be discussed on internal chat channels. Firms across the tech industry have repeatedly cited arcane violations of these technical restrictions and other workplace policies to justify retaliating against workers who speak out or seek to unionize.

Like broad trade secrecy claims, what matters here is not that any single NDA or other contractual restriction on worker speech is enforceable. Indeed, a growing literature considers potential reasons for invalidating (at least some) NDAs under a variety of different legal doctrines. But even unenforceable contracts can produce “important behavioral changes in parties” because of the fear of litigation and the “potential financial and opportunity costs of a protracted legal battle that they cannot afford or may (erroneously) lose.”

Compounding those chilling effects, transformations in the nature of work have also encouraged broader use of workplace surveillance. The rise of remote work and freelance or “gig” work has diminished mutual trust in the workplace and increased fears of corporate espionage and governing data security and access.

---


124 See, e.g., Alan E. Garfield, Promises of Silence: Contract Law and Freedom of Speech, 83 CORNELL L. REV. 261, 280–85 (1998) (explaining that nondisclosure agreements may be invalidated through proving an inability to create mutual assent or through proffering evidence of unconscionability, such as severely unequal power dynamics); Heidi Kitrosser, Classified Information Leaks and Free Speech, 2008 U. ILL. L. REV. 881, 907 (noting the Supreme Court’s recognition that a “prohibition on disclosure clearly is a prohibition on speech”); Hoffman & Lampmann, supra note 108, at 169, 192 (arguing that the courts should recognize a public policy exception to the enforcement of “hush agreements”); Gordon, supra note 105, at 1115 (arguing that courts should decline to enforce certain NDAs for violating the public policy of free expression).


“exfiltration” of company secrets. The default rule of employer control or “prerogative” allows firms to continually monitor and surveil workers. These technologies make it easier for employers to detect violations and chill speech and labor organizing.

Regardless of whether these mechanisms are ultimately defensible, the scope and extent of corporate control of information imposes serious constraints on individual employees who seek to share information, with significant downstream effects as regulators, lawmakers, and the public are kept in the dark.

3. Restrictions on Research and Journalism

Other bodies of law protect firms from outside scrutiny on an even broader scale. First, computer crime law places informational obstacles in the path of researchers, journalists, and the broader public. Under the Computer Fraud and Abuse Act (CFAA), it is unlawful to “access” and obtain “information” from a “protected computer” “without authorization.” To put it bluntly, the CFAA gives online platforms discretion to grant or deny “authorization” for access and backs those choices up with the force of criminal prosecution and civil liability. As Professor Thomas Kadri has described it, the CFAA permits online platforms to “enforce their preferences about who may access their services and gather information from the internet.”

The CFAA has created substantial uncertainty about the scope of criminal liability and the impact of platform policies barring access. Consider the example of Cybersecurity for Democracy, an NYU research project studying misinformation on Facebook. In 2020, Facebook sent a cease and desist letter to the NYU researchers contending that their use of an unauthorized browser extension to gather information about political

127 Id.
ad targeting violated the firm’s terms of service.\footnote{132}{Jeff Horwitz, Facebook Seeks Shutdown of NYU Research Project into Political Ad Targeting, WALL ST. J. (Oct. 23, 2020), https://www.wsj.com/articles/facebook-seeks-shutdown-of-nyu-research-project-into-political-ad-targeting-11603488553 [https://perma.cc/9MNY-ENEJ].} The implicit threat discouraged the researchers from continuing their work in spite of (or perhaps because of) legal ambiguities: There are significant questions about “whether journalists and researchers who violate platforms’ terms of service in the course of digital investigations are subject to liability under the CFAA.”\footnote{133}{ALEX ABDO, RAMYA KRISHNAN, STEPHANIE KRENT, EVAN WELBER FALCÓN & ANDREW KEANE WOODS, KNIGHT FIRST AMEND. INST., A SAFE HARBOR FOR PLATFORM RESEARCH 10 (2022), https://s3.amazonaws.com/kfai-documents/documents/17a0a57342/3.1.22-Safe-Harbor.pdf [https://perma.cc/N4YJ-ET8T].} To the extent the CFAA does penalize these activities, there are also substantial questions about the constitutionality of these restrictions.\footnote{134}{See, e.g., Sandvig v. Barr, 451 F. Supp. 3d 73, 76 (D.D.C. 2020) (declining to reach the constitutional question in a pre-enforcement challenge to the CFAA).} This degree of legal uncertainty can discourage researchers from undertaking projects that might be seen as a potential risk.

Other bodies of law can similarly impede research, journalism, and public discourse. For example, online platforms have argued that data protection law, including the General Data Protection Regulation, prevents them from disclosing data to journalists or researchers for academic purposes.\footnote{135}{MATHIAS VERMEULEN, KNIGHT FIRST AMEND. INST., THE KEYS TO THE KINGDOM 4 (2021), https://s3.amazonaws.com/kfai-documents/documents/2e579e7afa/7.28.21-Vermeulen.pdf [https://perma.cc/9Q7A-GX8D].} Indeed, Facebook contended that it was \textit{required} to terminate Cybersecurity for Democracy’s access to its platform pursuant to a consent decree it had reached with the Federal Trade Commission (FTC) to settle earlier privacy claims.\footnote{136}{Shannon Bond, NYU Researchers Were Studying Disinformation on Facebook. The Company Cut Them Off, NPR (Aug. 4, 2021), https://www.npr.org/2021/08/04/1024791053/facebook-boots-nyu-disinformation-researchers-off-its-platform-and-critics-cry-f [https://perma.cc/U6TA-LLW4]; see also Cristiano Lima, FTC Rejects Facebook’s Justification for Cutting Off Researchers as “Inaccurate,” WASH. POST (Aug. 5, 2021), https://www.washingtonpost.com/technology/2021/08/05/facebook-nyu-fct-dispute/ (noting that the FTC subsequently dismissed Facebook’s assertion as “inaccurate”).} Meanwhile, rising demands for researcher access to platform data have fostered partnerships such as Social Science One, in which Facebook agreed to provide vetted researchers with access to certain datasets for academic purposes.\footnote{137}{Our Facebook Partnership, SOC. SCI. ONE, https://socialscience.one/our-facebook-partnership [https://perma.cc/4SPC-ZPTS].} But Social Science One and its ilk have been criticized as permitting the platform to “cherry-pick” uncritical partners.\footnote{138}{Thomas E. Kadri, Platforms as Blackacres, 68 UCLA L. REV. 1184, 1189 (2022).} Social scientists, for their part, have critiqued these frameworks
as facilitating the “platform enclosure of knowledge production about human behavior.”

C. The Limits of Voluntary Transparency

Against a background of widespread corporate control of information, a few exceptions to secrecy emerge. First, tech companies have taken steps to disclose information in the public interest of their own accord. For example, many technology companies now publish transparency reports documenting takedown requests, legal process demanding the disclosure of user information, and private enforcement of content-related standards. These transparency reports emerged in substantial part as a response to Edward Snowden’s 2013 revelations of mass surveillance by the intelligence community with the cooperation of tech and telecommunications companies.

Transparency reporting is an outgrowth of, not an exception to, corporate informational control. To facilitate transparency reporting, tech firms have challenged statutory restrictions that prevent them from disclosing information to the public about criminal legal process and national security. These challenges usually mount arguments that restrictions on the disclosure of this information violate firms’ expressive rights. For example, in litigation in the Ninth Circuit, tech firms argued that nondisclosure orders that accompany national security letters are unconstitutional prior restraints on speech. Microsoft similarly challenged the government’s imposition of secrecy orders in litigation in the Western District of Washington. Twitter challenged the government’s determination that it could not publish the total number of national security demands it had received because that number was classified. In the wake of the Snowden disclosures, Google, Facebook, 

---

142 See id. at 532–33 (describing the “performative” use of warrant canaries as a public relations or brand management tool).
143 In re Nat’l Sec. Letter, 863 F.3d 1110, 1119–21 (9th Cir. 2017), amended and superseded by In re Nat’l Sec. Letter, 33 F.4th 1058 (9th Cir. 2022). National security letters are administrative subpoenas issued in connection with national security investigations. Id. at 1114.
Microsoft, and Yahoo all challenged rules that had significantly limited their ability to disclose national security demands to their users.\footnote{Craig Timberg & Cecilia Kang, Google Challenges U.S. Gag Order, Citing First Amendment, WASH. POST (June 18, 2013), https://www.washingtonpost.com/business/technology/google-challenges-us-gag-order-citing-first-amendment/2013/06/18/96835c72-d832-11e2-a9f2-42ec3912ae0e_story.html [https://perma.cc/3K9F-4GWL]; Cecilia Kang, Facebook, Microsoft Release Number of Data Requests from Government, WASH. POST (June 14, 2013), https://www.washingtonpost.com/business/technology/2013/06/14/61a6ff1e-d55c-11e2-a73e-826d299f4f59_story.html [https://perma.cc/PD5B-TVDP]; Hayley Tsukayama, Yahoo Joins Other Tech Firms by Releasing Request Data, Calling for Looser Restrictions, WASH. POST (June 18, 2013), https://www.washingtonpost.com/business/technology/yahoo-joins-other-tech-firms-by-releasing-request-data-calling-for-looser-restrictions/2013/06/18/ba159f20-d818-11e2-a016-925479b094cc_story.html [https://perma.cc/FQ9F-D9L2].} Supports of the tech industry’s self-regulatory transparency regime might point to these efforts to voluntarily disclose critical information as evidence that secrecy in the tech sector is more limited than I have made it out to be. Indeed, legal scholars have applauded tech company efforts to shed light on surveillance through transparency reporting and First Amendment litigation.\footnote{See, e.g., Ashley Deeks, Can Tech Companies and Local Governments Mitigate Abuses of Government Secrecy?, LAWFARE (Dec. 3, 2020), https://www.lawfareblog.com/can-tech-companies-and-local-governments-mitigate-abuses-government-secrecy [https://perma.cc/PDSB-2N9W] (commending tech companies for “challeng[ing] and check[ing] executive conclusions”); Wexler, supra note 140, at 164–65 (praising tech companies for engaging in self-help); Hannah Bloch-Wehba, Process Without Procedure: National Security Letters and First Amendment Rights, 49 SUNY U. L. REV. 367, 379 (2016) (praising internet service providers for using individual rights issues as a defense to government compliance); Jonathan Manes, Online Service Providers and Surveillance Law Transparency, 125 YALE L.J.F. 343, 344 (2016) (observing that if online service providers pursued more extensive transparency, they would enhance public knowledge); Alan Z. Wexler, Surveillance Intermediaries, 70 STAN. L. REV. 99, 109 (2018) (describing how large communications intermediaries use transparency reports and information to “try to turn public opinion against government surveillance”).} But although these disclosure mechanisms certainly reduce secrecy, they ultimately reinforce the legal framework that confers control of information upon corporations. At their core, First Amendment challenges to government secrecy mandates argue that firms, not the state, ought to retain the option to disclose surveillance information.

