
DATA RIGHTS FOR WORKERS

PAULINE T. KIM* & RACHEL H. LEAVITT**

ABSTRACT

Workers are subject to immense amounts of data collection on the job, and the algorithmic management tools built with that data can produce negative effects, including deskilling jobs, destabilizing work hours, reducing wages, and creating dangerous and degrading working conditions. Workers thus have significant interests in how their data is collected and used, and yet they have been excluded from nearly all recently enacted or proposed data protection laws. Their exclusion stems from data protection's roots in privacy law and theory, which primarily focused on consumers as data subjects. Current data protection laws, even if expanded to cover workers, would provide little protection because those laws are framed by an individual consumer model of privacy that does not account for the distinctive ways workers are vulnerable to firms' data practices. Traditional labor law protections are also insufficient to protect their rights because they fail to address a central cause of workers' disempowerment today—the largely unrestrained collection and exploitation of their data by firms. Protecting workers' rights will require legally recognizing their collective interests in data and providing robust channels for worker participation in decisions about how data-driven technologies are deployed. Empowering collective worker voice over data practices is essential to ensure that the gains from these technologies will be widely shared rather than just enriching a few.

* Daniel Noyes Kirby Professor of Law, Washington University School of Law. We are grateful for helpful feedback from Annette Bernhardt, Marion Crain, Peggie Smith, Danielle D'Onfro, Neil Richards, danah boyd, Cynthia Khoo, Jennifer Rothman, Victoria Schwartz, Jonathan Harris, and participants at the Privacy Law Scholars Conference, the Washington University School of Law Faculty Workshop, and the BC-MIT Worker and Employer Power Workshop. Many thanks to Julia Monti, Kelly Miller, and Nicholas Ogilvie-Thompson for excellent research assistance.

** J.D., Washington University School of Law.

CONTENTS

INTRODUCTION.....	617
I. COMPREHENSIVE DATA PROTECTION AND THE EXCLUSION OF WORKERS	624
II. DATA PROTECTION, PRIVACY, AND WORKERS	632
III. WORKPLACE DATA PRACTICES	641
A. <i>Data Collection and Algorithmic Management</i>	642
B. <i>Potential Harms to Workers' Rights</i>	645
1. Labor Displacement and Deskilling	646
2. Increased Precarity.....	648
3. Health and Safety.....	650
4. Discrimination and Bias	651
5. Collective Speech and Activity	652
6. Chilling Speech.....	653
IV. THE LIMITS OF WORK LAW	655
V. THE LIMITS OF DATA PROTECTION MODELS.....	659
A. <i>Conceptual Limits of the Consumer Model</i>	660
B. <i>Practical Limits of Data Protection</i>	664
VI. WORKERS' COLLECTIVE INTERESTS IN DATA	668
CONCLUSION	673

INTRODUCTION

Workers today are subject to immense amounts of data collection when they contribute their labor to an enterprise,¹ starting before they even enter into a work relationship. Firms collect a wide range of information about applicants and potential recruits, including traditional indicia like work experience and education, digital profiles compiled by outside agencies, records of activities on social media and other online platforms, and biometric data harvested from recorded interviews. The collection of workers' data intensifies once they are on the job. Firms can gather data using audio and video recording, keystroke monitoring, RFID badges, activity trackers, and other tools to capture workers' whereabouts, activities, output, and physiological states in real time. These types of data collection have traditionally been understood in terms of privacy—forms of surveillance or intrusions seen as threats to workers' dignitary interests.

Today, however, workers' concerns surrounding firms' data practices are not solely or even primarily about unwanted observation or intrusion, and the potential harms go far beyond embarrassment or hurt feelings. Rather, firms' vast data collection threatens to undermine workers' fundamental labor rights and interests.² Aggregated worker data and advanced computational systems combine to create a wide range of algorithmic management tools—automated systems that can screen and hire employees, set work schedules, determine compensation, regulate work tasks, establish performance standards, and automate tasks.³ These data-driven tools are not just about increased efficiency. Algorithmic forms of management can result in the deskilling of jobs, unstable work hours, reduced wages, and dangerous and degrading work conditions.⁴ By increasing firms' leverage vis-à-vis labor, these data practices enable firms to drive down wages and working conditions and to capture more of the surplus of

¹ See Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CALIF. L. REV. 735, 740-47 (2017); IFEOMA AJUNWA, *THE QUANTIFIED WORKER: LAW AND TECHNOLOGY IN THE MODERN WORKPLACE* 1-5 (2017); Richard A. Bales & Katherine V.W. Stone, *The Invisible Web at Work: Artificial Intelligence and Electronic Surveillance in the Workplace*, 41 BERKELEY J. EMP. & LAB. L. 1, 9-20 (2020); Jeffrey M. Hirsch, *Future Work*, 2020 U. ILL. L. REV. 889, 913-15; BRISHEN ROGERS, *DATA AND DEMOCRACY AT WORK* 82-88 (2023). See generally HILKE SCHELLMANN, *THE ALGORITHM: HOW AI DECIDES WHO GETS HIRED, MONITORED, PROMOTED, AND FIRED AND WHY WE NEED TO FIGHT BACK NOW* chs. 7-10 (2024).

² See Annette Bernhardt, Lisa Kresge & Reem Suleiman, *The Data-Driven Workplace and the Case for Worker Technology Rights*, 76 INDUS. & LAB. RELS. REV. 3, 8-14 (2023); Nathan Newman, *Reengineering Workplace Bargaining: How Big Data Drives Lower Wages and How Reframing Labor Law Can Restore Information Equality in the Workplace*, 85 U. CIN. L. REV. 693, 698-701 (2017) (“[T]he harm much employer use of data inflicts is not harm to individual workers in the form of discrimination but collective harm in the form of weaker collective organization and lower wages.”); ROGERS, *supra* note 1, at 96-101.

³ See, e.g., Bales & Stone, *supra* note 1, at 9-14.

⁴ See, e.g., Bernhardt et al., *supra* note 2, at 8-14 (chronicling potential harms to workers from data-driven technologies).

production.⁵ Workers' data can also be used to train robots or generative artificial intelligence ("AI") models that can reproduce their labor automatically, replacing the need for humans.⁶ Workers thus have significant interests in determining what data is collected about them and how it is processed.

In this, workers would appear to be quite similar to consumers, whose interests in their personal data have received considerable attention in recent years. As of February 2026, twenty states have passed comprehensive data protection laws,⁷ and numerous federal data protection bills have been proposed.⁸ These bills provide consumers with individual rights relating to the collection and use of their data and impose certain obligations on entities that process personal data. And yet, with the sole exception of California's statute, all the enacted data protection statutes specifically exclude workers and their data from coverage.⁹

In parallel conversations, a great deal of attention has focused on the risks surrounding artificial intelligence and the use of algorithms to make socially consequential decisions¹⁰—systems that are in essence computationally

⁵ See Newman, *supra* note 2, at 696-97.

⁶ See Bernhardt et al., *supra* note 2, at 10.

⁷ See U.S. State Privacy Legislation Tracker, INT'L ASS'N OF PRIV. PROS., <https://iapp.org/resources/article/us-state-privacy-legislation-tracker> (Feb. 23, 2026). While there is some debate as to whether an additional law—the Florida Data Bill of Rights—constitutes a "comprehensive" data protection statute, we do not include it in our count, given its relatively narrow definition of data controller that significantly limits the statute's scope. See Andrew Folks, *Defining 'Comprehensive': Florida, Washington and the Scope of State Tracking*, INT'L ASS'N OF PRIV. PROS. (Feb. 22, 2024), <https://iapp.org/news/a/defining-comprehensive-florida-washington-and-the-scope-of-state-tracking> [<https://perma.cc/6FHS-588P>].

⁸ See, e.g., American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2021); *The American Privacy Rights Act Puts People in Control of Their Data*, HOUSE COMM. ON ENERGY & COM. (Apr. 23, 2024), <https://energycommerce.house.gov/posts/the-american-privacy-rights-act-puts-people-in-control-of-their-data> [<https://perma.cc/HHF3-FWJN>].

⁹ See *infra* Part I. In 2024, Colorado passed a bill, entitled "An Act Concerning Consumer Protections in Interactions with Artificial Intelligence," providing protections from unfair decisions by artificially intelligent systems. S.B. 24-205, 2024 Gen. Assemb., Reg. Sess. (Colo. 2024). The statute's protections extend to workers, but we do not include it among our count of state data protection laws because it focuses on artificial intelligence ("AI") decision-making and discriminatory effects rather than control over personal data. *Id.* Colorado had earlier passed a separate law, the "Colorado Privacy Act," addressing data protection that follows the general pattern of excluding workers and employment data from protection. S.B. 21-190, 2021 Gen. Assemb., Reg. Sess. (Colo. 2021).

¹⁰ See, e.g., Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 677-93 (2016) ("[D]ata mining holds the potential to unduly discount members of legally protected classes and to place them at systematic relative disadvantage."); Deborah Hellman, *Measuring Algorithmic Fairness*, 106 VA. L. REV. 811, 834-42 (2020); Pauline T. Kim, *Data-Driven Discrimination at Work*, 58 WM. & MARY L. REV. 857, 874-90 (2017) [hereinafter Kim, *Data-Driven Discrimination*] (highlighting how algorithms developed with inaccurate or biased data can discriminate based on protected classes, such as race or sex, in employment context); Jon Kleinberg, Jens Ludwig, Sendhil Mullainathan & Cass R. Sunstein, *Discrimination in the Age of Algorithms*, 10 J. LEGAL ANALYSIS 1, 26-30 (2018).

complex forms of data use. In contrast to data protection laws, workers have figured prominently in these discussions, with employment often cited as a particular site of concern about unfair or discriminatory systems. The proposed Algorithmic Accountability Act¹¹ would have included workers; President Biden's Executive Order on AI highlighted AI's effects on workers among its central concerns;¹² and a few states have taken explicit steps to protect workers from algorithmic discrimination.¹³

This Article explores the contradictions in how workers are treated in discussions about data protection and algorithmic governance, arguing that their inconsistent treatment is in part the result of data protection's roots in privacy law and the latter's central focus on the rights of the consumer. The United States has traditionally taken a sectoral approach to privacy, enacting regulations to deal with personal information collected in the context of specific types of consumer relationships.¹⁴ Enforcement actions taken by the Federal Trade Commission ("FTC") for privacy violations have also focused on the consumer.¹⁵ This regulatory focus is mirrored in privacy law scholarship, which generally conceives of the data subject as a consumer vulnerable to corporate manipulation.¹⁶ Except in recent literature on algorithmic harms, workers have largely been absent in these discussions, or mentioned in passing, on the assumption that their interests can be subsumed under those of consumers.

Worker organizations and advocates are well aware of how data collection and the deployment of digital technologies can harm workers.¹⁷ Unions have long sought to bargain about the use of electronic monitoring tools in the workplace, and recent labor actions have focused on the use of AI by employers.¹⁸ Labor advocates and worker organizations have articulated basic

¹¹ Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. (2022); S. 3572, 117th Cong. (2022); Algorithmic Accountability Act of 2023, H.R. 5628, 118th Cong. (2023).

¹² Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023). This Executive Order was revoked by President Trump. Exec. Order No. 14179, 90 Fed. Reg. 8741 (Jan. 23, 2025).

¹³ See, e.g., COLO. REV. STAT. § 6-1-1701-1707 (2024). Illinois amended the Illinois Human Rights Act to explicitly prohibit an employer's use of AI in ways that subject employees to discrimination on the basis of protected classes or zip codes used as proxies for protected classes and to require employers to provide notice to employees regarding its use of AI in decision-making. 775 ILL. COMP. STAT. ANN. 5/2-101-102 (West 2025). The California Civil Rights Council approved final regulations to clarify the application of existing anti-discrimination laws to the use of artificial intelligence in employment decisions. CAL. CODE REGS. tit. 2, § 11008-11076 (2025).

¹⁴ See Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 906-16 (2009).

¹⁵ See Woodrow Hartzog & Daniel Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2235-40 (2015) (describing how Federal Trade Commission ("FTC") enforces privacy and data security through its powers under Section 5 of Federal Trade Commission Act).

¹⁶ See *infra* Part I.

¹⁷ See Bernhardt et al., *supra* note 2, at 14.

¹⁸ See, e.g., Alex Winter, *The SAG Deal Sends a Clear Message About AI and Workers*, WIRED (Nov. 13, 2023, at 18:43 ET), <https://www.wired.com/story/hollywood-actors-sag-arti>

principles and policy statements about the use of digital technologies in the workplace.¹⁹

Labor law scholars and researchers have also raised alarms about the impact of extensive data collection and the use of algorithmic management tools on workers' rights.²⁰ For the most part, however, these scholars have doubled down on traditional labor and employment protections, arguing for strengthening existing laws. Others have gestured in the direction of data protection laws, suggesting that workers should be included in those protections, but without closely analyzing whether those laws would be effective if applied to workers.²¹

We argue that both existing work law and the dominant data protection models are inadequate to protect workers' interests in their data. Traditional labor and employment laws were largely developed in the industrial era, based on certain assumptions about how workplaces are organized and managed. These assumptions no longer hold because massive data collection and algorithmic management practices are altering how work is structured and power

ficial- intelligence- contract [<https://perma.cc/M8F5-VA97>] (noting Screen Actors Guild-American Federation of Television and Radio Artists reached tentative agreement with Alliance of Motion Pictures and Television Producers containing terms to regulate producers' AI usage and protect actors from AI tools used to manipulate their work).

¹⁹ See, e.g., Bernhardt et al., *supra* note 2, at 17-22 (outlining principles such as full coverage of workers and employers, disclosure and transparency, limitations on collecting worker data, and restrictions on electronic monitoring and employer use of algorithms); MISHAL KHAN & KUNG FENG, A FIRST LOOK AT LABOR'S AI VALUES: AN ANALYSIS OF RECENT STATEMENTS ABOUT TECHNOLOGY BY UNIONS AND OTHER WORKER ORGANIZATIONS, UNIV. OF CAL. BERKELEY LAB. CTR. (Sep. 18, 2025), <https://laborcenter.berkeley.edu/wp-content/uploads/2025/09/Labors-AI-Values-v2.pdf> [<https://perma.cc/EY3M-KHAG>] (identifying key values for protecting workers' data rights, including transparency and disclosure, guardrails around collection and use of worker data, accountability structures, and worker input in design and deployment of technologies); ARTIFICIAL INTELLIGENCE: PRINCIPLES TO PROTECT WORKERS, AFL-CIO 2-4 (Oct. 15, 2025), <https://aflcio.org/reports/workers-first-ai?> [<https://perma.cc/F9F2-327V>].