In recent years, online platforms have begun to publish broader transparency reports that disclose, for example, data about automated takedowns of content.\footnote{Hannah Bloch-Wehba, Global Platform Governance: Private Power in the Shadow of the State, 72 SMU L. REV. 27, 49 (2019); Regulation 2021/784 of the European Parliament and of the Council of 29 April 2021 on Addressing the Dissemination of Terrorist Content Online, 2021 O.J. (L 172) 94–95 (requiring hosting service providers to disclose, among other things, information related to automated tools used to detect terrorist content).} Yet even as they voluntarily publish a wide variety of information in their transparency reports, tech firms have resisted the imposition of transparency mandates through law, suggesting that...
their beneficence has limits. When tech firms authorize disclosures of information, they do so in service of their claims to be acting in the public interest. Transparency reporting and legal efforts to seek permission to disclose information show that firms will wield their discretion and control over information in the interest of informing their users and the broader public. Transparency reporting is thus a self-imposed exception to the background norm of secrecy that bolsters companies’ claims that they are acting in service of the public interest.

By contrast, the second exception to secrecy that has emerged has garnered far less acclaim within the conference rooms of Silicon Valley. The rise of technology firms, and their embrace of secrecy default rules, has prompted an increasing number of tech workers to come forward with unauthorized disclosures of information. Rather than reaffirming tech firms’ control of information, whistleblowing and leaking are a direct challenge to that control. In turn, these disclosures have given rise to regulatory action, congressional hearings, and other initiatives that are sometimes quite discomfiting to tech firms.

III. WHISTLEBLOWING IN THE SHADOW OF THE LAW

This Part begins to account for how, in the absence of systematic regulation or reform, we actually do extract information from the technology industry: through leaks and whistleblowing. Many of the most significant technology policy issues of the day have come to light because of unauthorized disclosures by industry insiders. Amid a burgeoning tech worker movement, employees are increasingly airing the industry’s dirty laundry in public.


150 For discussion of the tech worker movement, see generally Anat Alon-Beck, Times They Are a-Changin’: When Tech Employees Revolt!, 80 Md. L. REV. 120 (2020), which discusses how tech employees are “revolting and demanding that their employers step up to the plate, redefine corporate purpose, and pursue long-term value while using a stakeholder lens”; Stavros Gadinis & Amelia Miazad, Corporate Law and Social Risk, 73 VAND. L. REV. 1401 (2020), which discusses the role of employees in corporate social accountability; Jennifer S. Fan, Employees as Regulators: The New Private Ordering in High Technology Companies, 2019 UTAH L. REV. 973, which observes tech workers’ ability to alter their employer’s behavior; and Bloch-Webha, supra note 23, which analyzes the impact tech workers have on constraining algorithmic governance.
Tech whistleblowing shapes legislative oversight at the federal and state levels, generating demand for policy reform. Leaked documents and information also play a critical role in media coverage and public opinion. Indeed, leaks are sometimes the only mechanism by which crucial information reaches regulators and the public.

This Part explores how information flows, via whistleblowers and leaks, to Congress, to regulators, and to the public. Section III.A summarizes how existing laws permit and shape whistleblowing activities. It argues that the current legal frameworks encourage disclosures about potential securities and labor law violations but tend to discourage other disclosures outside these domains. Section III.B examines whistleblowing activities outside the scope of formal protections: through leaks to lawmakers, the press, and the public. It argues that, despite the absence of formal statutory or common law protections, unauthorized disclosures often provide crucial information that stimulates legislative oversight, market responses, and public discussion.

A. Legally Sanctioned Whistleblowing

Why protect whistleblowers at all? One rationale is about effective law enforcement and regulation. As Professor Mary Lyndon puts it, technical advances have enabled firms to predict and observe risks that previously might have gone unnoticed.\textsuperscript{151} These advances turn information into a valuable commodity for industry, for scientific research, and for regulators, all of whom have competing interests in transparency and secrecy.\textsuperscript{152} For example, while “social, political, and market interests” in monitoring environmental and health risks have surged, firms also have “strong countervailing incentives to avoid” scrutiny and the potential liability and disclosure requirements that might result.\textsuperscript{153}

Technical and organizational complexity within firms also makes it easier to do wrong.\textsuperscript{154} Detecting and deterring “complex economic wrongdoing,” in Professor Pamela Bucy’s formulation, requires “inside


\textsuperscript{152} Id. at 470–71, 478; see also Bucy, supra note 37, at 940–41 (discussing the essential role of “private justice” in providing inside information to regulators).

\textsuperscript{153} Lyndon, supra note 151, at 471.

\textsuperscript{154} Bucy, supra note 37, at 940 (citing the “complex nature of economic crime and the diffuse nature of the business environment where such activity takes place” as reasons that wrongdoing might go undetected).
Insiders can “identify abuses that public regulators do not even know to look for.” Whistleblowers are not only essential to law enforcement; they are also important to broader regulatory programs. Inside information is frequently an “essential ingredient” or “key resource” that enables public agencies to carry out their regulatory goals. For example, in financial regulation, as Professor Christina Skinner has argued, whistleblower programs “help[] regulators overcome traditional asymmetries in information, expertise, and resources by leveraging private market actors.”

The labor and employment law literature offers a somewhat contrasting justification for whistleblower protections. Employment law views whistleblowing primarily as an exception to the at-will employment rule permitting employers to terminate or punish workers for any reason at all. As Professor Orly Lobel recounts, with the rise of labor and employment regulations, federal statutes also included “anti-retaliation provisions designed to enable employees to claim their rights without fear of retribution.” State statutes, too, often include whistleblower provisions that protect employees who report wrongdoing, although many states limit whistleblower protections to public employees. States also often “recognize some form of judicially created public policy exception” to the at-will employment rule, protecting individuals who report misconduct in the workplace.

As the following discussion shows, tech whistleblowing has utilized channels that reflect both the law enforcement and the labor rights perspectives.

1. Securities and Commodities Law

Tech workers—many represented by the nonprofit law firm Whistleblower Aid—have begun to use the antiretaliation provisions of the Dodd–Frank Act to report false and misleading corporate disclosures by

---

155 Pamela H. Bucy, Private Justice, 76 S. CAL. L. REV. 1, 5 (2002) (defining “inside information” as “significantly helpful information about economic wrongdoing produced by someone who has experience, insight, or contacts to, the industry or perpetrator involved”).

156 Bucy, supra note 37, at 941.

157 Bucy, supra note 155, at 8.

158 Skinner, supra note 24, at 917.

159 See supra text accompanying note 102.

160 Lobel, supra note 30, at 441.

161 Cherry, supra note 37, at 1045, 1047.

162 Id. at 1045.
publicly traded firms. Under the Dodd–Frank Act, individuals who provide “original information” relating to securities violations to the SEC are protected against retaliation by their employers. In addition to the antiretaliation provision, Dodd–Frank also created a bounty program at the SEC, ensuring that whistleblowers stand to reap a reward between 10% and 30% of the overall monetary sanctions collected if the final judgment exceeds $1 million. Dodd–Frank also permits whistleblowers to make anonymous submissions of information and bars the SEC from disclosing information that “could reasonably be expected to reveal” their identity.

Perhaps the foremost example of a tech worker making use of Dodd–Frank’s whistleblower provisions is Frances Haugen, the “Facebook whistleblower” who has argued that Facebook misled investors about the company’s role in propagating hate speech and misinformation, promoting human trafficking, harming teenage girls’ mental health, and more. Haugen took “tens of thousands of pages” of internal Facebook documents when she left the firm. Represented by law firm Whistleblower Aid, Haugen filed anonymous whistleblower submissions based on those documents with the SEC’s Office of the Whistleblower. She subsequently shared those documents with Congress as well as with journalists at the Wall Street Journal. But by sharing the documents with the SEC first, Haugen

---


165 Id. § 78u-6(b).
166 Id. § 78u-6(h)(2).

168 Pelley, supra note 163.

169 See supra Section II.B; see also Jeff Horwitz, Facebook to Curb Internal Debate over Sensitive Issues Amid Staff Discord, WALL. ST. J. (Sept. 17, 2020), https://www.wsj.com/articles/facebook-to-curb-internal-debate-over-sensitive-issues-amid-employee-discord-11600368481 [https://perma.cc/KB4-NP7B]; Horwitz, supra note 6; Wells, supra note 5 (discussing the publishing of Facebook’s files).
qualified for the antiretaliation provisions of Dodd–Frank and shielded herself from retaliation by Facebook. After she went public, Haugen also testified before congressional subcommittees and the UK Parliament.