²⁰ See, e.g., Ajunwa et al., *supra* note 1, at 743-56, 763-72; Bales & Stone, *supra* note 1, at 22-55 (asserting existing regulatory frameworks are insufficient to address concerns regarding workers' data privacy, AI-based antitrust practices, employment discrimination, and labor law violations); Hirsch, *supra* note 1, at 915-45 (examining how emerging technologies such as AI impact workplace, including risks of job displacement, discrimination and bias in AI decision-making, and safety); Newman, *supra* note 2, at 714-25 (arguing technological developments facilitating extensive data-driven surveillance in workplace has enabled wage suppression and diminished workers' collective bargaining power).

²¹ See, e.g., Pauline T. Kim & Matthew T. Bodie, *Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy*, 35 A.B.A. J. LAB. & EMP. L. 289, 309-11 (2020) (suggesting European Union's General Data Protection ("GDPR") Regulation model as potential framework for United States workers' privacy protection); Hirsch, *supra* note 1, at 956-57 (positing centralized workplace laws, such as national regulatory scheme, would better address technology-related workplace concerns); Halefom H. Abraha, *Regulating Algorithmic Employment Decisions Through Data Protection Law*, 14 EUR. LAB. L.J. 172-91 (2023) (proposing data protection laws as source of protection from algorithmic management, but arguing significant gaps remain).

is distributed in the workplace. Relying on minimum standards laws is not enough because they fail to address a central cause of workers' relative disempowerment today: the largely unrestrained collection and exploitation of worker data by firms. Labor advocates have also introduced numerous bills at the state level to address workplace technologies. The proposed bills, however, typically offer only limited protection, focusing on a particular type of technology and often draw heavily on concepts like notice and consent from data protection law.

The dominant model of data protection in the United States is also inadequate to protect workers' interests. Those laws are rooted in a consumer model, which is animated by an image of the autonomous individual engaging in market transactions for goods and services.²² While workers also have interests in how their personal data is used, the work relationship differs in significant ways. For most people, work is foundational—essential for obtaining basic necessities, and to that extent, prior to their role as consumers. In addition, work relationships are generally thicker and more relational. They are explicitly hierarchical, granting firms rights of control, and workers' role in the firm can be displaced by technology in ways that consumers cannot. All of these are reasons that the consumer model is a poor fit conceptually, making it risky to rely on this frame to protect workers' interests.

There are practical limitations to relying on existing data protection statutes as well. Even if they applied, the rights created by these laws, such as rights of access and correction, are not easily exercised by the individual worker. And by exercising those rights, a worker is unlikely to make any difference in the operation of workforce-wide algorithmic management systems. These statutes also impose obligations on data processors, but these obligations are ill-defined and lack clear enforcement mechanisms. Without more substantive content or more robust channels for enforcing them, they are unlikely to significantly influence firms' data practices.

We argue that what is missing from existing regulatory models is a clear recognition that workers have *collective* interests in their data. It is not that workers each individually have similar interests; rather, they have interests *as a group* in how their data is used. Their interests cannot be separated from one another because they jointly share the *same* interest. In other words, algorithmic management practices are a local public good that will affect all workers alike. When firms make choices about how to deploy those systems, individual workers cannot effectively opt out. The tools are intended to operate system-wide and so firms' choices will benefit or harm all workers alike.

Because workers have collective interests in their data, the law should create channels for workers to assert those interests collectively. If data rights such as rights to access or correct are granted, workers should be able to exercise them as a group. Unions or other worker representatives should be allowed to access

²² Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1747-49 (2021).

aggregate data on behalf of all represented workers to understand how they are used to set performance standards or determine working conditions. Adequately protecting worker interests also requires mechanisms for exercising collective worker voice that can shape decisions around data processing. In line with the calls for greater stakeholder or public participation in algorithmic governance,²³ worker representatives should be given a seat at the table when firms are making decisions about what worker data will be collected and how data-driven technologies will be deployed in the workplace.

Importantly, worker bargaining or consultation around data practices does not mean the end of technological innovation in the workplace. Economists have distinguished between different types of technological innovation in firms.²⁴ Technology can be productivity enhancing when new tools are developed that complement human skills, making workers more productive. New tools can also improve workers' lives by mitigating hazards or performing the most dangerous tasks. However, other applications of technology do little to enhance overall productivity. Instead, their effect is primarily to enhance employer power, thereby allowing firms to capture more of the surplus value from production, while wages and working conditions decline. Many monitoring and surveillance tools fall into this category. As Brishen Rogers argues, mandated bargaining around data uses would "incentivize employers to adopt productivity-enhancing

²³ See, e.g., Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529, 1559-77 (2019); Michele Estrin Gilman, *Beyond Window Dressing: Public Participation for Marginalized Communities in the Datafied Society*, 91 FORDHAM L. REV. 503, 522-29 (2022) (advocating for greater public participation in algorithmic accountability regulatory regimes to enhance democratic processes and serve as corrective mechanism to marginalizing political system); John Logan Koepke & David G. Robinson, *Danger Ahead: Risk Assessment and the Future of Bail Reform*, 93 WASH. L. REV. 1725, 1731, 1805-07 (2018) ("Without careful design and open governance . . . it is more likely than not that these [pretrial risk assessment] tools will perpetuate or worsen the very problems reform advocates hope to solve."); Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1312 (2008) (proposing government agencies "establish information technology review boards that would provide opportunities for stakeholders and the public at large to comment on a system's design and testing"); Margot E. Kaminski & Gianclaudio Malgieri, *Algorithmic Impact Assessments Under the GDPR: Producing Multi-Layered Explanations*, 11 INT'L DATA PRIV. L. 125, 139 (2021) (arguing model algorithmic impact assessment should involve civil society, impacted individuals, and technical experts, including experts in law and ethics); Hannah Bloch-Wehba, *Algorithmic Governance from the Bottom Up*, 48 BYU L. REV. 69, 89-90 (2022) (examining how tech workers partner with social and racial justice movements to call for greater democratic control over algorithmic governance in private and public sectors).

²⁴ See generally Daron Acemoglu & Simon Johnson, *POWER AND PROGRESS: OUR THOUSAND-YEAR STRUGGLE OVER TECHNOLOGY AND PROSPERITY* (2023) (arguing who controls new technology and how it is implemented determines whether it benefits society or exacerbates economic inequality); Daron Acemoglu & Pascual Restrepo, *The Wrong Kind of AI? Artificial Intelligence and the Future of Labour Demand*, 13 CAMBRIDGE J. REGIONS ECON. & SOC'Y 25 (2020) (distinguishing technological advances that enhance productivity and prosperity from AI-based automation technologies that contribute to job displacement and greater economic inequality).

rather than power-augmenting technologies.”²⁵ In other words, it would not stop innovation but redirect it toward applications that create greater shared benefits.

This Article makes three principal contributions to the literature. First, it brings together two disparate literatures that have not closely engaged with one another. Privacy law scholars emphasize how data shapes power and social relations but have largely ignored the workplace. Labor law scholars highlight the role of information and data in determining working conditions but have not closely scrutinized the application of data protection laws to the workplace. Second, this Article highlights and interrogates the exclusion of workers from current data protection efforts, offering a detailed analysis of the prevailing framework for data protection laws and exposing its shortfalls for protecting workers’ rights. Third, it makes the case for recognizing *collective* data rights for workers. While privacy law scholars have recognized the relational nature of data, and labor law scholars have called for more democratic governance and participation rights in the workplace, what has been missing is a clear articulation of the inherently collective nature of workers’ interests in firms’ data practices and the implications for protecting workers’ basic labor rights. This Article fills that gap.

Our analysis proceeds as follows. Part I analyzes recently enacted and proposed data protection laws that create frameworks for algorithmic governance. It documents how workers are almost entirely excluded from data protection provisions and yet figure prominently in proposals to address algorithmic harms. Part II further explores this inconsistent treatment of workers, explaining how data protection’s roots in privacy law have led both legislatures and scholars to focus primarily on consumers as data subjects in need of protection, neglecting the ways in which workers are also vulnerable to firms’ data practices. In Part III, we document the massive collection of data from workers and how firms leverage that information. The resulting algorithmic management tools afford firms increased power that threatens workers’ interests and undermines established labor rights.

We consider next the extent to which existing legal frameworks can offer protection for these worker interests. Part IV explains that traditional labor and employment regulations are inadequate to protect workers’ fundamental rights because they fail to address a central cause of workers’ growing disempowerment—the largely unrestrained collection and exploitation of their data by firms. Part V turns to data protection law and concludes that even if recently enacted statutes applied to workers, they would do little to alleviate the data-driven harms they face. As a conceptual matter, the consumer model on which these laws are premised fits poorly, relying heavily on a transactional model which is unlikely to adequately protect workers. And practically, these statutes offer rather anemic protections, relying on procedural rights and offering few legally enforceable standards to limit data collection and use. Part VI argues that what is needed is clear recognition of the *collective* nature of workers’

²⁵ ROGERS, *supra* note 1, at 143.

interests in their data and the creation of legal mechanisms for workers to exercise voice as a group rather than solely as individuals. We then conclude.

I. COMPREHENSIVE DATA PROTECTION AND THE EXCLUSION OF WORKERS

In recent years, numerous United States jurisdictions have enacted or considered comprehensive data protection statutes, and yet workers have been excluded from nearly all of them. This Part analyzes the recent wave of data protection laws, documenting the near-total exclusion of workers, and their inconsistent and ambiguous treatment by policymakers.

The traditional American approach to data protection has relied on narrowly-defined, sector-specific regulations, but in recent years many legislatures have turned to an omnibus model. This development has led commenters to speculate about a “constitutional moment” for privacy rights,²⁶ or a “Brussels effect”—i.e. the influence of the European Union’s (“EU”) General Data Protection Regulation (“GDPR”).²⁷ California was the first U.S. jurisdiction to take a comprehensive approach, regulating data collection and use across industries and technologies in the California Consumer Privacy Act of 2018 (“California CPA”).²⁸ That statute created individual data rights, such as rights to access, correct, and delete one’s personal information, and imposed new obligations on entities that collect and process data. A subsequent ballot initiative amended the

²⁶ Woodrow Hartzog & Neil M. Richards, *Privacy’s Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1694, 1697-709 (2020) (“Europe’s data protection framework has influenced U.S. law to the point that American privacy law is facing its constitutional moment.”).

²⁷ The “Brussels Effect” refers to an argument by Anu Bradford that the European Union’s (“EU”) has significant influence globally because its regulations have influenced standards for international businesses in areas like data privacy, consumer health and safety, and the environment. ANU BRADFORD, *THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD* 25-65 (2020). This thesis has been applied to argue that the EU’s GDPR has influenced data protection standards and laws worldwide, although other scholars have questioned its causal effects. *See, e.g.*, Chander et al., *supra* note 22, at 1764-75 (arguing “Brussels Effect” on United States privacy law is secondary to “California Effect” with California Consumer Privacy Act of 2018); Jens Frankenreiter, *Cost-Based California Effects*, 39 YALE J. ON REGUL. 1155, 1216-17 (2022) (finding impact of “Brussels Effect” on U.S. data privacy law is more limited than previously suggested, based on analysis of changes in privacy policies of publicly available U.S. websites).

²⁸ California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (West 2025). The California Consumer Privacy Act of 2018 (“California CPA”) emerged as a legislative alternative to a ballot initiative proposed by a group called Californians for Consumer Privacy. Following its enactment, the group agreed to withdraw the proposal from voter consideration. John Myers & Jazmine Ulloa, *California Lawmakers Agree to New Consumer Privacy Rules that Would Avert Showdown on the November Ballot*, L.A. TIMES (June 21, 2018, at 20:40 PT), <https://www.latimes.com/politics/la-pol-ca-privacy-initiative-legislature-agreement-20180621-story.html> (“Democrats in the California Legislature and a wealthy San Francisco developer . . . reached a tentative agreement to enact major new consumer privacy rules in exchange for the withdrawal of a measure privacy activists were poised to get on the November ballot.”).

California CPA, creating additional rights for data subjects and establishing a state regulatory agency to enforce its requirements.²⁹

Other states soon followed California's lead, taking a broadly similar approach granting individual data rights and imposing obligations and restrictions on data processors. By February 2026, twenty states had enacted comprehensive data protection statutes, and dozens of additional bills had been introduced.³⁰ This legislative activity likewise reached the federal level. Dozens of federal data protection bills have been proposed. The 2021 American Data Privacy and Protection Act ("ADPPA")³¹ advanced furthest in the legislative process, receiving near unanimous bipartisan support in the House Committee on Energy and Commerce.³² In 2024, Congress considered the American Privacy Rights Act ("APRA"),³³ which was heralded by its co-sponsors as "bipartisan, bicameral draft legislation" that offers "the best opportunity we've had in decades to establish a national data privacy and security standard that gives people the right to control their personal information."³⁴

Significantly, however, the overwhelming majority of these statutes—enacted or proposed—do not offer *workers* protection for their personal information.³⁵

²⁹ California Privacy Rights Act of 2020, 2020 Cal. Legis. Serv. Proposition 24 (West) (codified at CAL. CIV. CODE § 1798.100).

³⁰ See INT'L ASS'N OF PRIV. PROS., *supra* note 7. The enacted and proposed data privacy bills are less transformative than they may appear. Although they entail a move toward omnibus-style privacy legislation, they largely fall back on a notice and consent paradigm. Chander, Kaminski, and McGeeveran argue that, instead of a transformative rethinking of data protection as a matter of fundamental rights, the California CPA follows a "transactional" model "concerned with protecting *consumers* in their dealings with *commercial* entities," that falls "well within the consumer protection tradition of American privacy law." Chander et al., *supra* note 22, at 1756, 1762. The other state statutes follow similar frameworks and have been similarly criticized. See, e.g., Hartzog & Richards, *supra* note 26, at 1707-12 (critiquing California CPA for focusing on "industry transparency and individual notions of consent, control, and choice"); Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 792-810 (2020) (critiquing United States privacy law for prioritizing symbolic compliance structures and corporate risk avoidance over substantive privacy protections for consumers).

³¹ H.R. 8152, 117th Cong. (2021).

³² Press Release, House Comm. on Energy & Com., Bipartisan E&C Leaders Hail Committee Passage of the American Data Privacy and Protection Act (July 20, 2022), <https://energycommerce.house.gov/posts/bipartisan-ec-leaders-hail-committee-passage-of-the-american-data-privacy-and-protection-act> [<https://perma.cc/J9JF-6B74>] (celebrating committee passage of American Data Privacy and Protection Act ("ADPPA") as bipartisan effort to establish national data privacy protections after vote of 53-2).

³³ H.R. 8818, 118th Cong. (2024).

³⁴ Press Release, House Comm. on Com. Sci. & Transp., What Others Are Saying: The American Privacy Rights Act (Apr. 19, 2024), <https://www.commerce.senate.gov/2024/4/what-others-are-saying> [<https://perma.cc/V6HA-77S9>].

³⁵ See, e.g., U.S. SENATE COMM. ON COM., SCI., & TRANSP., THE AMERICAN PRIVACY RIGHTS ACT OF 2024: SECTION-BY-SECTION SUMMARY I (2024), <https://www.commerce.senate.gov/services/files/E7D2864C-64C3-49D3-BC1E-6AB41DE863F5> [<https://perma.cc/R9>

With the sole exception of the California CPA, all enacted data protection laws expressly exclude workers from their coverage.³⁶ That workers should be

TH-SPW3] (noting proposed bill would not cover employee data). The draft language of the ADPPA also excluded workers and worker data, expressly exempting “employee data” from coverage. H.R. 8152 § 2(8)(B)(ii). Furthermore, it defined “employee” comprehensively to mean an “employee, director, officer, staff member individual working as an independent contractor . . . , trainee, volunteer, or intern of an employer,” thereby encompassing all types of workers, not just those in standard employment relationships. *See* H.R. 8152 § 2(15). At the state level, most proposed data protection bills have similarly excluded workers. *See* sources cited *infra* note 36. A few have would have included worker protections, although as of January 2026, none have been enacted. *See, e.g.*, S.B. 0052, 104th Gen. Assemb., Reg. Sess. § 5-10, at 10, § 5-5(8), at 2 (Ill. 2025) (defining “consumer” as “a natural person who is a State resident, however identified, including by any unique identifier” and explicitly noting “privacy interests of employees and independent contractors should also be protected, taking into account the differences in the relationship between employees or independent contractors and businesses as compared to the relationship between consumers and businesses”); H.B. 1012, 60th Leg., 1st Sess. § 2(7), at 7, § 2(14), at 8, § 2(14)(i), at 10 (Okla. 2025) (defining “consumer” as “an individual who is a resident of this State,” and “personal information” as including “information that identifies, relates to, describes, can be associated with or can reasonably be linked to . . . professional or employment-related information”); H.B. 2953, 87th Leg., Reg. Sess., at 5-6 (W. Va. 2025) (defining covered “personal information” to include “information that identifies, relates to, or describes a particular consumer or household, or is reasonably capable of being directly or indirectly associated or linked with, a particular consumer or household” including “[p]rofessional or employment-related information”).

³⁶ *See* Colorado Privacy Act, COLO. REV. STAT. § 6-1-1303(6)(b) (2025) (excluding “individuals acting in [an] . . . employment context” from Colorado Privacy Act coverage); Connecticut Consumer Data Privacy and Online Monitoring Act, CONN. GEN. STAT. ANN. § 42-515(8) (West 2025) (“‘Consumer’ does not include an individual acting in a commercial or employment context or as an employee”); Delaware Personal Data Privacy Act, DEL. CODE ANN. tit. 6, § 12D-102(8) (2025) (“‘Consumer’ does not include an individual acting in a commercial or employment context”); Indiana Consumer Data Protection Act, IND. CODE ANN. § 24-15-2-8 (West 2025) (clarifying “consumer” definition “does not include an individual acting in a commercial or employment context”); Iowa Consumer Data Protection Act, IOWA CODE ANN. § 715D.1(7) (2025) (excluding “a natural person acting in a commercial or employment context” from “consumer” definition); Montana Consumer Data Privacy Act, MONT. CODE ANN. § 30-14-2802(6)(b) (2024) (excluding “an individual acting in a commercial or employment context”); S. 332, 220th Leg., 2022 Sess. § 1 (N.J. 2022) (enacted) (clarifying “consumer” definition does not cover “employment context”); Oregon Consumer Privacy Act, OR. REV. STAT. ANN. § 646A.570(7) (West 2025) (“‘Consumer’ means any natural person who resides in this state and acts in any capacity other than in a commercial or employment context.”); Tennessee Information Protection Act, TENN. CODE ANN. § 47-18-3302(7)(B) (2025) (exempting “natural person acting in [an] . . . employment context”); Texas Consumer Data Protection Act, TEX. BUS. & COM. CODE ANN. § 541.001(7) (West 2025) (“‘Consumer’ means an individual who is a resident of this state acting only in an individual or household context. The term does not include an individual acting in a commercial or employment context.”); Utah Consumer Privacy Act, UTAH CODE ANN. § 13-61-101(10)(b) (West 2025) (excluding “individual[s] acting in an employment . . . context”); Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-575 (2025) (“‘Consumer’ means a natural person who is a resident of the Commonwealth acting only in an individual

excluded is not obvious. The EU's GDPR affords data protection to natural persons, including in their capacity as workers.³⁷ In seeking to regulate unfair and abusive data practices, legislatures in the United States might similarly have defined protections broadly. After all, firms collect immense amounts of data about people in their roles as workers, not just as consumers. And how firms use that worker information can determine who gets access to jobs, how much they are paid, and under what conditions they labor.³⁸ Thus, people have interests in how their data is collected and used in the workplace, just as they have interests in controlling their personal information when they purchase goods or services.

When the California CPA was passed in 2018, it broadly defined a "consumer" as a "natural person who is a California resident,"³⁹ and included "professional or employment-related information" in the definition of "personal

or household context. It does not include a natural person acting in a commercial or employment context.").

³⁷ The GDPR, like its predecessor the Data Protection Directive, defines "personal data" expansively to mean "any information relating to an identified or identifiable natural person" without restrictions as to role or relationship. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 4(1), 2016 O.J. (L 119) 1, 33 (EU) [hereinafter GDPR]; see Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 2, 1995 O.J. (L 281) 31, 38 (EC) ("[P]ersonal data shall mean any information relating to an identified or identifiable natural person . . ."). The EU data authority has specifically addressed the employment context. See Article 29 Data Prot. Working Party, *Opinion 2/2017 of the Article 29 Data Prot. Working Party on Data Processing at Work*, 17/EN WP 249, at 3 (June 8, 2017) (assessing "additional obligations placed on employers by the General Data Protection regulation"). It recognizes "employees are seldom in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship," and therefore, absent "exceptional situations," employers must rely on grounds other than consent in order to lawfully process worker data. *Id.* at 4. Because work relationships may raise unique concerns, the GDPR allows member states to enact additional regulations applicable to the workplace. GDPR, *supra*, art. 88(1)-(2) ("Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context."). Some member states, including Germany and Greece, regulate and protect the personal data of workers through this "opening clause," though most member states have protections for worker data rights embedded within labor laws enacted prior to the GDPR. See Halefom H. Abraha, *A Pragmatic Compromise? The Role of Article 88 GDPR in Upholding Privacy in the Workplace*, 12 INT'L DATA PRIV. L. 276, 283 (2022) (noting few EU nations' data protection legislation explicitly reference GDPR Article 88).

³⁸ See ANNETTE BERNHARDT, LISA KRESGE & REEM SULEIMAN, UNIV. OF CAL. BERKELEY LAB. CTR., DATA AND ALGORITHMS AT WORK 6 (Nov. 2021), <https://laborcenter.berkeley.edu/wp-content/uploads/2021/11/Data-and-Algorithms-at-Work.pdf> [<https://perma.cc/UL75-X26P>] ("Hiring software is an especially important example, because employers are increasingly using it to partially or even wholly automate the recruitment, screening, and evaluation of job candidates—with substantial risk of bias and discrimination.").

³⁹ A.B. 375, 2017-2018 Leg., Reg. Sess. § 1798.140(g) (Cal. 2018).

information.”⁴⁰ The California CPA’s legislative findings expressly referenced employment, acknowledging that “[i]t is almost impossible to apply for a job . . . without sharing personal information.”⁴¹ And yet, despite these references to employment-related data, the authors of the initial California CPA ballot proposal later stated that they “did not intend to impact the relationship between employers and employees.”⁴²

Regardless of the initial intent, the inclusion of workers within the protections of the California CPA caused immediate consternation. Tech companies lobbied extensively for revisions in their favor, including limiting the law’s applicability to the workplace.⁴³ Business groups, such as the California Chamber of Commerce, likewise sought to exclude workers from the California CPA’s coverage.⁴⁴ Because of the controversy, the California legislature passed a compromise bill that temporarily exempted employment-related information from coverage until January 1, 2021, in order to allow additional time to consider the employer and worker interests at stake.⁴⁵ When voters passed the California Privacy Rights Act of 2020 (“CPRA”), a ballot initiative aimed at strengthening the law, it further extended the temporary exclusion of workers until January 1,

⁴⁰ *Id.* §§ 1798.140(o)(1)(I), 1798.140(o)(1).

⁴¹ *Id.* § 2(c).

⁴² CAL. ASSEMB. COMM. ON PRIV. & CONSUMER PROT., REPORT ON A.B. 25, REG. SESS., at 6 (2019) [hereinafter REPORT ON A.B. 25].

⁴³ See Issie Lapowsky, *Tech Lobbyists Push to Defang California’s Landmark Privacy Law*, WIRED (Apr. 29, 2019, at 15:09 ET), <https://www.wired.com/story/california-privacy-law-tech-lobby-bills-weaken> [<https://perma.cc/H3H6-UTTL>] (highlighting technology company lobbying efforts against California CPA employee data coverage); Kartikay Mehrotra, Laura Mahoney & Daniel Stoller, *Google, Industry Try to Water Down First U.S. Data-Privacy Law*, BLOOMBERG, <https://www.bloomberg.com/news/articles/2019-09-04/google-industry-try-to-water-down-first-u-s-data-privacy-law> (Sep. 4, 2019, at 12:27 ET) (“Google and its industry allies are marking a late bid to water down the first major data-privacy law in the U.S.”); Francisco Collantes, *California State Legislature Passes Five Amendments to the California Consumer Privacy Act Before Recess*, HARV. J.L. & TECH. DIGEST (Oct. 2, 2019), <https://jolt.law.harvard.edu/digest/california-state-legislature-passes-five-amendments-to-the-california-consumer-privacy-act-before-recess> [<https://perma.cc/AD6S-9HQZ>] (“Some of Silicon Valley’s largest tech companies were concerned about the implications of this sort of statutory data protection for their business and lobbied extensively to weaken the [California CPA’s] requirements.”).

⁴⁴ *Privacy Act Exemptions*, CAL. CHAMBER OF COM. (Jan. 2022), <https://web.archive.org/web/20230921220923/https://advocacy.calchamber.com/policy/issues/privacy-act-exemptions> (advocating against California CPA covering employees).

⁴⁵ See A.B. 25, 2019 Leg., Reg. Sess., at 92 (Cal. 2019) (“This bill would exempt, until January 1, 2021 . . . information collected from a natural person . . . acting as . . . an employee.”). Authors of A.B. 25 noted that its language was “reflective of a work in progress based on discussion with entities such as the California Chamber of Commerce, Californians for Consumer Privacy, Common Sense Media, and the Internet Association.” REPORT ON A.B. 25, *supra* note 42, at 5. Notably, the voices of labor organizations and groups concerned primarily with representing workers’ rights and interests appear left out, even though the discussion centered on the future of worker data rights under California law. See *id.* at 1.

2023.⁴⁶ When the exemption expired, workers finally became covered under California’s data protection law, more than four years after the legislation was initially passed.

Other state legislatures apparently learned from the controversy over workers in the California CPA. Each of the subsequently enacted state data protection laws expressly excludes workers. For example, the Virginia Consumer Data Protection Act (“VCDPA”) protects “consumer[s],” defined as “a natural person who is a resident of the Commonwealth acting only in an individual or household context,”⁴⁷ and expressly excludes “a natural person acting in a commercial or employment context.”⁴⁸ The VCDPA also restricts which data is protected, exempting “data processed or maintained . . . in the course of an individual applying to, employed by, or acting as an agent or independent contractor.”⁴⁹ The other state privacy statutes similarly define “consumers” to exclude individuals acting in a commercial or employment context,⁵⁰ and exempt employment-related data from coverage.⁵¹ The most prominent federal bills, the ADPPA and APRA, also excluded employee data from protection.⁵²

Employment, however, is not wholly absent from these statutes. The VCDPA provides a typical example. It gives consumers the right to opt out of data

⁴⁶ See California Privacy Rights Act of 2020, 2020 Cal. Legis. Serv. Proposition 24 (West) (codified at CAL. CIV. CODE §§ 1798.100-.199.100) (setting employee exemptions expiration date). The CPRA’s purpose and intent provisions assert that workers’ privacy interests “should also be protected,” while “taking into account the differences in the relationship between employees or independent contractors and businesses as compared to the relationship between consumers and businesses.” *Id.* § 3(A)(8). One notable difference in rights for data subjects who are workers may be found in the CPRA’s anti-retaliation provisions, which offer examples of prohibited retaliation or discrimination against customers, while leaving workers’ rights not to be retaliated against undefined. See CAL. CIV. CODE § 1798.125 (West 2025).

⁴⁷ VA. CODE ANN. § 59.1-575 (2025).

⁴⁸ *Id.*

⁴⁹ *Id.* § 59.1-576(C)(14).

⁵⁰ See sources cited *supra* note 36.