Although the SEC whistleblower program protects anonymity, Haugen is not the only tech whistleblower to “out” herself after ensuring that she would qualify for statutory protection. In 2022, while Twitter was embroiled in a legal dispute with Elon Musk about his agreement to buy the company, Peiter Zatko (aka Mudge), the company’s former head of security, filed a whistleblower complaint with the SEC. Mudge’s complaint set forth a litany of data security and privacy lapses within the company, including accusations that Twitter had violated a 2011 settlement with the FTC that had required the company to implement a “comprehensive information security program.”

Like Haugen, Mudge touched off a wave of congressional activity and regulatory oversight by blowing the whistle. In the wake of Mudge’s disclosures, he, too, shared the information with Congress and appeared to testify before the Senate. Senators Chuck Grassley and Richard Blumenthal both raised concerns about the FTC’s capacity to enforce its consent decree. The FTC, meanwhile, reportedly opened an inquiry into Twitter’s compliance with the 2011 order. A second Twitter whistleblower

---


172 Menn et al., supra note 163.


told Congress in January 2023 that the firm’s privacy and security practices continued to be inconsistent with its legal obligations.177 Although SEC whistleblowing appears increasingly common, other financial regulatory agencies also maintain whistleblower programs that incentivize insiders to come forward. The Commodity Futures Trading Commission (CFTC), for example, accepts whistleblower tips under the Commodities Exchange Act in a program that, like the SEC whistleblower program, offers both protections against retaliation and rewards.178 In May 2019, the CFTC posted a “Whistleblower Alert” to encourage individuals to “be on the lookout” for virtual currency fraud.179 In the fall of 2022, as cryptocurrency company FTX was imploding, CFTC Commissioner Kristin Johnson called for “vocal whistleblowers and tipsters” to share information with the agency about cryptocurrency fraud.180 *Bloomberg* reported that the “opaqueness” of cryptocurrency and digital assets made whistleblowing even more crucial to offset the significant information asymmetries between the industry and regulators.

### 2. Labor Law
As tech workers, alongside movements for racial and social justice, are increasingly mobilizing in the workplace, they have also taken advantage of labor law’s protections for worker speech.181 Some federal statutes governing labor and the workplace, including the NLRA, the Fair Labor Standards Act (FLSA), and the Occupational Safety and Health (OSH) Act, incorporate explicit whistleblower protections that protect workers who report violations

---


from retaliation. Other protections offer broader support for speech in connection with workplace advocacy.

Statutory whistleblower protections are critically important, but they are also structurally flawed. The OSH Act protects employees from retaliation if they complain about violations internally or if they file a complaint with the Occupational Safety and Health Administration (OSHA). But a 1997 audit report by the Department of Labor found that “nearly 82 percent of the workers who had asked their employers to correct safety/health hazards stated that they were subsequently fired in retaliation for complaining.” OSHA is also “so understaffed it can take years for complaints to be investigated.” And gig workers who are independent contractors do not qualify for whistleblower protection under the OSH Act, which protects only “employee[s].” The result is that, in practice, workers know that they can be fired with impunity. Not surprisingly, this knowledge deters internal complaints. As one former safety inspector at an Amazon facility put it after being fired for reporting safety problems, “it’s hard to find employment when you’ve been branded as the whistleblower.”

OSHA’s protections have become particularly salient during the COVID-19 pandemic, as workplace safety issues for warehouse personnel became a rallying point for Amazon workers. Amid widespread supply chain hiccups, demand for online shopping soared and warehouse workers were concerned about exposure to coronavirus and leave policies.

---

182 29 U.S.C. § 158(a)(4) (defining it as an “unfair labor practice” to retaliate against employees who file charges under the NLRA); id. § 215(a)(3) (prohibiting retaliation against employees who file complaints or participate in proceedings under the FLSA); id. § 660(c)(1) (prohibiting retaliation against employees who file complaints or participate in proceedings under the OSH Act).
183 Id. § 660(c)(1).
186 29 U.S.C. § 660(c)(1); see also Miriam H. Cherry, Employment Status for “Essential Workers”:
The Case for Gig Worker Parity, 55 LOY. L.A. L. REV. 683, 700–01 (2022) (noting that gig workers are not fired in the traditional sense of employment but are rather “deactivated,” which is potentially worse than being fired).
187 Hernández, supra note 185.
188 Kate Conger, Senators Want to Know if Amazon Retaliated Against Whistle-Blowers, N.Y. TIMES (May 11, 2020), https://www.nyt.com/2020/05/07/technology/amazon-coronavirus-whistleblowers.html [https://perma.cc/7955-2JBR].
Some workers participated in walkouts, strikes, and protests, urging their employers to adopt safer policies.190

In March and April 2020, Amazon fired Chris Smalls and Bashir Mohamed, warehouse workers who had raised concerns about coronavirus measures and become active in organizing.191 Smalls and Mohamed, who worked at warehouses in New York and Minnesota, respectively, were both fired for violating social distancing guidelines—allegations they each disputed as the reason for their firing. Instead, each argued that they had been fired for speaking to their colleagues and advocating for safer policies. Lawmakers were concerned that the company was leveraging its power to retaliate against whistleblowers who had raised valid concerns about workplace hazards.192 Some state lawmakers, for their part, have proposed or adopted broader whistleblower protections in the wake of COVID-19.193

Sections 7 and 8 of the NLRA create somewhat broader protections that are also reshaping tech worker advocacy. Under Section 7, the NLRA confers the right to engage in “concerted activities for the purpose of . . . mutual aid or protection.”194 Section 8(a)(1) makes it an “unfair labor practice” to “interfere with, restrain, or coerce” employees exercising their Section 7 rights.195 “Mutual aid or protection” means that organizing must relate to the “terms and conditions of employment” to be considered a protected “concerted activity.”196 To be protected, a “concerted activity”

---

190 Dickerson, supra note 189, at 188 (“While some individual worker groups staged walkouts during the pandemic to protest unsafe working conditions, worker bargaining power has eroded since the 1980s.”).


193 Hernández, supra note 185.


195 Id. § 158(a)(1).

must have a sufficiently “immediate relationship to employees’ interests as employees.”197 “Purely political protests” do not qualify.198

As Professor Cynthia Estlund has described it, the NLRA protects worker speech that seeks to advance worker interests “as employees,” which are interests that relate—whether directly or indirectly—to their own conditions of employment.199 Estlund has criticized this focus on “particular work-related grievances” as overly restrictive of worker rights and untethered from the original understanding of the phrase “mutual aid or protection.”200 As Estlund puts it, “surely employees do have a genuine interest as employees in the quality of what they collectively produce.”201

Current labor movements in tech confirm Estlund’s observation that workers are concerned with how their work product might be leveraged for political causes with which they disagree. For example, the Trump Administration’s contracts with tech companies from Microsoft to Palantir and beyond touched off a wave of worker opposition on the basis that the contracts might be used to oppress immigrants and communities of color.202 A series of high-profile controversies about contracts with law enforcement and national security agencies have spurred worker unrest and mobilization along with calls for a more democratic workplace.203

These examples illustrate how the NLRA’s protections for “concerted activity” have encouraged tech workers to engage in workplace organizing in conjunction with advocacy on “political” issues that are perhaps more

---

197 Estess, 437 U.S. at 567 –68 (emphasis added).
199 Cynthia L. Estlund, What Do Workers Want? Employee Interests, Public Interests, and Freedom of Expression Under the National Labor Relations Act, 140 U. PA. L. REV. 921, 938 – 39 (1992) (discussing cases in which “employee criticism” has been found too “attenuated” from the conditions of employment to be protected under Section 7); see also Richard Michael Fischl, Self, Others, and Section 7: Mutualism and Protected Protest Activities Under the National Labor Relations Act, 89 COLUM. L. REV. 789, 796 –97 (1989) (discussing how the NLRB and the courts have interpreted the requirement of “mutual aid and protection”).
200 Estlund, supra note 199, at 942 – 49.
201 Id. at 949.
“attenuated” from work conditions. Consider, for example, Google’s firing of several activist workers who were critical of the company’s contracts with Customs and Border Protection. The activists said that they were terminated in retaliation for their activities to “help organize our colleagues, to work together for a better, safer, fairer, and more ethical workplace”—in other words, in retaliation for engaging in concerted activity for their mutual aid and protection. The activists explicitly connected how Google’s business choices and policies, from AI ethics to content policy to sexual harassment, impacted their own workplace. Google, for its part, said the workers had violated “data security policies” that forbade them from accessing, among other things, other employees’ materials and work. One worker was fired for creating a code-based pop-up that said “Googlers have the right to participate in protected concerted activities.” Google ultimately settled with all of the workers under a confidential agreement in 2022.

To understand the line between unprotected “political” advocacy and protected concerted activity to improve working conditions, consider Amazon workers’ experience advocating for climate justice. In 2019, over one thousand Amazon employees walked out of the company’s office in protest of the company’s contributions to the climate crisis. Amazon Employees for Climate Justice (AECJ), a worker group devoted to climate advocacy, called on the company to commit to zero emissions by 2030 and to end contracts providing Amazon Web Services to “fossil fuel companies

---


207 Id. (“We spoke up when we saw Google making unethical business decisions that create a workplace that is harmful to us and our colleagues.”).