⁵¹ The Colorado Privacy Act contains exclusions for “data maintained for employment records purposes.” COLO. REV. STAT. § 6-1-1304(2)(k) (2025). Using language identical with the Virginia Consumer Data Protection Act (“VCDPA”), the Connecticut and Utah statutes limit the scope of protections to leave out employment-related data for hiring and other employment actions, emergency contact information, and benefits. Compare VA. CODE ANN. § 59.1-576 (2025), with UTAH CODE ANN. § 13-61-102(2)(o) (West 2025), and CONN. GEN. STAT. ANN. § 42-517(b)(15) (West 2025). See also DEL. CODE ANN. tit. 6, § 12D-103(c)(11) (2025); IND. CODE ANN. § 24-15-1-2(13) (West 2025); IOWA CODE § 715D.2(3)(q) (2025); MONT. CODE ANN. § 30-14-2804(o) (2024); OR. REV. STAT. ANN. § 646A.572(i) (West 2025); TENN. CODE ANN. § 47-18-3311(a)(20) (2025); TEX. BUS. & COM. CODE ANN. § 541.003(15)-(17) (West 2025).

⁵² See American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 101(12)(B), (25) (2021) (defining “employee data” and eliminating such from “covered data” definition); American Privacy Rights Act of 2024, H.R. 8818, 118th Cong. § 101(12)(B), (25) (2024) (defining “employee information” and eliminating such from “covered data” definition).

processing that involves “profiling in furtherance of decisions that produce legal or similarly significant effects.”⁵³ “Profiling means any form of automated processing performed on personal data to evaluate” a natural person, and “[d]ecisions that produce legal or similarly significant effects” include “employment opportunities.”⁵⁴ In other words, the statute categorically excludes applicants and employees from the definition of “consumer,” but at the same time gives “consumers” the right to opt out of automated decision systems when used to make employment decisions. Many of the other state statutes have a similar structure, excluding workers from coverage, but giving consumers a right to opt out of profiling used for employment decisions.⁵⁵

These statutes’ treatment of workers and their interests in their data is incoherent because they create a right that, by definition, applies to no one. Perhaps what the legislatures were attempting to do was to exclude workers from most of the individual data protection rights, such as the right to access, correct, or delete their personal data, while giving workers the right to opt-out of automated decision systems. If that is the case, however, not only does the statutory text fail to accomplish such a result, it is unclear what rationale exists for including workers in one type of data processing right and excluding them from all others.

There has also been growing legislative activity at the state level, driven by labor rather than privacy advocates, seeking to enact worker-specific protection from data-driven harms.⁵⁶ Hundreds of bills have been proposed, yet only a small handful have been enacted.⁵⁷ Thus, while there is growing awareness of the close connection between data rights and working conditions, legislation protecting workers has so far failed to gain traction like consumer data protection laws. At the same time, these efforts have the potential to develop models for robust worker protection in the future.

While workers’ interests have largely been overlooked in recent policymaking around data protection, they have been front and center in

⁵³ VA. CODE ANN. § 59.1-577(A)(5)(iii) (2025).

⁵⁴ *Id.* § 59.1-575.

⁵⁵ *See, e.g.,* COLO. REV. STAT. §§ 6-1-1303(6), (10), -1306(1)(a)(C) (2025) (defining “consumer” as “not includ[ing] an individual acting in [an] . . . employment context” and granting right to opt out of “decisions that produce legal or similarly significant effects concerning a consumer,” such as decisions regarding “employment opportunities”). The draft ADPPA also treated workers inconsistently, excluding “employee data” from coverage, H.R. 8152 § 2(8)(B)(ii), while including algorithms that “determin[e] access to . . . employment” under its civil right provisions. *Id.* § 207(c). Thus, in the section addressing algorithmic harms, workers were a focus of concern; elsewhere in the bill they were excluded from protection. *See id.*

⁵⁶ Mishal Khan & Annette Bernhardt, *The Current Landscape of Tech and Work Policy in the U.S.: A Guide to Key Laws, Bills, and Concepts*, UNIV. OF CAL. BERKELEY LAB. CTR. (Sep. 18, 2025), <https://laborcenter.berkeley.edu/tech-and-work-policy-guide> [<https://perma.cc/GN9L-EXXH>] (surveying “current U.S. public policy that regulates employers’ use of digital workplace technologies”).

⁵⁷ *See id.*

conversations about algorithmic decision-making and the risks attendant to the growing use of AI.⁵⁸ For example, when the Algorithmic Accountability Act of 2023 was introduced in Congress,⁵⁹ its co-sponsors prominently featured employment as a central concern. “AI is making choices, today, about who gets hired for a job,” said Senator Ron Wyden in a press release about the bill.⁶⁰ Senator Cory Booker listed “recruiting and hiring tools that discriminate against women and minority candidates” as one of the “real-world examples of AI systems that have flawed or biased algorithms.”⁶¹ The bill’s protections were clearly intended to encompass workers, listing “employment, worker management, or self-employment” among the “critical decisions” that would have been regulated by the Act.⁶² Similarly, some state efforts to address discriminatory or harmful AI have included workers.⁶³

⁵⁸ Workers featured prominently in President Biden’s Executive Order on AI, which instructed agencies across the federal government to take steps to ensure that AI benefits rather than harms society. Exec. Order No. 14110, 88 Fed. Reg. 75191, 75191 (Oct. 30, 2023) (emphasizing “irresponsible use [of AI] could . . . displace and disempower workers”). One of the eight guiding principles and priorities outlined in the Executive Order stated that “[t]he responsible development and use of AI require a commitment to supporting American workers.” *Id.* § 2(c). This principle further prioritized “responsible uses of AI that improve workers’ lives, positively augment human work, and help all people safely enjoy the gains and opportunities from technological innovation.” *Id.* President Trump revoked this Executive Order, emphasizing instead the removal of regulatory barriers to the rapid development of AI. Exec. Order No. 14179, 90 Fed. Reg. 8741, 8741 (Jan. 23, 2025) (“This order revokes certain existing AI policies and directives that act as barriers to American AI innovation . . .”).

⁵⁹ See Algorithmic Accountability Act of 2023, H.R. 5628, 118th Cong. § 2(8) (2023) (defining “critical decision” to include “a decision or judgment that has any legal, material, or similarly significant effect on a consumer’s life relating to access to or the cost, terms, or availability of . . . employment”). The bill had originally been introduced in 2022. See Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. § 2(8) (2022) (including “employment, workers management, [and] self-employment” in definition of “critical decision”); Algorithmic Accountability Act of 2022, S. 3572, 117th Cong. § 2(8) (2022) (same).

⁶⁰ Press Release, Ron Wyden, U.S. Sen. for Or., Wyden, Booker, and Clarke Introduce Bill to Regulate Use of Artificial Intelligence to Make Critical Decisions like Housing, Employment and Education (Sep. 21, 2023), <https://www.wyden.senate.gov/news/press-releases/wyden-booker-and-clarke-introduce-bill-to-regulate-use-of-artificial-intelligence-to-make-critical-decisions-like-housing-employment-and-education> [<https://perma.cc/GPP5-HR9J>].

⁶¹ *Id.* The proposed legislation would have required entities that deploy automated decision systems to conduct impact assessments and to seek to eliminate or mitigate negative impacts that have “legal or similarly significant effects on a consumer’s life” and defined “consumer” broadly to mean “an individual.” H.R. 5628 §§ 3(b)(1)(H), 2(6).

⁶² H.R. 5628, § 2(8). The bill’s requirements apply to any “critical decision” that has a “legal, material, or similarly significant effect” on a consumer’s life, including affecting “access to or the cost, terms, or availability of . . . employment, workers management, or self-employment.” *Id.*

⁶³ See, e.g., Colorado Consumer Protections for Artificial Intelligence Act, COLO. REV. STAT. § 6-1-1701(3)(b) (2025) (including “employment” and “employment opportunity” within “consequential decision” definition).

Policy discussions about AI in the workplace have largely focused on the risks of job displacement, as well as concerns about algorithmic discrimination. These concerns are inextricably related to data protection because AI and other algorithmic decision systems necessarily entail the collection and analysis of data. They are in essence computationally intensive forms of data use. And yet, workers have been treated completely differently depending upon whether a regulatory effort was framed as data protection or algorithmic governance. The near total exclusion of workers from enacted and proposed data protection bills implies that workers lack interests in how their data is collected and used. At the same time, they are a central focus of concerns about potential bias and unfairness in AI and algorithmic decision systems.

II. DATA PROTECTION, PRIVACY, AND WORKERS

What explains the inconsistent treatment of workers in policymaking and governance around data collection and use? Why is it that they are almost entirely excluded from efforts framed in terms of data protection and privacy, while they are at the center of concerns about biased and unfair AI decision-making, which is itself a form of data use? As explored in this Part, the ambiguous situation of workers stems from data protection's roots in privacy law, and the way privacy rights discourse has evolved in the United States. In particular, as the concept of privacy developed to encompass concerns about data protection, the interests of workers were largely overlooked—at least until concerns about discriminatory algorithms became salient in the literature.

Privacy, famously, is a “concept in disarray.”⁶⁴ Its precise meaning is difficult to pin down, encompassing many seemingly distinct concerns.⁶⁵ One strand of privacy theory has long focused on the collection and use of personal information by business and government entities, providing the foundation for the current crop of data protection laws in the United States. This lineage is visible in the recent legislative initiatives, some of which are framed in terms of “data protection” (e.g., VCDPA, Indiana Consumer Data Protection Act, Tennessee Information Protection Act)⁶⁶ and others in terms of “consumer privacy” (e.g., California CPA, Colorado Privacy Act, Texas Data Privacy and Security Act, American Privacy Rights Act),⁶⁷ although all are directed at the same harms and draw on the same set of legal tools.

⁶⁴ DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2008).

⁶⁵ See, e.g., Woodrow Hartzog, *What Is Privacy? That's the Wrong Question*, 88 U. CHI. L. REV. 1677, 1677 (2021) (“Throughout history, privacy has evaded a precise meaning.”); SOLOVE, *supra* note 64, at 40 (“Privacy is not one thing, but a cluster of many distinct yet related things.”).

⁶⁶ See VA. CODE ANN. §§ 59.1-575-585 (2025); IND. CODE ANN. § 24-15 (West 2025); TENN. CODE ANN. §§ 47-18-3301-3315 (2025).

⁶⁷ See CAL. CIV. CODE §§ 1798.100-199.100 (West 2025); COLO. REV. STAT. §§ 6-1-1303-1314 (2025); H.R. 8818, 118th Cong. (2024).

Early conceptions of privacy were rooted in tort and constitutional law and focused on states of being, like seclusion, solitude, or confidentiality.⁶⁸ Legal doctrine looked to social norms to define privacy rights, asking whether individuals had a “reasonable expectation of privacy” in a particular place or thing,⁶⁹ or whether an intrusion was “highly offensive to a reasonable person.”⁷⁰ Privacy law’s traditional focus is on protecting individual dignity and autonomy. Workers receive some protection under this regime, but only for egregious intrusions. Constitutional protections apply only to government employees, and even then, courts frequently find that public employees’ interests in privacy are outweighed by the employers’ need to supervise and control the workplace.⁷¹ For similar reasons, the privacy tort has limited reach in the workplace. It provides redress for norm-violating actions like surreptitious videotaping in employee bathrooms or locker rooms,⁷² but otherwise puts few limits on employers’ ability to collect and exploit worker data.⁷³

⁶⁸ See, e.g., Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 723-24 (1999) (describing liberal conception of privacy informing privacy torts and constitutional provisions as concerned with things like spatial seclusion, solitude, confidentiality, and secrecy); Hartzog, *supra* note 65, at 1677 (explaining earliest privacy rules and frameworks “leveraged specific concepts such as solitude, confidentiality, and substantive due process”); Paul M. Schwartz & William M. Treanor, *The New Privacy*, 101 MICH. L. REV. 2163, 2175-76 (2003) (characterizing “old privacy” as envisioning “privacy-as-sanctuary”).

⁶⁹ See, e.g., *O’Connor v. Ortega*, 480 U.S. 709, 715 (1987) (holding public employee’s claim search violated his Fourth Amendment rights depended upon whether he had reasonable expectation of privacy in places and items searched).

⁷⁰ The intrusion on seclusion tort imposes liability on a defendant “who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person.” RESTATEMENT (SECOND) OF TORTS § 652B (A.L.I. 1977). Liability under the public disclosure tort arises when a defendant “gives publicity to a matter concerning the private life of another . . . if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.” *Id.* § 652D.

⁷¹ See *O’Connor*, 480 U.S. at 719-20 (“In the case of searches conducted by a public employer, we must balance the invasion of the employees’ legitimate expectations of privacy against the government’s need for supervision, control, and the efficient operation of the workplace.”); Stephen Allred, *Employee Privacy and Workplace Searches*, POPULAR GOV’T, Spring 2002, at 33, 34-35 (discussing lower court decisions applying *O’Connor* standard and how standard makes it difficult for employee to assert overriding privacy interest if employer has developed and posted policy informing employees workplace is subject to periodic searches).

⁷² For examples of cases in which courts found privacy violations, see *Acuff v. IBP, Inc.*, 77 F. Supp. 2d 914, 919-36 (C.D. Ill. 1999) (video surveillance of nurse’s office where employees were provided medical treatment); *Johnson v. Allen*, 613 S.E.2d 657, 659-63 (Ga. Ct. App. 2005) (video surveillance of restroom); *Doe v. Dearborn Pub. Schs.*, No. 06-CV-12369-DT, 2008 WL 896066, at *4-6, *10 (E.D. Mich. Mar. 31, 2008) (video surveillance of area gym teachers used to change clothes); *Koeppel v. Speirs*, 808 N.W.2d 177, 180-86 (Iowa 2011) (hidden video camera in restroom).

⁷³ See Pauline T. Kim, *Data Mining and the Challenges of Protecting Employee Privacy Under U.S. Law*, 40 COMPAR. LAB. L. & POL’Y J. 405, 412-15 (2019) [hereinafter Kim, *Data*

As computer databases came into general use in the twentieth century, concerns about secret dossiers and their threats to individual autonomy came to the fore.⁷⁴ These concerns led to the articulation of Fair Information Principles (“FIPs”), which were intended to create rules around the collection and use of personal data.⁷⁵ FIPs typically include principles such as purpose specification, transparency, notice, individual control, access, data quality, and data security.⁷⁶ Much of the early scholarly work on data privacy focused on FIPs, and these principles have been widely incorporated into legal standards.⁷⁷

Significantly, the United States took a sectoral approach to implementing data protection principles.⁷⁸ Protections depend upon the type of information collected and the nature of the entity that holds it, creating fragmented regulation that leaves many sectors and large amounts of data uncovered.⁷⁹ To the extent that federal statutory protections exist, they primarily focus on certain types of consumer information held by large commercial entities. Thus, consumers’ informational interests are protected to some degree when they interact with financial institutions (Gramm-Leach-Bliley Act), seek medical care (Health

Mining] (arguing because privacy torts are aimed at egregious invasions, they offer little protection from firms’ routine data gathering and processing practices).