209 Id.

210 Id.
to accelerate oil and gas extraction.” AECJ members were not alone in their discontent: thousands of tech workers across disparate firms walked out of their workplaces to demonstrate against the industry’s dismal track record.

Continued employee advocacy on climate issues prompted Amazon to crack down on worker expression. AECJ leaders went on the record with the Washington Post to criticize the company’s continued partnerships with the oil and gas industry. In November 2019, AECJ leaders Maren Costa, Emily Cunningham, and Jamie Kowalski were notified that they had violated Amazon’s “external communications policy” by speaking to reporters and posting on social media about the company’s climate impact. That policy required employees to get approval from Amazon’s public relations department before speaking externally about “Amazon’s business, products, services, technology, or customers.” Amazon warned at least some of these employees that violating these policies could lead to termination.

In response, AECJ members began violating the communications policy en masse, denouncing their employer’s efforts at intimidation.

AECJ’s climate advocacy arguably had little to do with “working conditions” and therefore might have been unprotected under the NLRA. Nonetheless, the company tolerated the advocacy even as workers violated internal rules and policies. Amazon only began to crack down on AECJ’s advocacy when, a few months later and with COVID-19 circulating, Amazon warehouse workers began raising concerns about health and safety issues. The warehouse workers reached out to Cunningham and Costa for help and

---


214 Id.


216 Greene, supra note 213.

advice. Cunningham and Costa both circulated a petition inside Amazon in support of warehouse workers and also tweeted that they would match donations to a fund in support of warehouse workers. Both were fired in April 2020, around the same time that Amazon also fired Chris Smalls and Bashir Mohamed, the warehouse organizers.

In March 2021, the NLRB issued an advice memorandum concluding that Amazon had unlawfully terminated Costa and Cunningham. The memorandum concluded that the Board “need not reach the question of whether [Costa’s and Cunningham’s] climate activism was protected” because they had engaged in an “act of classic collective action,” leading “hundreds of highly skilled tech employees with demonstrated power to join forces with the warehouse movement, comprised of thousands of employees who have remained largely voiceless thus far.” Even though Costa and Cunningham were ultimately vindicated, the narrowness of their victory is noteworthy. After all, it was not their advocacy on climate justice that was protected, but their advocacy in support of warehouse workers’ conditions. Amazon settled with them in September 2021.

B. Whistleblowing Without Protections

The foregoing Sections illustrated how, in two separate domains—securities law and labor law—the law creates exceptions to the rule that workers can be penalized and even fired for “a good reason, a bad reason, or no reason at all.” And these statutory whistleblower protections do not stand alone: the tort of wrongful termination against public policy also limits employers’ ability to fire workers who are engaged in “publicly beneficial activities, such as whistleblowing.”

---


220 Conger, supra note 188.


222 Id. at 7–8.


224 Racabi, supra note 98, at 94.

225 Lobel, supra note 30, at 442; Racabi, supra note 98, at 101.
But in many domains, there is no statutory protection, and common law protection is uncertain at best. Workers who choose to blow the whistle outside of existing legal channels thus operate under the shadow of the rules that their employers impose: NDAs, data security and communications policies, and limitations on disclosing corporate information. Without antiretaliation provisions, workers who choose to blow the whistle take on serious legal, reputational, and financial risk. If the ineffectiveness of existing protections deters workers from using established channels to blow the whistle, the total absence of protection is likely to aggravate that chilling effect, especially in light of well-known examples of retaliation.

Still, many tech workers blow the whistle with no protections at all. Consider, for example, the story of Christopher Wylie. In March 2018, the Guardian and Observer published a story about an app, thisisyourdigitallife, through which “hundreds of thousands of users were paid to take a personality test and agreed to have their data collected for academic use.”

Unbeknownst to users, the app harvested data not only from the users who took the test but also from their Facebook friends. Cambridge Analytica, which was run by Trump strategist Steve Bannon, then used the harvested data to target users with political advertising.

The Guardian story rested in substantial part on disclosures by Christopher Wylie, a former Cambridge Analytica employee who violated his nondisclosure agreement with his former employer to go public. Wylie claimed to have come up with the idea to use psychological targeting in political strategy. In order to acquire the data necessary to do the targeting, Cambridge Analytica entered into an agreement with Aleksandr Kogan, a Cambridge academic whose research firm, Global Science Research, would harvest the data. Wylie provided this agreement to the Guardian, along with bank records and receipts. Although it was widely known that “Facebook

---

226 Racabi, supra note 98, at 101.

227 Id. at 102 (describing how the default rule of employment at will is “a crucial factor of control” and a source of “employers’ ability to dominate and coerce their workers”); see also Bhuiyan, supra note 17 (discussing examples of Timnit Gebru, the “Thanksgiving Four” fired from Google, and the climate activists terminated by Amazon); Ghaffary, supra note 17 (discussing high-profile whistleblowers and their firings).


230 Cadwalladr, supra note 1.

231 Id.
data obtained without users’ knowledge was being exploited by Cambridge Analytica on behalf of right-wing candidates in the United States and the United Kingdom, Wylie’s information undermined Cambridge Analytica and Facebook’s claims that nothing untoward had taken place.\textsuperscript{232}

Wylie’s disclosures prompted a significant public reaction. Although aspects of Cambridge Analytica’s use of Facebook data had been known, Wylie’s disclosures (and those of other unnamed “former employees and contractors”) fostered both a livelier public debate and a greater interest in oversight.\textsuperscript{233} Facebook Chief Security Officer Alex Stamos reportedly departed the company in part because of clashes with top executives regarding how best to address the platform’s vulnerability to disinformation.\textsuperscript{234} The hashtag #DeleteFacebook began trending on Twitter.\textsuperscript{235} The company’s stock took an enormous dive.\textsuperscript{236}

Congress and federal regulators also sprang into action. Multiple congressional committees convened hearings in the wake of the Cambridge Analytica scandal. In April 2018, Facebook CEO Mark Zuckerberg testified before a joint hearing of the Senate Commerce and Judiciary Committees, at which numerous senators grilled him about the company’s commitment to privacy and its plans to crack down on third-party apps.\textsuperscript{237} House Democrats interviewed Christopher Wylie, who also testified before the Senate Judiciary Committee in May 2018.\textsuperscript{238}

\begin{footnotes}
\item[233] See id. (noting that major news publications were aware of the Facebook and Cambridge Analytica practice of using user data); Rosenberg & Frenkel, supra note 229.
\item[236] Halpern, supra note 232.
\end{footnotes}
Wylie’s disclosures also prompted regulatory action. The FTC sued Cambridge Analytica and settled complaints against Kogan and Alexander Nix, the former Cambridge Analytica CEO. The FTC also sued Facebook for violating a 2012 consent decree about user privacy. In a historic settlement, the FTC ordered Facebook to pay $5 billion, the largest settlement ever so ordered. The settlement also required Facebook to implement a “comprehensive privacy program” and obtain regular independent assessments of the program. At the corporate-governance level, the company was ordered to create an Independent Privacy Committee and designate “compliance officers” for the privacy program who could only be removed by the Independent Committee.

Wylie is far from the only tech industry insider to have come forward with information of public concern. Consider Project Dragonfly, Google’s plan to “launch a censored search engine for China.” Google had very publicly pulled out of the Chinese market in 2010 after it said that hackers had attempted to gain access to the Gmail accounts of human rights activists. In August 2018, however, the Intercept published leaked documents showing that the company was developing a prototype of a search engine that would be engineered for compliance with the “Great Firewall.” Predictably, backlash ensued. Over a thousand Google employees signed onto a letter of protest. A handful of Google workers resigned over the ethical and transparency issues raised by the company’s secret development of such a controversial product. In November 2018, 20,000 Google employees walked off the job in protest of the Project Dragonfly.
Maven—a contract with the Department of Defense to supply computer vision to aid in bomb strikes—and the company’s sexual harassment policies.\(^{248}\) (Google later fired some of the participants of the walkout and then settled after these participants challenged their firings at the NLRB.)\(^{249}\)

But the backlash was not restricted to the company itself. In the days after the Project Dragonfly disclosures, six Senators sent a letter to Google CEO Sundar Pichai demanding more information about the plan to develop a censored search engine and asking specific questions about the company’s plans and operations.\(^{250}\) Pichai responded a few weeks later in a two-page letter that failed to answer any of the questions.\(^{251}\) In September 2018, Jack Poulson, a former research scientist at Google who had quit in protest after learning of Project Dragonfly, wrote to the members of the Senate Commerce Committee with some additional information and a request.\(^{252}\) Poulson asked the Committee to press Google’s representative, Keith Enright, on Project Dragonfly’s implications for privacy, censorship, and human rights.\(^{253}\) In congressional hearings and private meetings, lawmakers grilled Google’s executives again and again on its plans to enter the Chinese market.\(^{254}\) For his part, Poulson started the nonprofit Tech Inquiry, which

“maps out relationships between companies, nonprofits, and governments to better contextualize and investigate corporate influence.”

Or consider the experience of Ifeoma Ozoma and Aerica Shimizu Banks, the two former Pinterest employees who violated their nondisclosure agreements with the company to come forward with claims of racism, sexism, and pay discrimination. Although Title VII, the federal law prohibiting discrimination based on race, gender, and sex, includes whistleblower protections, the provision would not protect Ozoma and Bank’s disclosures: it only shelters current employees from retaliation by employers if they disclose violations in an official “investigation, proceeding, or hearing.”

If Ozoma and Banks had made their disclosures to the EEOC in conjunction with an official investigation, their nondisclosure agreement would have been unenforceable. Because they went public, the whistleblower protection provision did not apply to them. They went public anyway. Ozoma took a leading role in advocating for California’s Silenced No More Act, which bars firms from using nondisclosure agreements to limit discussion of sexual harassment in settlement agreements. In Washington, former Apple worker Cher Scarlett led efforts to introduce that state’s Silenced No More Act. Like Poulson, Ozoma and Scarlett have become leading voices in tech accountability circles because of their role in reforming secrecy practices.

A final example: in November 2020, Google fired Timnit Gebru, a leader of the company’s Ethical AI team. Gebru had cowritten a research paper on the perils of large language models in AI—the kind of model that
supports Google’s search engine functionality. Google had asked Gebru to retract the paper or remove her name after it was submitted to the Association for Computing Machinery Conference on Fairness, Accountability, and Transparency. When Gebru balked, she was fired—although Google maintains she resigned. Another coleader of the Ethical AI team, Margaret Mitchell, was listed on the paper as “Shmargaret Shmitchell” after Google required her to remove her name from the authors list. A few months later, Mitchell was fired as well. Google asserted that Mitchell had moved files outside of the firm’s computer system in violation of its security policy.

Gebru and Mitchell’s firings prompted a broader discussion about whistleblower protections in tech. From Gebru’s perspective, her firing showed the impossibility of challenging tech company narratives from within firms. Without whistleblower protections, she argued, firms would silence and retaliate against dissenting voices.

The asymmetric power of tech firms is particularly significant in the context of AI development because a small handful of firms are responsible for a large amount of AI research and development. Because many AI/ML researchers work in technology firms rather than in academia, the power of firms to control narratives—and worker speech—about AI/ML is perhaps particularly acute. One of Gebru’s coauthors, University of Washington

---


264 Id.


267 Id.

268 See Alicia Solow-Niederman, Information Privacy and the Inference Economy, 117 NW. U. L. REV. 357, 392 (2022) (arguing that concentration of “computing power of the necessary magnitude” to develop artificial intelligence “risks centralizing ML development in platform firms”); see also Solow-Niederman, supra note 22, at 676 (explaining that federal investment in research and development for AI “amounts to a small fraction of what private firms have invested”).

269 Hao, supra note 262.
Professor Emily Bender, put it bluntly, saying that Gebru’s firing “underscore[d] the value of academic freedom.”

The absence of broad protections for tech workers is important because the prospect of legal liability affects how workers decide whether to go public with their concerns. Beyond the substance of whistleblower protections, the procedural and structural aspects of existing whistleblower protections also shape (and deter) worker disclosures. The existing rules of whistleblower protection systematically encourage some kinds of disclosures and discourage others. Significant gaps and omissions have, accordingly, informed emerging efforts to strengthen worker speech rights and weaken corporate secrecy practices.

IV. THE BENEFITS AND DRAWBACKS OF WHISTLEBLOWING

So far, this Article has shown that the ascent of the information economy has brought with it major challenges for democratic governance and public knowledge. Against a background of broad secrecy, unauthorized leaks of information from tech company insiders play an essential role in oversight and accountability efforts.

This Part builds on the descriptive foundation I laid in the preceding pages to consider the benefits and costs of whistleblowing for tech accountability and transparency. Whistleblower disclosures provide valuable sources of insight into problematic dynamics that are otherwise largely invisible to lawmakers and regulators. And they serve to challenge the broad assertions of secrecy that have become commonplace in the technology industry. But whistleblowing is also a woefully underinclusive way of ensuring that crucial information about tech firms reaches an appropriate audience. And broadening whistleblower protections might also invite abuse and weaponization, as I discuss in more detail below.

270 Id.
A. Detecting Wrongdoing

One key justification for whistleblowing is that it helps ensure that law enforcement and regulatory agencies have the information that they need to carry out their functions.\(^\text{273}\) And indeed, many of the disclosures outlined in the previous Part did facilitate regulatory oversight and enforcement. When Christopher Wylie blew the whistle on Cambridge Analytica, for example, his disclosures not only prompted legislative hearings across multiple jurisdictions but also touched off multiple enforcement actions by the FTC.\(^\text{274}\) The NLRB reviewed Google employees’ allegations of impermissible retaliation, leading to settlements.\(^\text{275}\) Beyond agency action, whistleblowing also leads to normative and market-based effects, as the public learns of wrongdoing and reacts. For instance, news of Facebook’s cooperation with Cambridge Analytica prompted users to abandon the platform.\(^\text{276}\)

But even if insider information is helpful and necessary for enforcement and oversight, whistleblowing is not an ideal mechanism for extracting information. For one, few people blow the whistle, at least externally, because the costs of whistleblowing are so high.\(^\text{277}\) It is likely (though virtually impossible to prove) that for every whistleblower disclosure there is another episode of misconduct or wrongdoing that never reaches the public eye. Antiretaliation provisions and incentives are intended to reduce these obstacles. But “cultural transformation is not easily legislated.”\(^\text{278}\) Even if the law offered bulletproof legal protections and incentives, there would remain serious social and cultural obstacles to enhancing whistleblowing activity.\(^\text{279}\) The significant personal, financial, and professional costs of whistleblowing, and the cultural norms that frown on “going public” with concerns, might outweigh any protections that the law could offer.\(^\text{280}\)

\(^{273}\) See supra Section II.A.

\(^{274}\) See supra text accompanying notes 228–242 (describing Christopher Wylie and the Cambridge Analytica leaks).

\(^{275}\) Roth, supra note 209.

\(^{276}\) Hsa, supra note 235.

\(^{277}\) See Fred H. Alford, Whistleblowers: Broken Lives and Organizational Power 18–20 (2001) (contending that most whistleblower interviewees with whom the author spoke lost their jobs, careers, and houses); Miriam H. Baer, Recategorizing the Whistleblower’s Dilemma, 50 U.C. Davis L. Rev. 2215, 2220 (2017) (discussing how complicit employees may fear disclosure due to the increased risk of criminal punishment).

\(^{278}\) Estlund, supra note 98, at 110.

\(^{279}\) Alford, supra note 277, at 18–20.

\(^{280}\) See Mark Keil & Daniel Robey, Blowing the Whistle on Troubled Software Projects, 44 Comm’ns ACM 87, 88, 90 (2001); David P. Billington, Discipline and Play: The Art of Engineering, in ETHICS, POLITICS, AND WHISTLEBLOWING IN ENGINEERING 57, 69 (Nicholas Sakellariou & Rania Milleron eds., 2019) (“Engineers who blow the whistle are truly courageous people who are taking
Bounty rewards systems, such as the SEC whistleblower program, are intended to overcome these obstacles to disclosure.\footnote{Matt A. Vega, Beyond Incentives: Making Corporate Whistleblowing Moral in the New Era of Dodd-Frank Act “Bounty Hunting,” 45 CONN. L. REV. 483, 507, 513 (2012).} But bounties may present the opposite risk: by incentivizing disclosure through (sometimes massive) financial rewards, the program might “encourage employee opportunism . . . and become a sort of self-fulfilling prophecy.”\footnote{Id. at 509.} In one study of the relative impact of antiretaliation provisions, bounties, reporting mandates, and liability fines, Professors Orly Lobel and Yuval Feldman found that sufficiently large bounties can encourage whistleblowing even when the underlying conduct is not particularly severe, suggesting that bounties might err too far in the other direction by over-incentivizing disclosure.\footnote{Feldman & Lobel, supra note 178, at 1154, 1204.}

While more disclosure might seem like a good thing, incentivizing too many disclosures could have negative results. First, assuming that investigative resources are scarce, an uptick in the number of disclosures may result in lengthier investigations or fewer resources being devoted to investigation. This has been the experience at OSHA, for example, where the agency is understaffed relative to the number of complaints it receives.\footnote{See supra note 102 and accompanying text.} Moreover, at least some whistleblowers may not be motivated by the potential bounty and instead might use the antiretaliation provisions of whistleblower statutes as shelter to disclose information that is not evidence of wrongdoing and not relevant to enforcement efforts.

More generally, the patchy distribution of whistleblower protections produces uneven disclosures. If sectoral protections exist for fraud but not for data security or privacy breaches, we are systemically more likely to learn about fraud than breaches. This means that whistleblowing is potentially both over- and underinclusive as a mechanism for ferreting out information about wrongdoing from within firms. On the one hand, the social, cultural, and professional costs of blowing the whistle likely deter many individuals from coming forward with valuable information that Congress has not deemed sufficiently worthy of protection. On the other hand, the financial rewards of doing so likely encourage individuals to come forward with information that otherwise might seem unproblematic.
B. Spurring Legislative Action

Whistleblowing can also generate legislative action and help propel the development of the law, as dynamics that had previously gone unnoticed are made politically and legally salient. Whistleblower disclosures make corporate wrongdoing concrete, salient, and accessible to lawmakers. In this respect they resemble a form of “fire alarm” oversight in which third parties alert lawmakers to an issue of concern, prompting scrutiny. Whistleblower disclosures make corporate wrongdoing concrete, salient, and accessible to lawmakers. In this respect they resemble a form of “fire alarm” oversight in which third parties alert lawmakers to an issue of concern, prompting scrutiny. Fire alarms rely on “individual citizens and organized interest groups to examine administrative decisions . . . , to charge executive agencies with violating congressional goals, and to seek remedies” for those violations. Fire alarms are distinct from “police-patrol oversight,” which occurs when, “at its own initiative, Congress examines a sample of executive-agency activities, with the aim of detecting and remediying any violations of legislative goals.” In their influential paper conceptualizing the two models, political scientists Mathew McCubbins and Thomas Schwartz contend that members of Congress rationally preferred fire alarm oversight over the police-patrol model in part because it was more effective.