⁷⁴ See, e.g., ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY 3 (July 28, 2025), <https://bobgellman.com/rg-docs/rg-FIPshistory.pdf> [<https://perma.cc/B7PJ-WNP3>] (explaining Advisory Committee on Automated Personal Data Systems was established in 1970s “in response to growing use of automated data systems containing information about individuals”); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 590 (2014) (“As the Internet began to blossom in the mid-to-late 1990s, . . . privacy became an obvious concern because a significant amount of personal data could be gathered. Data security was another major concern, as many people were reluctant to use the Internet out of fear that their data could be improperly accessed.”).

⁷⁵ NEIL RICHARDS, WHY PRIVACY MATTERS 28-29 (2021).

⁷⁶ See Dan Feldman & Eldar Haber, *Measuring and Protecting Privacy in the Always-On Era*, 35 BERKELEY TECH. L.J. 197, 224 & n.140 (2020).

⁷⁷ See GELLMAN, *supra* note 74, at 14-17.

⁷⁸ Elsewhere, regulators have taken an omnibus approach. In the European Union, data protection is recognized as a fundamental human right, and the default assumption is that personal data should not be collected or processed without legal justification. See Charter of Fundamental Rights of the European Union, arts. 7-8, 2012 O.J. (C 326/391); Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Apr. 11, 1950, 213 U.N.T.S. 221. Rather than developing rules for specific industries or relationships, EU regulation follows the data, imposing requirements on all entities that collect and process personal information. See Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 4, 2016 O.J. (L 119) 1, 35-37; see also Meg Leta Jones & Margot E. Kaminski, *An American’s Guide to the GDPR*, 98 DENV. L. REV. 93, 114 (2020).

⁷⁹ See, e.g., Daniel Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, TEACHPRIVACY (Nov. 13, 2015), <https://teachprivacy.com/problems-sectoral-approach-privacy-law> [<https://perma.cc/DP3B-SUBN>]; RICHARDS, *supra* note 75, at 53; Feldman & Haber, *supra* note 76, at 212-13; Schwartz, *supra* note 14, at 905.

Insurance Portability and Accountability Act), rent videos (Video Privacy Protection Act), or allow their children to access online content (Children's Online Privacy Protection Act),⁸⁰ but these statutes have little relevance in the workplace context.

The Fair Credit Reporting Act ("FCRA"), which also focuses on consumer data, does cover data used for employment purposes.⁸¹ Firms must comply with a number of requirements under the FCRA when accessing consumer reports about applicants or employees, such as providing a clear disclosure that they plan to access such a report and obtaining consumer authorization before doing so.⁸² When a consumer report is used to make an adverse employment decision, the firm must make additional disclosures, including information about the right to dispute the report.⁸³ Even where it applies,⁸⁴ however, the FCRA's protections for workers are rather limited in practice.⁸⁵ The rights it creates are mostly procedural in nature, and it places few substantive limits on what data can be collected and shared.⁸⁶ As a result, it does little to slow firms' vast data gathering practices, nor does it attempt to limit how that data is subsequently used.⁸⁷

Beyond these specific statutory schemes, the Federal Trade Commission plays a prominent role in regulating firms' data practices, a role framed in terms of consumer protection.⁸⁸ Daniel Solove and Woodrow Hartzog describe how the FTC has developed a common law-like body of data privacy jurisprudence through its regulatory activities.⁸⁹ Its authority to do so is grounded in its

⁸⁰ Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338, 1436 (1999) (codified in scattered sections of 12 and 15 U.S.C.) (limiting "financial institutions" from disclosure of individual's "nonpublic personal information"); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, 2023 (1996) (codified in scattered sections of 26, 29, and 42 U.S.C.) (protecting "individually identifiable health information" maintained or disclosed by covered entity or business associate); Video Privacy Protection Act of 1988, Pub. L. 100-618, 102 Stat. 3195 (codified at 18 U.S.C. § 2710) (forbidding video tape service providers from disclosing customers' information); Children's Online Privacy Protection Act of 1998, Pub. L. 105-277, 112 Stat. 2681-728 (codified at 15 U.S.C. §§ 6501-6506) (regulating collection and use of children's personal information by online platforms).

⁸¹ Fair Credit Reporting Act, Pub. L. 91-508, 84 Stat. 1114 (codified at 15 U.S.C. § 1681-1681x) (regulating collection, use, and disclosure of consumer information by consumer reporting agencies).

⁸² Pauline T. Kim & Erika Hanson, *People Analytics and the Regulation of Information Under the Fair Credit Reporting Act*, 61 ST. LOUIS U. L.J. 17, 23 (2016).

⁸³ *Id.* at 23-24.

⁸⁴ The Fair Credit Reporting Act ("FCRA") only applies to a "consumer report" that is obtained from a "consumer reporting agency." *Id.* at 21.

⁸⁵ *Id.* at 32 ("[E]ven if the FCRA is interpreted expansively . . . , it will do little to protect employees from privacy intrusions or unfair or discriminatory uses of their data.").

⁸⁶ *Id.* at 25.

⁸⁷ *Id.* at 25-26, 32.

⁸⁸ Solove & Hartzog, *supra* note 74, at 600 ("Today, the FTC is viewed as the de facto federal data protection authority.").

⁸⁹ *See id.* at 586-87.

Section 5 enforcement powers to prevent “unfair or deceptive acts or practices” that cause or are likely to cause “substantial injury to consumers.”⁹⁰ The FTC’s cases are thus “focused on ensuring that consumers receive the benefit of their bargain in individual business-to-consumer transactions.”⁹¹ As Chander, Kaminski, and McGeeveran put it, United States data privacy law rests on a “transactional consumer protection model” based on “discrete interaction[s]” between consumers and firms.⁹² And although the FTC has in the past indicated its view that workers are covered under the fairness protections,⁹³ its enforcement efforts have been overwhelmingly focused on consumers.⁹⁴

Because most laws are framed in terms of consumers, workers’ interests in controlling their personal data are largely overlooked in discussions of data protection. Apart from the FCRA, only a handful of narrowly drawn regulations offer any protection for workers’ personal information.⁹⁵ For example, federal anti-discrimination statutes limit the collection and use of genetic information and prohibit medical inquiries at certain times in the hiring process.⁹⁶ These provisions may act as data protection rules, but are primarily aimed at preventing genetic or disability discrimination.⁹⁷ A scattering of state laws also regulates employer data collection, but these laws are even narrower in scope and effect. Typically, they reach only very specific types of information—for example, social media passwords⁹⁸—and their protections often require no more than

⁹⁰ *Id.* at 599; 15 U.S.C. §§ 45(a), (n).

⁹¹ Chander et al., *supra* note 22, at 1747.

⁹² *Id.* at 1748.

⁹³ FTC, POLICY STATEMENT ON ENFORCEMENT RELATED TO GIG WORK 10-11 (Sep. 15, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Matter%20No.%20P227600%20Gig%20Policy%20Statement.pdf [<https://perma.cc/5TGW-W3JE>]; see also Benjamin Wiseman, Assoc. Dir., Div. of Priv. & Identity Prot., FTC, Remarks at the Harvard Journal of Law and Technology on Worker Surveillance and AI 5-7 (Feb. 8, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Jolt-2-8-24-final.pdf [<https://perma.cc/AR3F-V4R2>] (“[T]he FTC will not hesitate to combat emerging privacy harms and other abuses in the marketplace. The same applies to worker surveillance.”).

⁹⁴ See Solove & Hartzog, *supra* note 74, at 586 (arguing FTC’s jurisprudence focuses on consumer expectations of privacy).

⁹⁵ See Hirsch, *supra* note 1, at 931 (summarizing statutory protections for employee privacy and their limited coverage).

⁹⁶ See, e.g., 42 U.S.C. § 12112(d) (imposing restrictions on medical examinations and inquiries); 42 U.S.C. § 2000ff-1(a) (prohibiting employers from discriminating based on genetic information); Kim, *Data Mining*, *supra* note 73, at 408-11 (discussing federal laws that protect employees’ from discrimination on basis of medical and genetic information).

⁹⁷ Kim, *Data Mining*, *supra* note 73, at 408.

⁹⁸ See *Privacy of Employee and Student Social Media Accounts*, NAT’L CONF. OF STATE LEGISLATURES, <https://www.ncsl.org/technology-and-communication/privacy-of-employee-and-student-social-media-accounts> (Aug. 8, 2022) (“State lawmakers began introducing legislation beginning in 2012 to prevent employers from requesting passwords to personal Internet accounts to get or keep a job.”).

giving notice⁹⁹ and are waivable if the employee consents.¹⁰⁰ These narrow statutory provisions, together with the common law and constitutional rights discussed earlier, provide only a thin patchwork of protection for workers' privacy interests.¹⁰¹ And because these laws focus on narrowly defined types of information or particularly egregious intrusions, they are ill suited to protect workers against the cumulative impact of routine yet massive data gathering and processing practices of firms.¹⁰²

The law's inattention to workers' interest in their data is also apparent in privacy law scholarship's implicit focus on consumers and relative neglect of workers. Privacy law scholars have argued that rampant data collection and exploitation by government and business entities cause significant individual and societal harms.¹⁰³ They have decried the law's excessive reliance on notice and consent to protect privacy, arguing that people's limited time, attention, and cognitive resources make the prospect of "privacy self-management" wholly illusory.¹⁰⁴ And they have criticized the United States's narrow sectoral

⁹⁹ Some, such as electronic monitoring statutes, simply require employers to give notice of the fact of surveillance and typically do not require further disclosures of exactly what data is collected and how it will be used. *See, e.g.*, CONN. GEN. STAT. ANN. § 31-48d (West 2025); DEL. CODE ANN. tit. 19, § 705 (2025); N.Y. CIV. RIGHTS LAW § 52-c(2) (McKinney 2025).

¹⁰⁰ The Illinois Biometric Information Privacy Act, for example, has generated a great deal of litigation in part because firms were unaware of its requirements. Firms can easily protect themselves from challenges by their workers by giving notice and requiring consent as a condition of employment. *See* 740 ILL. COMP. STAT. ANN. 14/15 (West 2025).

¹⁰¹ *See, e.g.*, Hirsch, *supra* note 1, at 933-37 (observing current state statutes regulating employer monitoring are varied and inadequate to protect against current and future technologies); Bales & Stone, *supra* note 1, at 30 (noting existing statutes and common law doctrines "do not address the problem of scale and scope of today's surveillance capabilities").

¹⁰² *See* Kim, *Data Mining*, *supra* note 73, at 407.

¹⁰³ *See, e.g.*, Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 796-97 (2022); RICHARDS, *supra* note 75, at 75 ("[T]he unwanted disclosure of many kinds of information about ourselves can have deeply harmful consequences to our identity, to our livelihood, to our political freedom, and to our psychological integrity."); Hartzog & Richards, *supra* note 26, at 1725; Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1891-93 (2013); Margot E. Kaminski, *The Case for Data Privacy Rights (or, Please, a Little Optimism)*, 97 NOTRE DAME L. REV. REFLECTION 385, 386 (2022).

¹⁰⁴ *See, e.g.*, RICHARDS, *supra* note 75, at 54-56 ("[Privacy self-management] pretends to be agnostic about the substance of privacy rules, while everyone knows that the power to set defaults over harried and confused consumers is the real power to decide the substance of these rules—literally—by default."); Hartzog & Richards, *supra* note 26, at 1734 (contending notice and choice models "create incentives for companies to hide the risks in their data practices through manipulative design, vague abstractions, and complex words as [they] also shift risks onto data subjects," and are a "spectacular failure" (quoting Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1498-99 (2019))); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 434 (2016) (arguing under notice and choice regime, "[c]onsumers are left exposed and bewildered, lamenting what they see as the 'death of privacy'" (quoting

approach, which relies on industry-specific rules rather than comprehensively regulating dataflows across entities in omnibus fashion.¹⁰⁵

In this rich literature, there is an imagined data subject that drives the analysis—a person situated in particular ways that create vulnerabilities and risks of harm. Most often, that person is imagined as a consumer, such as Ryan Calo’s “mediated” consumer,¹⁰⁶ or Neil Richards’ “situated” consumer,¹⁰⁷ or more generically as consumers subject to surveillance by commercial entities.¹⁰⁸ Consumers are vulnerable to large commercial entities that collect their personal information in increasingly granular form—tracking their movements, recording their behavior, and sensing their physiological states—and then leveraging that data to build precise individual profiles and predict future behavior.¹⁰⁹

These practices are the foundation of what Shoshana Zuboff calls “surveillance capitalism” and Julie Cohen has described as “informational capitalism.”¹¹⁰ In this system, firms’ data practices open the door to multiple types of harms. Consumers may be misled about when their information is collected and how it will be used.¹¹¹ They may be manipulated into buying

Neil M. Richards, *Four Privacy Myths*, in *A WORLD WITHOUT PRIVACY?* 33 (Austin Sarat ed., 2015)); Solove, *supra* note 103, at 1883-86.

¹⁰⁵ See, e.g., RICHARDS, *supra* note 75, at 53-54; Feldman & Haber, *supra* note 76, at 212-13. But see Schwartz, *supra* note 14, at 905 (arguing “federal sectoral statutes have more promise for information privacy”).

¹⁰⁶ Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1003-18 (2014) (discussing the “mediated” consumer).

¹⁰⁷ RICHARDS, *supra* note 75, at 184-90 (discussing the “situated” consumer).

¹⁰⁸ See, e.g., SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* 82 (2019) (describing how individuals are objects from which data is extracted); Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1384 (2017) (focusing on privacy interests of consumers); Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32, 32 (2011) [hereinafter Nissenbaum, *A Contextual Approach*] (same); HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* 31-46 (2009) [hereinafter NISSENBAUM, *PRIVACY IN CONTEXT*].

¹⁰⁹ See, e.g., Nissenbaum, *A Contextual Approach*, *supra* note 108, at 33 (exploring growing concern over “pervasive surreptitious tracking, manipulative behavioral advertising, and fickle privacy commitments”); Wolfie Christl, *How Companies Use Personal Data Against People* 29 (Cracked Labs, Working Paper, Oct. 2017), [https://crackedlabs.org/dl/CrackedLabs_Christl_Data Against People.pdf](https://crackedlabs.org/dl/CrackedLabs_Christl_Data%20Against%20People.pdf) [https://perma.cc/LPK9-TCR3] (“Pervasive digital tracking and profiling... [has] become a powerful toolset for systematically influencing behavior.”).