The parade of hearings that followed disclosures by Haugen, Mudge, Wylie, and others illustrates how lawmakers respond to whistleblower disclosures with oversight hearings. I am not the first to suggest that whistleblowing and leaking might contribute to oversight by Congress. More generally, whistleblowers play a role as fire alarms in multiple contexts in which decision-makers might act in response to disclosure of potential wrongdoing. Whistleblowing acutely highlights wrongdoing that might otherwise escape scrutiny and thus generates reactions by oversight agencies, markets, and lawmakers.

Whistleblowing’s fire alarm role is notable in part because a persistent shibboleth in tech policy circles concerns how law and regulation “lag

---

286 Id.
287 Id.
288 Id. at 171, 176.
289 See supra Part III (discussing how Congress reacted to public disclosures).
291 Though McCubbins and Schwartz’s model was developed to explain how lawmakers conducted agency oversight, the “fire alarm” metaphor has since been expanded to other contexts in which oversight responds to an acute stimulus. See, e.g., David Orozco, Compliance by Fire Alarm: Regulatory Oversight Through Information Feedback Loops, 46 J. CORP. L. 97, 131 (2020) (“Whistleblowers are an important information feedback loop within the compliance system that connect regulators and executives and act as a powerful fire-alarm.”).
behind” technological developments. Critics of the perceived “gap” between technology and law have argued that legislatures address issues only “as a function of headlines and perceived political urgency and expediency.” There is an element of truth to this: the complaint largely reflects the congressional preference for fire alarm oversight.

But that is a feature, not a bug, of fire alarm oversight. At least arguably, the fire alarm function of whistleblower disclosures generates legislative proposals that are timely, concrete, and actionable. For example, the experience of Pinterest whistleblowers Ifeoma Ozoma and Aerica Banks prompted California to adopt the Silenced No More Act. Following advocacy from Apple workers, Washington also adopted the act in 2022. Despite these victories, to the extent lawmakers depend on individuals to reveal problematic dynamics and practices, reactive lawmaking may also miss important opportunities for legal development and change.

At the same time, broadening whistleblower protections could create significant costs by enabling more actors inside and outside the legislature to weaponize whistleblower disclosures for politically motivated ends. Consider how the U.S. House of Representatives Committee on the Judiciary’s Select Subcommittee on the Weaponization of the Federal Government has selectively embraced leaked information to argue that social media platforms and the government have colluded to suppress protected speech. In particular, the Subcommittee has relied on internal Twitter documents leaked to and selectively published by a handful of “cherry-picked” commentators as evidence of ideological bias and conservative

292 Crootof & Ard, supra note 69, at 359.
294 See supra text accompanying notes 256–259.
Censorship. While the Subcommittee appears not to have produced any evidence of actual wrongdoing, they have issued subpoenas and legal threats to university researchers and consortia working on issues related to election and health misinformation and disinformation. Broadening transparency and access to information from within the industry could heighten these theatrics and amplify real risks to researchers, individuals, and the industry.

C. Equity Considerations

On one view, perhaps the willingness of whistleblowers such as Wylie, Banks, and Ozoma to come forward in violation of their nondisclosure agreements illustrates that reform—whether through ex ante restrictions on the appropriate scope of nondisclosure agreements, or ex post limitations on enforcement—is unnecessary. After all, the thinking might go, clearly individuals are willing to violate these constraints when the stakes are high enough. Moreover, as Hoffman and Lampmann note, “all courts agree that NDAs which prohibit speech, notwithstanding a legal duty to disclose . . . are void.” From this perspective, the law already ensures that legally mandated disclosures will not be obstructed by contractual secrecy requirements. And individuals may still make disclosures even in violation of contractual secrecy requirements if they deem the disclosures sufficiently important.

But this view overlooks the substantial social, personal, and economic penalties that confront would-be whistleblowers. For one, Wylie, Banks, and Ozoma had all already left their employers by the time they made their disclosures. But for current employees, the prospect of being fired and losing a paycheck is real. Consider how Apple has reacted to employee activism on environmental issues and gender equality. In 2021, the company fired Ashley Gjøvik, a former program manager who had raised concerns about workplace surveillance, harassment, bullying, and environmental safety at an Apple office located on a former Superfund site. Apple asserted that

---


Gjøvik had leaked confidential information in violation of the company’s policies; Gjøvik claimed that the company had retaliated in response to her concerns about working conditions.\footnote{Schiffer, supra note 300.} The following month, Apple fired Janneke Parrish, who had led #AppleToo, an employee group that collected stories from Apple workers “describing verbal abuse, sexual harassment, retaliation and discrimination at work.”\footnote{Kellen Browning, Another Apple Worker Says the Company Retaliated Against Her, N.Y. TIMES (Nov. 2, 2021), https://www.nytimes.com/2021/11/02/technology/apple-worker-retaliation.html [https://perma.cc/MWG7-EZQK].}

The likelihood that someone will violate a nondisclosure agreement or other corporate policy depends on what they have to lose. For a worker who is “neither uncommonly brave nor litigious, whose job is crucially important to her and her family, and who is guided in her actions by expectations about the consequences of those actions,” the prospect of being summarily fired is likely to deter knowing or outright violations of a nondisclosure agreement or other corporate policy.\footnote{Estlund, supra note 271, at 103.} By contrast, as Estlund puts it, even the “prospect of liability” for wrongful discharge is unlikely to discourage employers from retaliating against workers who speak out because employers know that retaliation may deter other workers—and those workers, too, are unlikely to seek legal redress.\footnote{Id. at 104.}

Empirical research confirms that the burden of whistleblowing is not evenly distributed. In 1988, whistleblowing scholars Marcia Miceli and Janet Near described how group insiders who conform to organizational norms and who are perceived as experienced and competent may be “less likely to experience retaliation and, therefore, should feel freer than other members to blow the whistle.”\footnote{Marcia P. Miceli & Janet P. Near, Individual and Situational Correlates of Whistle-Blowing, 41 PERS. PSYCH. 267, 270 (1988).} Miceli and Near suggest that insiders “with longer work histories, (i.e., those who may be viewed as competent, or whites and males) . . . may be more likely to blow the whistle.”\footnote{Id. at 270–71.} Later evidence has found, however, that women are “far more likely than men to blow the whistle.”\footnote{Feldman & Lobel, supra note 178, at 1196.} But women also considered antiretaliation protections to be more important than did men and “cared more about maintaining anonymity” than did men.\footnote{Id. at 1197.} Feldman and Lobel attribute this discrepancy to the possibility that women experienced lower job security than men.\footnote{Id.} That finding is
consistent with later work by Miceli and Near, along with coauthors, which found that being a female whistleblower “was associated with retaliation.”

The costs of whistleblowing matter because they discourage many ethically minded people from going public with their concerns. These costs might not matter to the Facebook whistleblower Frances Haugen, who “has her own financial resources” because she bought “crypto at the right time.” But for many others, the absence of incentives and protections is a significant deterrent from coming forward. These distributional realities exacerbate the problem of selective disclosure, making it more likely not only that oversight agencies will hear about only certain kinds of issues but also that they will hear from only certain kinds of people.

D. Potential Reforms

The previous three Sections illustrated that, at least compared to holistic transparency and accountability mandates, whistleblowing may well be an underinclusive, and even undemocratic, way of extracting information from private entities. Whistleblowing depends on self-appointed, unelected individuals to choose which kinds of corporate wrongdoing are of potential concern—and to bring those practices into the light. At both a systemic and an individual level, this is a costly way of getting information into the open. Not surprisingly, reliance on whistleblowers leads to significant knowledge gaps.

The answer is not to limit protections for whistleblowing, but to broaden and refine them. This Section situates the role of whistleblowing within the overall ecosystem of tech transparency and accountability. I argue that protections for whistleblowing are a necessary component of systemic regulation of the technology sector.

1. Incorporating Whistleblower Protections into the Regulation of Platforms and Algorithms

New legislative proposals consider various mechanisms for promoting the transparency and accountability of informationally intensive economic activity. In recent years, dozens of laws at the state and federal level have

312 See RAHUL SAGAR, SECRETS AND LEAKS 114 (2014) (“[W]hen unauthorized disclosures occur, vital decisions on matters of national security are effectively being made by private actors, an outcome that violates the democratic ideal that such decisions should be made by persons or institutions that have been directly or indirectly endorsed by citizens.”).
been proposed or enacted to govern social media platforms, often with an explicitly partisan bent. For instance, Florida and Texas have each enacted laws imposing disclosure requirements on large online platforms. At the federal level, the Platform Accountability and Transparency Act would provide researcher access to data and information from within large social media platforms.

Algorithmic governance has come in for similar scrutiny. The Algorithmic Accountability Act, for instance, would require private entities that use automated decision systems in “critical” decisions to conduct impact assessments. And a New York City law that took effect on January 1, 2023 requires employers to conduct “bias audits” if they use automated decision systems for making employment decisions.

Each of these proposals embrace an approach to regulation that is to some extent transparency-oriented. And, with the exception of the Florida and Texas laws, each is characterized to some extent by its resemblance to “new governance” or “collaborative governance,” models of regulation that are meant to be more “dynamic, reflexive, and flexible” than their command-and-control predecessors. In short, “new” and “collaborative” governance models anticipate a broader role for private stakeholders, including industry, to facilitate modes of regulation and oversight that would not be possible without cooperation and partnership. Exemplifying these shifts, transparency requirements such as researcher access, audits, and impact assessments rely on regulated firms to produce new forms of information for new audiences, including oversight bodies, the public, and individual users.

---

314 Tex. Bus. & Com. Code §§ 120.051–.052 (requiring platforms to publish an acceptable use policy and to disclose “accurate information regarding its content management, data management, and business practices”); Fla. Stat. § 501.2041(2)–(3) (requiring platforms to “publish” standards and to provide a “thorough explanation” to users whose content the platform “censor[s] or shadow ban[s]”).
318 Goldman, supra note 149, at 1207–09 (describing editorial transparency laws and citing the “social media censorship” laws of Florida and Texas as examples).
320 Van Loo, supra note 24, at 397–98 (describing collaborative governance).
They represent a resounding embrace of what Professor Jody Freeman called the “private role in public governance.”

The risk of collaborative governance or new governance is that public-oriented regulation might easily be co-opted by the private participants that enable it. In organizationally and technically complex settings, the expertise of the private entity often outmatches that of the public regulator. As Professor Julie Cohen has put it, “[e]mergent, nontraditional regulatory models have tended to be both opaque to external observation and highly prone to capture.”

Because new proposals for regulating technology depend on collaboration with the very targets of that regulation, external checks are particularly important. Whistleblower provisions could counteract this tilt in favor of private power by protecting disclosures that would mitigate against the risk of institutional capture and address persistent informational asymmetries. In short, whistleblowing is a kind of safety valve or backstop to ensure that regulators get the information they need and that regulation works correctly. This kind of safety valve is particularly necessary because, to a greater or lesser extent, each proposal requires cooperation by the regulated entity: disclosing the right data, giving access to the right researchers, and conducting the right impact assessment. As legislators craft increasingly elaborate new regulatory frameworks, they should build in a variety of different safety valves to ensure that these emerging, highly managerial forms of regulation ultimately remain accountable to the public. Whistleblower protections can help.

2. Incorporating Whistleblower Protections into the FTC Act

The FTC’s expansive role in privacy, security, and consumer protection enforcement has made it the leading regulator of emerging technology. Through its “authority to police deceptive and unfair trade practices,” the FTC enforces privacy policies and other promises that tech companies make. The FTC has aggressively wielded this authority and, in turn, developed a “surprisingly rich jurisprudence” of privacy decision-making.

321 See Jody Freeman, The Private Role in Public Governance, 75 N.Y.U. L. Rev. 543, 643 (2000) (“Perhaps standard-setting groups should adhere to at least some internal procedural rules designed to promote information disclosure, reasoned decision making, and fairness.”).

322 See Solow-Niederman, supra note 22, at 640 (“Public-private partnerships by definition require an equal public partner. But this prerequisite is missing when it comes to AI.”).

323 Cohen, supra note 20, at 173.


326 Id. at 586.
Still, however, the FTC’s enforcement power is limited. Consider, once again, Mudge’s revelations that Twitter’s data security protocols were much weaker than they should have been.327 The FTC had entered into a consent decree with Twitter over a decade prior.328 Pursuant to that settlement, Twitter had agreed to obtain regular assessments of its security safeguards from a “qualified, objective, independent third-party professional.”329 Twitter was also required to maintain records and to establish a comprehensive information security program.330 None of these many obligations, however, alerted the FTC to the security issues that Mudge alleged existed. At the hearing, Mudge suggested that “the FTC is a little [in] over their head, compared to the size of the big tech companies . . . . They’re left letting companies grade their own homework.”331 The failure to detect these violations suggests that the FTC may rely too heavily on private industry’s cooperation with public regulators to the detriment of its own regulatory capacity.

Twitter’s performance illustrates the risk that the FTC’s “managerial reconfiguration and privatization of dispute resolution” will ultimately be less effective than it seems.332 As Professor Ari Waldman has pointed out, FTC enforcement actions have been interpreted and reframed within industry as primarily concerned with “corporate-friendly privacy discourses” about notice and consent.333 Waldman has argued that regulated companies might adhere symbolically to privacy laws, but that in doing so they also “entrench[] corporate power.”334 If true, Mudge’s disclosures exemplify these dynamics to a tee: all the corporate security programs and assessments the FTC could order did not ensure that Twitter did more than symbolically carry out its obligations.

Adding whistleblower protections to the FTC Act would provide a check on these dynamics by ensuring that insiders could alert the FTC’s enforcement division if something is going awry. The FTC could incorporate an antiretaliation provision that prevented regulated entities from disciplining, discharging, or discriminating against employees because those

---

327 See supra text accompanying notes 172–173.
329 Id. at 4.
330 Id. at 3–5.
332 COHEN, supra note 20, at 188.
334 Id. at 103.
employees filed a complaint, began proceedings, or gave testimony. Indeed, the FTC Whistleblower Act of 2021 (FTCWA), which was introduced in the House by Congresswomen Jan Schakowsky and Lori Trahan but died in committee, would have protected whistleblowers who disclosed violations of the nation’s consumer protection and antitrust laws.\footnote{FTC Whistleblower Act of 2021, H.R. 6093, 117th Cong. (2021).}

Such a provision is necessary in part because, as Twitter’s data security breaches show, the FTC lacks the authority and the personnel to systematically monitor compliance with its orders. Many FTC settlements require companies to collect and maintain records, but not necessarily to share them with the agency.\footnote{See, e.g., In re Twitter, Inc., No. C-4316, at 5 (F.T.C. Mar. 2, 2011).} The FTC also lacks “visitation authority for either competition or consumer protection,” limiting its ability to monitor compliance with consent decrees.\footnote{Van Loo, supra note 24, at 393.} This lack of authority perpetuates information asymmetries between the regulators and the regulated entities. While the FTC has authority under Section 6(b) of the FTC Act to require regulated entities to produce specific information, and can undertake and publish studies and reports, the agency may not have all the information it needs to decide to deploy those resources.\footnote{15 U.S.C. § 46(b), (f).}

That the FTC needs more information to be able to make informed decisions about how to exercise its authority seems plain. But the proposed FTCWA included extremely broad substantive and procedural protections. For one, the FTCWA defined “covered disclosures” as any “formal or informal communication or transmission that an individual reasonably believes relates to a potential or suspected violation of any law, rule, or regulation enforced by the Commission.”\footnote{H.R. 6093 § 5(3) (emphasis added).} The FTCWA went beyond protecting disclosures to the FTC, providing antiretaliation provisions for anyone who made a covered disclosure to anyone who the whistleblower reasonably believed “has the authority to . . . take any other action to address the violation in the covered disclosure.”\footnote{Id. § 2(a)(1)(C).} This wording is far broader than Dodd–Frank’s SEC whistleblower protections, which define a “whistleblower” as someone who “provides . . . original information to the Commission.”\footnote{15 U.S.C. § 78u-6(a)(6) (emphasis added).} The provision might be interpreted broadly to protect whistleblowers who leak to the press, phone members of Congress, or communicate with any other individuals who might be able to “take . . .
action to address” the purported violations. Like the Dodd–Frank Act, the FTCWA would have created a private right of action enabling a whistleblower to bring a suit against their employer in any federal court, but its remedies and award provisions were also more aggressive than Dodd–Frank’s.

The FTCWA is one response to the urgent need for FTC whistleblower protections. Whistleblowers can serve as an early warning system notifying the FTC of potential issues. Receiving a whistleblower disclosure might enable the FTC, for example, to request all the reports and assessments a firm had conducted for agency review. Whistleblower disclosures might also tip off the enforcement division to fruitful avenues for investigation. Without whistleblower protections, however, there is no reason for a would-be whistleblower to inform the FTC of any particular problem under the agency’s jurisdiction. Still, the breadth of the FTCWA—and, ultimately, its failure—suggests that its protections might have gone further than necessary to facilitate effective enforcement of the FTC’s authority.

3. Adapting Whistleblower Law

If whistleblower protections are to address the political, technological, and economic moment we find ourselves in, they will need not just to be expanded but also to change. Most importantly, whistleblower protections could be expanded to incentivize and protect disclosures that not only alert authorities to violations of existing laws but also point lawmakers and regulators to potential areas where the law ought to be developed further. In order to serve this role, however, whistleblower protections must evolve beyond the law enforcement paradigm. First, the substance of whistleblower protections must be expanded beyond their focus on violations of existing law to cover potential ethical lapses and missteps. Second, the institutions that receive whistleblower reports should adapt to receive whistleblower disclosures outside of the context of enforcement actions in order to shape and guide policy.

Because of whistleblower provisions’ historical focus on law enforcement, these protections generally extend to workers who disclose legal violations. The law enforcement rationale for legal whistleblower

---

342 H.R. 6093 § 2(a)(1)(C).
343 Id. § 2(c); 15 U.S.C. § 78u-6(h)(1)(B). The FTC Whistleblower Act would have also given whistleblowers more financial relief and awards. Dodd–Frank’s statutory remedies include double back pay, 15 U.S.C. § 78u-6(h)(1)(B), while the FTCWA’s remedies included triple back pay, H.R. 6093 § 2(c)(2). In addition, the FTCWA provided for financial awards between 10% and 30% of any monetary sanctions that the FTC ultimately collected after successfully resolving a covered action. H.R. 6093 § 3(a).
344 See supra Section II.A.
provisions holds that protections and incentives are crucial to enable insiders to provide information about wrongdoing inside organizations. Inside information is particularly important under conditions of information asymmetry, because law enforcement depends on those with knowledge of wrongdoing to bring it to light.