¹¹⁰ ZUBOFF, *supra* note 108; JULIE E. COHEN, *BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM* (2019).

¹¹¹ See, e.g., WOODROW HARTZOG, *PRIVACY’S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES* 142 (2018); Gregory Conti & Edward Sobiesk, *Malicious Interface Design: Exploiting the User*, WWW, 2010, at 272-73; Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 442-45 (2018).

products or services they do not need or on terms that are disadvantageous.¹¹² Their data may be sold to other entities for unknown future uses, or exposed through data breaches to nefarious actors, putting them at greater risk of identity theft or fraud.¹¹³ And consumers' personal data may be aggregated with other data and analyzed to infer sensitive information such as health risks or sexual behaviors.¹¹⁴ The cumulative impact is to undermine consumers' autonomy and exploit their individual vulnerabilities, while enabling firms to extract surplus value and concentrate their own wealth.¹¹⁵

Insufficient data protection affects more than consumers' material interests. Lack of privacy protections has rendered marginalized persons vulnerable to degrading exposure through revenge porn and other forms of racist and misogynistic abuse.¹¹⁶ Privacy is also critical to creativity and innovation because it provides interstitial spaces for behavioral variation and experimentation,¹¹⁷ and it is necessary for intellectual exploration.¹¹⁸ Thus, the data subject is also recognized as a *citizen*—someone who is a member of multiple, overlapping communities and has capacities to explore, learn, create, and build relationships. And because the flourishing of citizens is essential for self-governance, inadequate data protection threatens our democratic institutions.¹¹⁹

¹¹² See, e.g., Ryan Calo & Alex Rosenblat, *The Taking Economy: Uber, Information, and Power*, 117 COLUM. L. REV. 1623, 1651 (2017); Michal Lavi, *Manipulating, Lying, and Engineering the Future*, 33 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 221, 270-76 (2023); Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES L. 157, 171-72 (2019); Calo, *supra* note 106, at 996.

¹¹³ See Andrew M. Parks, *Unfair Collection: Reclaiming Control of Publicly Available Personal Information from Data Scrapers*, 120 MICH. L. REV. 913, 923-24 (2022); Elvy, *supra* note 111, at 445-46, 452; Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>.

¹¹⁴ See, e.g., Anya E.R. Prince, *Reproductive Health Surveillance*, 64 B.C. L. REV. 1077, 1090-91 (2023).

¹¹⁵ See COHEN, *supra* note 110, at 6.

¹¹⁶ Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1890, 1908, 1919-20 (2019) (noting sexual privacy invasions disproportionately harm women and marginalized communities); Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 347-50 (2014).

¹¹⁷ Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1905 (2013) ("Privacy shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable."); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1424-26 (2000) [hereinafter Cohen, *Examined Lives*].

¹¹⁸ See, e.g., NEIL RICHARDS, *INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE* 16-18 (2015) (noting "[i]f we are interested in the development of new ideas and new, original speech, we must safeguard the processes of intellectual explorations" by guaranteeing intellectual privacy).

¹¹⁹ Cambridge Analytica's efforts to sway the 2016 election by manipulating Facebook's user data is often offered as a salient example of the threats to democracy posed by insufficient

While recognizing the importance of data protection for the consumer and citizen, the privacy law literature has paid little sustained attention to *workers* as data subjects. Articles and books that purport to address data protection comprehensively often fail to discuss workers at all. When they do, it is often just a passing mention—for example, the worry that consumers’ private information will get into the hands of their employers.¹²⁰ Mainstream privacy law literature seems to assume that workers’ data interests are of marginal concern or can be subsumed within protections for consumer data. To the extent that workers’ privacy rights have been addressed in the literature, they have largely been treated separately, most often by labor law scholars writing about the distinct topic of “workplace privacy.”¹²¹

This lack of broader attention to workers is somewhat curious, given that privacy law theorists often emphasize that control over information is not just about avoiding individual exposures, but about how power is distributed and wielded.¹²² The workplace has long been a prime site for contestation over power in industrial societies, and it is one of the principal places in which shifts in power in our “information economy” are playing out today. Julie Cohen, one of the few privacy law scholars to have given this dynamic sustained attention, describes how the “informationalization of production” has restructured work

data protections. See Karl Manheim & Lyric Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 YALE J.L. & TECH. 106, 109-10 (2019) (“Perhaps the biggest social cost of the new technological era of AI is the erosion of trust in and control over our democratic institutions.”); Hartzog & Richards, *supra* note 26, at 1709-11 (detailing how Cambridge Analytica “illicitly gathered personal data on millions of American Facebook users to be deployed for manipulation of their votes and other electoral meddling”); Ezra Wolfson, *Privacy in the Digital Age: Is Our Data Safe?*, 3 INT’L COMPAR., POL’Y & ETHICS L. REV. 477, 481-90 (2020) (arguing need for action following Cambridge Analytica scandal).

¹²⁰ See, e.g., Kaminski, *supra* note 103, at 390; Citron & Solove, *supra* note 103, at 837-41 (discussing reputational harms to workers when employer decisions are based on erroneous information); Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent*, 93 TEX. L. REV. 85, 93-94 (2014) (arguing data collection from Internet of Things devices “may lead to new forms of economic discrimination as lenders, employers, insurers, and other economic actors, use [such] data to sort and treat differently unwary consumers”).

¹²¹ See, e.g., Paul M. Secunda, *Privatizing Workplace Privacy*, 88 NOTRE DAME L. REV. 277, 278 (2012); Matthew W. Finkin, *Employee Privacy, American Values, and the Law*, 72 CHI.-KENT L. REV. 221, 239-42 (1996); Lawrence E. Rothstein, *Privacy or Dignity?: Electronic Monitoring in the Workplace*, 19 N.Y.L. SCH. J. INT’L & COMPAR. L. 379, 379 (2000).

¹²² See, e.g., Neil M. Richards & Woodrow Hartzog, *A Relational Turn for Data Protection?*, 6 EUR. DATA PROT. L. REV. 492, 493 (2020); Lisa M. Austin, *Enough About Me: Why Privacy Is About Power, Not Consent (or Harm)*, in *A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO?* 131-89 (Austin Sarat ed., 2014); Daniel J. Solove, *Privacy and Power, Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1396-1402 (2001); Julie E. Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIRIES L. 1, 5-10 (2019).

relations, increasing precarity for workers and giving rise to the gig economy.¹²³ As explained in the next Part, these changes allow firms to extract more surplus value from labor and to concentrate their own wealth. However, because the privacy law literature has mostly conceived of the data subject as consumer or citizen, the recent moves toward data protection legislation are framed as consumer protection, with workers' interests excluded.

Discussions around algorithmic discrimination are the exception to the relative neglect of workers in the privacy law literature. As AI and other automated decision systems have become more pervasive in society, the literature has taken an "algorithmic turn,"¹²⁴ drawing attention to a broader array of harms that result from the processing of data. Expanding beyond privacy law's traditional concerns with dignity and autonomy, scholars have pointed to harms that are more tangible, and often economic in nature. In particular, a significant focus has been on algorithmic discrimination, and employment is typically cited as a core area where screening and ranking algorithms can cause discriminatory harm, depriving members of disadvantaged groups of employment opportunities.¹²⁵

While recognizing the risks of discrimination in the workplace, this literature has paid far less attention to the myriad other ways automated systems can degrade working conditions and undermine established workers' rights. As a result, although workers were included in proposals for algorithmic governance like the Algorithmic Accountability Act, the intended scope of protections was unclear.¹²⁶ The draft legislation called for impact assessments of algorithmic systems and cited concerns about discrimination, security, and privacy, but did not mention impacts such as effects on working conditions and inequality.¹²⁷

III. WORKPLACE DATA PRACTICES

If the mainstream privacy law literature has paid scant attention to workers, scholars in other fields have thoroughly documented how increased datafication of the workplace is undermining workers' rights. For example, sociologist Karen Levy offers a detailed analysis of how intensified data collection and analysis have significantly worsened working conditions for long haul truck drivers.¹²⁸ Other scholars have described ways in which firms' collection and processing of worker data can facilitate discrimination, contribute to work instability,

¹²³ COHEN, *supra* note 110, at 30-33.

¹²⁴ Maria P. Angel, *Privacy's Algorithmic Turn*, 30 B.U. J. SCI. & TECH. L. 1, 2-3 (2024); Hartzog, *supra* note 65, at 1681.

¹²⁵ See, e.g., Barocas & Selbst, *supra* note 10, at 677-93; Kim, *Data-Driven Discrimination*, *supra* note 10, at 883-92; Ifeoma Ajunwa, *The Paradox of Automation as Anti-Bias Intervention*, 41 CARDOZO L. REV. 1671, 1712-14 (2020).

¹²⁶ See Algorithmic Accountability Act of 2025, H.R. 5511, 119th Cong. (2025).

¹²⁷ See *id.*

¹²⁸ See, e.g., KAREN LEVY, DATA DRIVEN: TRUCKERS, TECHNOLOGY, AND THE NEW WORKPLACE SURVEILLANCE 151 (2023).

undermine worker bargaining power, compromise health and safety, and lead to lowered compensation.¹²⁹ In addition, massive data collection and advanced computing tools promote fissuring of the workplace, replacing traditional employment with contracting arrangements, and fueling the rise of the gig economy.¹³⁰ As a result, those workers lack the legal safeguards provided to employees through minimum standards legislation.

This Part provides an overview, explaining how firms today are leveraging worker data to manage labor and how new automated tools are undermining basic workers' rights. It explains why workers, as data subjects, have interests in restricting the collection and use of their personal data by the firms that employ them that are as compelling, if not more so, than consumers' interests.

A. *Data Collection and Algorithmic Management*

Even before the digital age, firms collected information about individual workers, such as basic contact and background information, and records of work performance. Personnel records were closely tied to the individual worker, and the central concerns were misuse and disclosure of confidential, sensitive information by a supervisor or manager. Digital technologies have caused a sea change in both the nature of workplace data collection and the potential risks it poses.

Today, firms collect enormous amounts of data from workers using digital interfaces, electronic monitoring tools, and surveillance systems. This vast trove of information has in turn driven innovation in algorithmic techniques, providing firms with new tools for managing their workforce. Workers are subject to data collection from their first contact with a firm, and that data in turn feeds algorithmic management systems that are then used to create inferences, make predictions, and to inform or assist personnel decisions with little or no legal limitations.

Consider first the hiring process. In addition to information that applicants provide about their background and experience, firms also harvest information about how those applicants interacted with their online system, recording, for example, what browser each individual used,¹³¹ or how long it took to provide

¹²⁹ See sources cited *supra* note 1; see also Karen Levy & Solon Barocas, *Refractive Surveillance: Monitoring Customers to Manage Workers*, 12 INT'L. J. OF COMM'N 1166, 1171-78 (2018); MARY L. GRAY & SIDDHARTH SURI, *GHOST WORK: HOW TO STOP SILICON VALLEY FROM BUILDING A NEW GLOBAL UNDERCLASS*, at xxiii-xxxi (2019); Veena Dubal, *On Algorithmic Wage Discrimination*, 123 COLUM. L. REV. 1929, 1986-87 (2023); Matthew T. Bodie, *The Law of Employee Data: Privacy, Property, Governance*, 97 IND. L.J. 707, 735-36 (2022).

¹³⁰ Dubal, *supra* note 129, at 1969-76; Jeremias Adams-Prassl, *What If Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work*, 41 COMPAR. LAB. L. & POL'Y J. 123, 123-25 (2019); Newman, *supra* note 2, 714-25; Bodie, *supra* note 129, at 735-36.

¹³¹ See Ajunwa et al., *supra* note 1, at 742; see also Rebecca J. Wilson, Kiley M. Belliveau & Leigh Ellen Gray, *Busting the Black Box: Big Data, Employment and Privacy*, 84 DEF.

certain responses or to complete a form.¹³² If applicants submit a resume or record a video interview, firms collect additional data beyond the contents, such as by analyzing word choices in a written document or attempting to discern emotions through voice and facial analysis.¹³³ Still more information about an applicant may be scraped from social media or purchased from third-party data brokers. Some firms require applicants to take online tests or play video games to harvest additional data about individual behaviors and response times.¹³⁴

Once hired, firms collect highly granular information about workers' location, activities, and even physiological states while on the job.¹³⁵ Computer monitoring software tracks keyboard strokes and other activity, sending a real-time record of a worker's apparent level of engagement.¹³⁶ Workers may be required to wear activity trackers that provide precise information about their location and movements, while also collecting biometric data, enabling inferences about their physiological states or medical conditions.¹³⁷ Video surveillance, voice analysis, and facial recognition systems are similarly used to track workers' interactions with others and try to discern emotional states.¹³⁸

This vast amount of data collection fuels algorithmic tools that aid firms in all aspects of labor management. The hiring process involves multiple stages to sort and narrow the pool of potential candidates, and each can be algorithmically driven.¹³⁹ Algorithms influence who learns about a job opportunity and who actually applies.¹⁴⁰ Once an application has been received, AI tools analyze candidates' profiles, screen their resumes, and rate their interview performances.¹⁴¹ These algorithms rate applicants' suitability for a job, and recommend whom to hire and how much to pay.

COUNS. J. 1, 12 (2017) (observing employers' use of big data in hiring extends beyond information applicants knowingly submit).

¹³² See Jodi Kantor & Arya Sundaram, *The Rise of the Worker Productivity Score*, N.Y. TIMES (Aug. 14, 2022), <https://www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html> (showcasing how firms gather data, including metrics like response times and browser information as part of monitoring practices).

¹³³ See, e.g., Bales & Stone, *supra* note 1, at 11-12, 24-25 (2020) (illuminating how firms use AI tools to evaluate word choice and assess applicants' tone, voice, and facial expressions).

¹³⁴ *Id.* at 12-13; see also Kathleen McGarvey Hidy & Mary Sheila E. McDonald, *Risky Business: The Implications of Social Media's Increasing Role in Employment Decisions*, 18 J. LEGAL STUD. BUS. 69, 74 (2013).