Because whistleblowing protections do not extend to ethical harms, they are an awkward fit for employees who want to disclose problems that might not rise to the level of legal violations but are nonetheless salient to lawmakers and the public. Indeed, as I argued in Part II, the failure to substantively regulate issues such as bias, fairness, and accuracy pushes whistleblowers to use other channels to protect disclosure, such as securities law and labor law.

The absence of whistleblower provisions contributes to systemic information disparities in the regulation of law and technology. Consider Frances Haugen’s disclosure of Facebook’s “cross-check” program, which gave special treatment to content posted by high-profile users. In the aftermath of Haugen’s revelations, the Facebook Oversight Board reviewed its implementation of the system, but Facebook resisted producing complete data about its system even to its own Oversight Board.

Facebook’s dual standards might be icky, but they are not substantively illegal—indeed, others have argued that Facebook’s decision-making over how it treats the content that its users post is protected by the First Amendment. Despite the fact that there is broad distrust of the kinds of content-related decisions Facebook and other platforms make, there are

---

345 See supra Section II.A.

346 Bucy, supra note 155, at 59 (“Although legal and investigative talent are important in detecting and deterring illegal economic activity, inside information is more important. Knowledgeable insiders can produce information about inchoate or on-going malefiance of which law enforcement is unaware. Such insiders can also save enormous amounts of law enforcement resources by focusing governmental investigations and case preparation.”); cf. Geoffrey Christopher Rapp, Beyond Protection: Invigorating Incentives for Sarbanes-Oxley Corporate and Securities Fraud Whistleblowers, 87 B.U. L. REV. 91, 113–14 (2007) (“[A] public regulatory system will always lack one resource that is indispensable to effective detection and deterrence of complex economic wrongdoing: inside information. Only a strong whistleblower law aimed at generating incentives for corporate insiders to expose fraud can optimize the quantity of insider information brought into the public domain.” (internal quotation marks omitted)).

347 See supra Section II.A.


349 Newton, supra note 348.

currently few restrictions or requirements governing those decisions.\textsuperscript{351} The result is that Haugen used securities laws governing misrepresentation to investors as a safe harbor for her revelations. At one level, looking to whistleblower protections under securities law is a “creative” solution to the lack of substantive regulation, as Professor Nathaniel Persily has described it.\textsuperscript{352} But it also shows that the current legal structure systematically undervalues disclosures of unethical behavior unless they amount to fraud.

Yet offering legal protections to those who blow the whistle on “unethical” conduct invites gaming and misuse, as congressional attacks on disinformation and misinformation researchers illustrate. Amidst an ongoing political and “epistemic crisis . . . about the role that objectively provable, verifiable facts can or should play in decision-making,” broadening individuals’ ability to selectively and publicly disclose information from inside their employers could be a recipe for even further weaponization and polarization.\textsuperscript{353} The challenge is to foster and facilitate productive whistleblowing without unduly incentivizing counterproductive or harmful disclosures.

One option is for companies to embrace internal whistleblowing. For example, companies engaged in developing and using AI might establish internal whistleblowing channels as part of a risk-management approach informed by the National Institute of Standards and Technology’s (NIST) new AI Risk Management Framework. As part of its framework, NIST calls on organizations to use internal governance, policies, practices, and mechanisms in order to incorporate feedback, conduct ongoing review of risk management, and set priorities.\textsuperscript{354} As Professor Ari Waldman has highlighted, the risk of these internal governance mechanisms is that they might be co-opted in service of accountability theater without substance.\textsuperscript{355}

Whistleblowing channels provide internal avenues for dissenting opinions that might facilitate broader forms of discussion and debate.\textsuperscript{356} By employing internal whistleblowing on contested issues of tech ethics,
companies could embrace a far richer debate about the appropriate path forward, informed by opinions from rank-and-file workers as much as by management and leadership.

Still, internal whistleblowing is unlikely to generate the kinds of information that are necessary for informed regulation, lawmaking, and public discourse. In particular, by enforcing secrecy through contract and other legal mechanisms, the tech industry promotes a culture of secrecy and conformity that imposes serious costs for would-be whistleblowers even if they employ internal channels. And without mandating the creation of internal whistleblowing channels through statute, organizations would be free to ignore this recommendation.

Elsewhere, I have suggested that expert agencies engaged in the formulation of technology policy and best practices might establish whistleblower offices dedicated to receiving tech ethics complaints. NIST, the FTC, the Office of Science and Technology Policy, and other expert agencies could establish whistleblower “hotlines” to receive not just complaints of legal violations but also complaints about tech ethics. Because these agencies already possess substantial underlying expertise, they are uniquely capable of understanding whether complaints are justified or worth addressing. Ethics complaints would not lead to enforcement action, but they could play a critical role in fostering adequate information flow to help regulators and lawmakers make informed decisions about how best to address evolving and emerging risks.

CONCLUSION

Information is power. And amid a reckoning with the power of “Big Tech,” information—who has it, who wants it, how to get it, whether to share it—is at the center of contemporary debates about how to govern emerging technologies. Because corporations so thoroughly control information about their products, practices, and services, most policy and scholarly commentary has focused on identifying the optimal mechanisms for

357  Woo, supra note 17.
358  Cherry, supra note 37, at 1070–71 (discussing the lack of statutory procedural requirements under the Sarbanes–Oxley Act for employers handling internal-channel whistleblowing complaints and the resulting nonexistence of such procedures).
360  Max Weber, From Max Weber: Essays in Sociology 233 (H. H. Gerth & C. Wright Mills eds. & trans., 2009) ("[E]verywhere that the power interests of the domination structure toward the outside are at stake, whether it is an economic competitor of a private enterprise, or a foreign, potentially hostile polity, we find secrecy.").
enhancing the flow of information from firms to regulators, lawmakers, and the public.

This focus has left out a key source of information about corporate wrongdoing: whistleblowers. As a result, our burgeoning discourse about tech transparency and accountability is incomplete. Sidelining the workers who come forward with crucial information about tech accountability means that we have overlooked an important mechanism for checking misconduct: internal dissent.

For decades, scholars have understood that informational control by firms has significant implications for regulatory oversight. As Mark Nadel put it in 1975, corporate information control “tends to reduce the ability of government agencies to carry out their regulatory mandate.” Nearly five decades later, Nadel’s observation might well be applied to today’s technology sector. Trade secrecy obstructs democratic oversight of automated decision systems and AI, even as a growing chorus calls for more accountability for the use of these systems. As Julie Cohen has observed, the tech industry’s “secrecy imperative overrides even official demands to produce information about data extraction practices and related agreements.” Amid growing concern about the potential democratic implications of automation, algorithmic governance, social media platforms, and financial technology (to name just a few), corporate secrecy might similarly obstruct the democratic process and subvert regulatory agendas.

Despite a growing consensus that accountability and transparency of the tech industry is critical, whistleblowers have occupied almost no space in either scholarly or policy discourse about how to foster these values. This is a peculiar oversight. As in many other regulatory contexts that involve profound information asymmetry—fraud, insider trading, taxation, health and safety, among others—inside information is particularly important for law enforcement and policymaking. What’s more, many of the scandals, stories, and wrongdoing that are animating today’s policy discussions were brought to light by workers who blew the whistle.

Against the background of broad-scale secrecy, unauthorized leaks of information from tech company insiders play an essential, irreplaceable role in oversight and accountability efforts. They provide valuable sources of insight into problematic dynamics that are otherwise largely invisible to

361 Mark V. Nadel, Corporate Secrecy and Political Accountability, 35 PUB. ADMIN. REV. 14, 21 (1975).
362 See generally Katyal, supra note 17 (discussing the use of trade secrecy by corporations to circumvent disclosure of information to regulators); Graves & Katyal, supra note 83 (offering legislative proposals to limit the growing use of trade secrecy laws to hide information from the public).
363 COHEN, supra note 20, at 62.
lawmakers and regulators. They counteract the additional control and power that managerial regulatory techniques have conferred on firms. And they serve to challenge the broad assertions of secrecy so common in the technology industry.

The neglect of whistleblowing is doubly confounding because the development of tech law and policy is itself so dependent on information from insiders at firms and organizations. Information asymmetries constitute a major reason that law allegedly fails to keep pace with technological change: because lawmakers, regulators, and the public lack critical information that would foster public debate and potential regulatory action. Indeed, the inner workings of technology firms are increasingly relevant to public governance, yet we have few mechanisms for compelling them to function in more transparent ways.

Whistleblowing is both a symptom of and a corrective to the information asymmetries plaguing tech policy. But relying too heavily on individual whistleblowers is a suboptimal way of ensuring that regulators and the public get the information they need. Whistleblower protections are haphazard and incomplete. Some domain-specific disclosures are already protected by law, while other disclosures that are not (yet) deemed sufficiently valuable to protect could get workers fired or fined. And yet we continually rely on individuals to come forward—at great professional and personal cost—to solve systemic problems.

Ignoring the important role of whistleblowers implicitly suggests that individual disclosures are insignificant and not worth protecting. True, individual whistleblowing is no substitute for systemic reform. But without whistleblowers, new modalities of regulation will also fail, co-opted by industry for its own gain.364

364 WALDMAN, supra note 333, at 97–98 (describing how the technology industry has shaped privacy law and regulation to its own advantage).