¹³⁵ Bernhardt et al., *supra* note 2, at 6-7; Ajunwa et al., *supra* note 1, at 772.

¹³⁶ Use of this type of monitoring software expanded greatly during the pandemic with the rise in work-from-home arrangements. See Kantor & Sundaram, *supra* note 132.

¹³⁷ Ajunwa et al., *supra* note 1, at 766.

¹³⁸ See Bales & Stone, *supra* note 1, at 17-19.

¹³⁹ MIRANDA BOGEN & AARON RIEKE, HELP WANTED: AN EXAMINATION OF HIRING ALGORITHMS, EQUITY, AND BIAS 14-43 (2018).

¹⁴⁰ Pauline T. Kim, *Manipulating Opportunity*, 106 VA. L. REV. 867, 875-81 (2020).

¹⁴¹ BOGEN & RIEKE, *supra* note 139, at 25-38.

On the job, workers are subjected to additional forms of automated management.¹⁴² Scheduling software determines when, where, and for how long they are assigned to work.¹⁴³ Algorithms judge workers' on-the-job performance, capture their interactions with co-workers or customers, and assess their emotional states, or morale.¹⁴⁴ These evaluations in turn drive decisions about who gets promoted, disciplined, or even terminated. For example, Amazon has reportedly used AI tools to monitor the speed of warehouse workers and enforce demanding productivity standards.¹⁴⁵ Other companies rely on voice analysis to assess the quality of call center workers' interactions with customers.¹⁴⁶

None of this is inevitable. Companies decide what data to collect in the first place, and how it will be used. Even where there is a legitimate reason to use a certain technology, a firm has many choices as to *how* it will actually be deployed. For example, an employer may need to use tracking devices in order to be able to locate critical employees in real time. Nevertheless, numerous choices remain. Will that tracking device collect other types of information in addition to location, such as movements, biometric data, or social interactions? What will happen to the data collected? How long will it be stored and where? Who will have access to it? Will it be used, not just to assign work tasks, but also to measure individual worker performance or to impose discipline? Will it be used to infer sensitive personal information or detect incipient worker organizing efforts?

The growth of algorithmic management tools is driving increased appetite for worker data. Tools that are deployed for one purpose often end up collecting additional information simply because it is possible to do so.¹⁴⁷ That data is then used to build novel management tools. In order for those tools to be most effective, more and more data is needed to train the algorithms that underlie them.¹⁴⁸ Thus, the trend is toward vastly increasing the types and granularity of

¹⁴² Bernhardt et al., *supra* note 2, at 6.

¹⁴³ *Id.* at 7.

¹⁴⁴ *Id.* at 6-7; *see also* Bales & Stone, *supra* note 1, at 17-18 (highlighting how wearable devices can “track workers’ precise locations and hand movements, gauging workers’ productivity and accuracy[,] . . . measure[] employees’ moods[,] . . . monitor heart rates, stress levels, and other physiological and psychological states”).

¹⁴⁵ Colin Lecher, *How Amazon Automatically Tracks and Fires Warehouse Workers for ‘Productivity,’* VERGE (Apr. 25, 2019, at 12:06 ET), <https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations> [<https://perma.cc/72EW-B7QD>] (observing Amazon utilizes “deeply automated tracking and termination process” to “fire[] more than 10 percent of its staff annually, solely for productivity reasons”).

¹⁴⁶ *E.g.*, Tom Simonite, *This Call May Be Monitored for Tone and Emotion*, WIRED (Mar. 19, 2018, at 07:00 ET), <https://www.wired.com/story/this-call-may-be-monitored-for-tone-and-emotion> [<https://perma.cc/Z3UH-UCG8>] (reporting insurer MetLife’s usage of program called Cogito to monitor both its workers’ and customers’ reactions in conversations).

¹⁴⁷ *See, e.g.*, LEVY, *supra* note 128, at 8.

¹⁴⁸ *See, e.g.*, Hirsch, *supra* note 1, at 897.

personal information collected about workers. Advanced computing techniques permit firms to exploit that data in new ways, providing previously unavailable insights through statistical inferences or predictions about specific workers.¹⁴⁹ These new algorithmic management tools, powered by workers' data, are fundamentally reshaping the work relationship, affording firms increased power that threatens workers' interests and undermines established labor rights in a number of ways.

B. *Potential Harms to Workers' Rights*

The harms posed by excessive and unjustified data gathering by employers have traditionally been cast in terms of privacy. Scholars and advocates criticized intrusive surveillance and monitoring practices because they threaten humiliating exposures and undermine workers' dignity and autonomy.¹⁵⁰ The widespread availability of electronic monitoring tools exacerbates these risks, ratcheting up levels of scrutiny and imposing even more degrading conditions of work. For example, Karen Levy has documented how long-haul trucking firms used concerns about safety to intensify scrutiny of drivers, monitoring not just their behavior, but also measuring their physiological states in real time.¹⁵¹ In order to exercise even greater control, some utilize wearable technologies like the SmartCap, "a baseball cap . . . that detects fatigue by monitoring a driver's brainwaves," or deploy driver-facing cameras that "monitor a driver's eyelids and head position for signs of fatigue or inattention."¹⁵² "If the driver's eyes close or look away from the road for too long, it sounds an alarm and sends a video to his boss."¹⁵³ An analogous device for the office is a "smart" chair cushion that can record and report the occupant's posture, heart rate, and time spent sitting.¹⁵⁴

By intensifying the degree of scrutiny and the intrusiveness of the monitoring, these technologies certainly implicate traditional privacy concerns about dignity

¹⁴⁹ See, e.g., Alex Tray, *Advanced Machine Learning Algorithms for HR Analytics*, COMM'NS ASS'N FOR COMPUTING MACH. (Dec. 5, 2024), <https://cacm.acm.org/blogcacm/advanced-machine-learning-algorithms-for-hr-analytics> [<https://perma.cc/T3GL-L4GA>].

¹⁵⁰ See, e.g., Anita Bernstein, *Foreword: What We Talk About When We Talk About Workplace Privacy*, 66 LA. L. REV. 923, 924-30 (2006); Larry O. Natt Gantt II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345, 414-15 (1995) ("[M]odern theorists have called employers to 'respect their employees [sic] personal dignity and integrity by allowing them sufficient autonomy to function without constant and ubiquitous supervision and inspection . . .'").

¹⁵¹ LEVY, *supra* note 128, at 4-11. Although federal regulations required the use of electronic logging devices to address concerns about driver fatigue and road safety, firms leveraged these technologies to increase their control over workers' behaviors and to expand the types of data they collected.

¹⁵² *Id.* at 145.

¹⁵³ *Id.* at 145-46.

¹⁵⁴ Tiffany May & Amy Chang Chien, *Slouch or Slack Off, This 'Smart' Office Chair Cushion Will Record It*, N.Y. TIMES (Jan. 12, 2021), <https://www.nytimes.com/2021/01/12/world/asia/china-office-cushion-surveillance.html>.

and autonomy. As Levy observes, the increasing use of monitoring technologies and AI in the work of truck driving “is experienced as an intimate biological incursion into their work and bodies.”¹⁵⁵ Indeed, “from the truckers’ point of view, there’s something viscerally offensive about the micromanagement enabled by these technologies.”¹⁵⁶ These types of dignitary harms are real harms that can have concrete effects on workers’ stress levels, work satisfaction, and mental health,¹⁵⁷ but because they are difficult to measure or quantify, they are often hard to vindicate legally.

The advent of big data and algorithmic management tools, however, represents not just an intensification of traditional practices, but a difference in kind. The availability of real-time, granular information about workers’ activities, joined with sophisticated computational tools, threatens to inflict new types of injuries on workers. The potential harms from these data practices are not just, or even primarily, about offensive intrusions or the revelation of personal information.¹⁵⁸ Instead, exploitation of workers’ data can lead to a wide range of material injuries.

1. Labor Displacement and Deskilling

Collection of data from workers about how they perform their work allows firms to build automated systems that can replace those workers or automate some of their tasks, substantially altering the nature of their work. Fears about technology replacing workers are long-standing, dating back to the beginning of the industrial revolution, but those concerns mostly focused on factory jobs. However, the assumption that white-collar workers are not easily replaced by machines has been unsettled by advances in generative AI.

When the effect of automation was primarily felt by workers who performed physical labor, the creation of the technology may have seemed independent of the worker. Now that white-collar jobs are threatened, the crucial role of data—

¹⁵⁵ LEVY, *supra* note 128, at 151.

¹⁵⁶ *Id.* at 148. A consequence of this monitoring is that truckers are essentially restricted from listening to their own bodies and relying on the specialized knowledge that they have accumulated and long prided themselves on. While a driver might contend that he is tired or that the weather conditions are hazardous, dispatchers with access to collected data may insist otherwise. *Id.* at 59-61. This type of micromanagement contravenes the independence that “initially attracted [many drivers] to the profession” and which “serves as a strong source of professional pride.” *Id.* at 60. As a result, “[t]ruckers resist surveillance to preserve their coveted privacy and independence, and to reestablish their long-held occupational autonomy,” using tactics ranging from physically tampering with electronic monitoring devices, retroactively editing collected data, exploiting technical loopholes, or using coordinated social efforts toward resistance, such as “collaborative omission.” *Id.* at 93-113.

¹⁵⁷ Hanna Kinowska & Łukasz Jakub Sienkiewicz, *Influence of Algorithmic Management Practices on Workplace Well-Being—Evidence from European Organisations*, 36 INFO. TECH. & PEOPLE 21, 27, 34 (2023).

¹⁵⁸ Kim, *Data Mining*, *supra* note 73, at 415 (arguing common law torts are “not geared toward addressing the privacy risks posed by data mining techniques” because of doctrine’s “focus[] on highly offensive intrusions or the collection of sensitive information”).

specifically data generated by workers—has become more apparent. For example, one of the key issues in the recent writers’ strike in Hollywood was whether or to what extent firms could use prior scripts—data produced through the writers’ labor—as training materials for generative AI to develop new scripts.¹⁵⁹ Similarly, the Screen Actors Guild-American Federation of Television and Radio Artists (“SAG-AFTRA”) strike challenged whether studios could collect digital representations of actors’ faces and bodies in order to generate artificial images or video, replacing the need for their physical presence.

Technologies like language or image-generating AI systems were not invented in some sterile laboratory. The basic models were trained on massive amounts of data, and that data was produced through human labor.¹⁶⁰ For example, image recognition capabilities first required that humans—performing either compensated or uncompensated labor—label millions and millions of images to train the AI system.¹⁶¹ Similarly, large language models were developed by ingesting immense amounts of human-generated text.¹⁶² Adapting those tools to make them useful for specific purposes, like writing scripts or news articles, will require yet more data—again produced by human labor. In other words, these new technologies cannot be used to replace human labor without workers first creating the data needed to train them. Thus, the concerns about job security that were central in the Hollywood writers’ and SAG-AFTRA strikes were struggles over worker data.

In addition to the risks of displacement, the introduction of algorithms and robots into the workplace has led to an increasingly polarized or “hollowed out” labor market, with workers encountering “declining job quality and wages.”¹⁶³ Data derived from human workers enabled employers to “deskill or ‘homogenize’ work” by redesigning the process and scope of work to require less specialized knowledge or training.¹⁶⁴ Firms could study how workers performed their jobs and use that data to fracture work into a series of discrete

¹⁵⁹ Daniel Arkin, *Hollywood Screenwriters Don’t Want Robots Taking Their Jobs, Either*, NBC NEWS (May 4, 2023, at 14:52 ET), <https://www.nbcnews.com/news/writers-strike-2023-hollywood-screenwriters-ai-concerns-rcna82543> [<https://perma.cc/54VH-LF EY>].

¹⁶⁰ See, e.g., Hirsch, *supra* note 1, at 897.

¹⁶¹ See KATE CRAWFORD, ATLAS OF AI: POWER, POLITICS, AND THE PLANETARY COSTS OF ARTIFICIAL INTELLIGENCE 69 (2021) (pointing out Google’s image recognition algorithms “depend[] on . . . extraction of mass . . . labor to fine-tune . . .”); GRAY & SURI, *supra* note 129, at 7 (“[T]o train machines to recognize the main object in an image, . . . [researchers] use[d] about 49,000 workers from 167 countries to accurately label 3.2 million images.”).

¹⁶² Stephanie Kirmer, *How Human Labor Enables Machine Learning*, MEDIUM (Oct. 31, 2023), <https://medium.com/data-science/how-human-labor-enables-machine-learning-367fccc8bc91> (“LLMs [i.e., large language models] require extraordinary quantities of text data to train. . . . [A]ll that data is generated by people, it doesn’t just appear on our hard drives by magic.”).

¹⁶³ CYNTHIA ESTLUND, AUTOMATION ANXIETY: WHY AND HOW TO SAVE WORK 13, 32 (2021).

¹⁶⁴ ROGERS, *supra* note 1, at 25.

tasks, incorporating automation for some tasks, leaving other limited tasks that require little training for workers to perform.¹⁶⁵ Surveillance technology and algorithmic management then monitor task completion, reinforcing the effect of deskilling by “replicat[ing] and captur[ing] some of workers’ tacit knowledge.”¹⁶⁶

Levy’s work provides a notable illustration of deskilling in the trucking industry. The introduction of electronic monitoring technologies in trucking has led to decreased need for truckers to attain specialized knowledge of local routes or even rely on their own knowledge about their fatigue and stamina levels.¹⁶⁷ Brishen Rogers similarly explains how Uber’s use of GPS navigation technology for drivers has allowed the company to reproduce the “specialized knowledge of how to navigate a crowded city [that] historically gave [taxi drivers] some labor market power,” and repackage it as employer property.¹⁶⁸ This development puts downward pressure on wages, given that “almost anyone with a vehicle [can] do the job.”¹⁶⁹ At the same time, the breakdown of mid-level jobs through automation means fewer opportunities for career advancement as well as accelerated inequality.¹⁷⁰

2. Increased Precarity

While employers have long sought ways to reap the benefits of labor without the costs of maintaining a traditional workforce, new and advancing data gathering technologies facilitate employers’ ability to do so. When hiring traditional employees, employers must comply with legal protections and requirements such as paying minimum wage and overtime, funding premiums for workers’ compensation and unemployment insurance, respecting workers’ rights to organize, and avoiding unlawful discrimination.¹⁷¹ Some employers seek to avoid such obligations through hiring independent contractors or subcontracting out work. These practices, often referred to as “fissuring” the

¹⁶⁵ *Id.* at 59.

¹⁶⁶ *Id.* at 78.

¹⁶⁷ *See* LEVY, *supra* note 128, at 59.

¹⁶⁸ ROGERS, *supra* note 1, at 78-79; Brishen Rogers, *The Law and Political Economy of Workplace Technological Change*, 55 HARV. C.R.-C.L. L. REV. 531, 562 (2020).

¹⁶⁹ ROGERS, *supra* note 1, at 79.

¹⁷⁰ ESTLUND, *supra* note 163, at 36, 39 (noting “[a]utomation is destroying many of the decent mid-level jobs . . . that provided stepping stones to higher-skill jobs” and “as automation displaces workers from many mid-level jobs, it is very likely to exacerbate inequality”).

¹⁷¹ ROGERS, *supra* note 1, at 108-09 (“When a company hires workers as employees, it must pay minimum wages and overtime, must respect those workers’ rights to unionize, must ensure its managers do not engage in illicit discrimination, must pay premiums for unemployment insurance and workers’ compensation”); *see also* COHEN, *supra* note 110, at 31 (“Arrangements in the era of precarity [resulting from informationalized economy] externalize the costs of work—the Starbucks barista’s mobile phone bills, the Uber driver’s fuel and auto insurance payments, and so on—and internalize the benefits.”).

employment relationship, create “legal gaps” separating employers from their labor force and the legal obligations that accompany an employment relationship.¹⁷²

Data once again play a crucial role in this fissuring of the workplace. Companies commonly utilize fractured forms of employment in the growing platform and gig economy, though they are also widespread in the retail, hospitality, and fast food industries through franchising.¹⁷³ They increasingly distance themselves from their labor forces, while at the same time “surveil[ing] and manag[ing] those workers as closely as traditional employees.”¹⁷⁴ The widespread collection of data from workers allows firms to “break production into discrete tasks, farm some of them out to suppliers, and . . . monitor those suppliers’ performance.”¹⁷⁵ The result is heightened economic insecurity and precarity for workers that undermines their economic and associational power.

Data-driven technologies may also increase precarity for workers who are acknowledged employees. Scheduling algorithms can intensify irregularity and unpredictability in work schedules.¹⁷⁶ In the retail context, employers may utilize algorithms to assign workers’ shifts to match consumer traffic in stores.¹⁷⁷ Data-driven staffing algorithms can create modified working schedules with little notice based on updated predictions, leading to uncertainty and instability for workers.¹⁷⁸ Unpredictable working schedules negatively impact the social and economic well-being of workers by increasing precarity in income and causing difficulties arranging or managing childcare responsibilities.¹⁷⁹ As a result, workers experience heightened levels of stress and tension in their

¹⁷² ROGERS, *supra* note 1, at 107; Tanya Goldman & David Weil, *Who’s Responsible Here? Establishing Legal Responsibility in the Fissured Workplace*, 42 BERKELEY J. EMP. & LAB. L. 55, 64 (2021) (“[The ‘fissured workplace’ model] shifts responsibilities from lead businesses to other organizations This fissuring comes from outsourcing, contracting, subcontracting”); David Weil, *Understanding the Present and Future of Work in the Fissured Workplace Context*, 5 RSF: RUSSELL SAGE FOUND. J. SOC. SCIS. 147, 149 (2019) (“[The fissured workplace] allows major businesses to . . . not be required to treat the workers who do it as their employees with the obligations that relationship holds.”).

¹⁷³ ROGERS, *supra* note 1, at 109-10.

¹⁷⁴ *Id.* at 107.

¹⁷⁵ *Id.* at 115.

¹⁷⁶ Levy & Barocas, *supra* note 129, at 8.

¹⁷⁷ *Id.* at 7-9.

¹⁷⁸ Pauline T. Kim, *AI and Inequality*, WASH. U. ST. LOUIS: SCHOLARLY REPOSITORY, Sep. 2021, at 1, 12, 13 (explaining software’s creation of “just-in-time” scheduling creates difficulty with arranging childcare, holding additional job, or pursuing schooling).

¹⁷⁹ *Id.* at 12-13; *see also* COHEN, *supra* note 110, at 31 (stating precarious workers struggle to pay basic expenses and fulfill family care responsibilities due to inability to predict income or work schedule).

professional, personal, and family life.¹⁸⁰ Workers of color and women disproportionately endure these effects.¹⁸¹

3. Health and Safety

Where employers utilize intensive data collection and monitoring tools to supervise production, workers may feel pressured to compromise their safety, risking physical injury to achieve algorithmically determined goals.¹⁸² At Amazon, workers use electronic devices, such as barcode scanners or tablets, which gather data on their speed of completing assigned tasks, ability to satisfy mandated quotas per hour, and amount of “time off task” (“TOT”), including lunch and bathroom breaks.¹⁸³ This system encourages workers to complete tasks as fast as possible and discourages workers from taking breaks to rest or use the bathroom.¹⁸⁴ Workers have reported that they “don’t have insight into how much TOT they’ve accumulated” and that “they skip water and bathroom breaks because they fear being disciplined and terminated.”¹⁸⁵ As performance expectations have ratcheted up, so have rates of injury. Indeed, Amazon’s injury rates are higher than the industry average.¹⁸⁶

In response, the Occupational Safety and Health Administration (“OSHA”) has issued multiple citations to Amazon for its excessive injury rates and ergonomic hazards at seven different facilities.¹⁸⁷ The agency charged that “employees were required to reach, twist, and bend while repeatedly lifting packages . . . at a high frequency, placing them at risk for lower back

¹⁸⁰ Levy & Barocas, *supra* note 129, at 8-9 (linking greater worker stress, increased work-family strain, and disruption of nonwork activities to unpredictable work schedules).

¹⁸¹ *Id.* at 9.

¹⁸² Ajunwa et al., *supra* note 1, at 744 (“The demand to meet electronically monitored goals means that workers take risks and push themselves physically in ways that result in more injuries.”); Bernhardt et al., *supra* note 2, at 9 (describing how work intensification has direct effects on workers’ physical health and safety, including high injury rates).

¹⁸³ ALESSANDRO DELFANTI, LILIAN RADOVAC & TAYLOR WALKER, UNI GLOB. UNION, THE AMAZON PANOPTICON 6 (June 2021), https://uniglobalunion.org/news_media/uploads/2021/07/amazon_panopticon_en_final.pdf [<https://perma.cc/V9TQ-JA9T>].

¹⁸⁴ *Id.*

¹⁸⁵ Lauren Kaori Gurley, *Internal Documents Show Amazon’s Dystopian System for Tracking Workers Every Minute of Their Shifts*, VICE (June 2, 2022, at 09:56 ET), <https://www.vice.com/en/article/5dgn73/internal-documents-show-amazons-dystopian-system-for-tracking-workers-every-minute-of-their-shifts> [<https://perma.cc/JUU7-VJFJ>].

¹⁸⁶ DELFANTI ET AL., *supra* note 183, at 6.

¹⁸⁷ Press Release, U.S. Dep’t of Lab., U.S. Department of Labor Cites Amazon for Again Exposing Workers to Ergonomic Hazards, This Time at Colorado Springs Delivery Station (Feb. 23, 2023), <https://web.archive.org/web/20230223210038/https://www.osha.gov/news/newsreleases/national/02232023-0> [<https://perma.cc/ECD8-Y6QQ>] (marking third OSHA action against Amazon in 2023).

injuries.”¹⁸⁸ Its inspections found “work processes that were designed for speed but not safety, and they resulted in serious worker injuries.”¹⁸⁹

Firms may also gamify their performance metrics by instituting systems where workers can earn points or other rewards through their completion of assigned tasks. In this way, gamification “blurs the line between ‘work’ and ‘leisure’” as employers incorporate games into routine or tedious tasks at work, in efforts to incentivize and increase worker productivity.¹⁹⁰ Despite its touted potential for increasing worker engagement and “liven[ing] up repetitive forms of work,” gamification in the workplace can lead to considerable risks for workers.¹⁹¹ These systems are often designed to generate competition among workers, thus “capitaliz[ing] on [workers’] relations with their coworkers . . . in order to pressure them into compliance with the goals of the company.”¹⁹² Tracking productivity in this way can create adverse health outcomes for workers, where games urge workers to skip breaks to rest or eat meals.¹⁹³

Workers’ mental health may also suffer as a result of monitoring systems. In the context of ride-sharing, research has shown that “[b]eing tracked, evaluated, and judged by each passenger seemed to have a negative psychological impact on drivers who did not have [near perfect scores].”¹⁹⁴ Drivers can become hyper aware of the ratings evaluation system, and “[t]rying to deliver good services for all service interactions could pose psychological stress to workers.”¹⁹⁵

4. Discrimination and Bias

The rise of algorithmic management tools in the workplace also heightens the risks that workers may face discrimination and bias. Where algorithms are built using inaccurate, biased, or unrepresentative datasets, they can produce biased decisions that disadvantage already marginalized groups based on race, sex, or

¹⁸⁸ Citation & Notification of Penalty, Amazon.com Services, LLC, d/b/a DCS3 Delivery Station, Inspection No. 1615182, at 6 (U.S. Dep’t Lab. Feb. 15, 2023), https://www.dol.gov/sites/dolgov/files/OPA/newsreleases/2023/02/23-359-NAT_OSHA_AmazonCitation_02132023151256.pdf.

¹⁸⁹ Press Release, U.S. Dep’t of Lab., Federal Safety Inspections at Three Amazon Warehouse Facilities Find Company Exposed Workers to Ergonomic, Struck-by Hazards (Jan. 18, 2023), <https://web.archive.org/web/20250523025645/https://www.osha.gov/news/newsreleases/national/01182023> [<https://perma.cc/G6Y2-NQ9H>].

¹⁹⁰ Miriam A. Cherry, *The Gamification of Work*, 40 HOFSTRA L. REV. 851, 852-53 (2012).

¹⁹¹ *Id.* at 854; *see also* LEVY, *supra* note 128, at 70.

¹⁹² LEVY, *supra* note 128, at 53.

¹⁹³ Nicole Lewis, *Be Careful: Gamification at Work Can Go Very Wrong*, SOC’Y HUM. RES. MGMT. (Feb. 28, 2019), <https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/gamification-at-work-can-go-very-wrong.aspx>.

¹⁹⁴ Min Kyung Lee, Daniel Kusbit, Evan Metsky & Laura Dabbish, *Working with Machines: The Impact of Algorithmic and Data-Driven Management on Human Workers*, in CHI 2015: PROCS. OF THE 33RD ANN. ACM CONF. ON HUM. FACTORS IN COMPUTING SYS. 1603, 1608 (2015).

¹⁹⁵ *Id.* at 1610.

other protected characteristics.¹⁹⁶ The use of data-driven technologies to make personnel decisions can lead to discriminatory outcomes even when protected characteristics are not included in the model.¹⁹⁷ Neutral variables may be highly correlated with demographic characteristics, creating proxies and producing disparate outcomes that systematically exclude disadvantaged groups.¹⁹⁸ Furthermore, intentional discrimination is possible when data analytic tools are used to infer protected characteristics, predicting, for example, when an employee or applicant has a disability or is pregnant.¹⁹⁹ Employer use of algorithms in hiring or other personnel decisions can thus result in sorting and ranking workers in ways that disadvantage individuals based on protected characteristics and exacerbate inequality.²⁰⁰

5. Collective Speech and Activity

Collective speech among fellow workers is crucial to preserving workers' rights to self-organization and association. This speech is protected by law when it relates to workplace conditions.²⁰¹ However, workplace surveillance systems may suppress workers' efforts to organize or engage in protected concerted activity.²⁰² Employers may attempt to use data-driven technologies to attain an unfair advantage in their efforts to oppose union organizing.²⁰³ Such systems could be used to identify—or even predict—supporters of organizing efforts who might then be subject to unlawful retaliation.²⁰⁴ In the hiring process, an increasing number of firms administer personality assessment testing of potential candidates, which could be used to illegally sort out workers likely to lead unionization efforts.²⁰⁵ Those who are hired may find themselves subject to monitoring systems designed or used to quell collective action at work.

¹⁹⁶ Kim, *Data-Driven Discrimination*, *supra* note 10, at 861.

¹⁹⁷ See Pauline T. Kim, *Race-Aware Algorithms: Fairness, Nondiscrimination and Affirmative Action*, 110 CALIF. L. REV. 1539, 1549-50 (2022) (explaining algorithms can rely on proxies and produce biased outcomes even when features like race are not included in model complications presented by de-biasing algorithms, as discrimination is regardless shaped by “pre-existing biases”).

¹⁹⁸ *Id.* (“It is not always intuitively obvious which features can act as a proxy and some of those variables may be relevant to the predicted outcome even though they correlate with race.”).

¹⁹⁹ Kim, *Data-Driven Discrimination*, *supra* note 10, at 862 (describing how data miners can infer information such as whether someone is pregnant).

²⁰⁰ *Id.* at 866.

²⁰¹ National Labor Relations Act of 1935, 29 U.S.C. § 157.

²⁰² See, e.g., Charlotte Garden, *Labor Organizing in the Age of Surveillance*, 63 ST. LOUIS U. L.J. 55, 63 (2018).

²⁰³ *Id.*

²⁰⁴ See *id.*

²⁰⁵ Newman, *supra* note 2, at 706-10 (stating pre-employment assessments are marketed to companies as ways to avoid hiring employees who will agitate for more pay or benefits with other employees).

Employer use of surveillance systems to monitor workers' union-organizing activities has significantly increased in recent years.²⁰⁶ For example, Whole Foods reportedly used workforce analytics to create a heat map designed to monitor worker unionization efforts and predict stores most "at risk" of unionization.²⁰⁷ At Google, employees reported the installation of a browser extension that monitored and reported workers who created any internal calendar event inviting more than one hundred participants, "partially to weed out employee organizing."²⁰⁸ Employer use of data analytics means that companies can monitor and predict such activity at an individual level, with vendors offering to construct profiles for employees likely to be "most at risk for attrition, which can be overlaid onto current data to identify those who most closely match the profile."²⁰⁹

6. Chilling Speech

In addition to concerted protected activity to address working conditions, worker speech also plays an important role in ensuring that firms comply with important regulatory requirements. Such speech is legally protected by laws that prohibit retaliation against workers for asserting rights or reporting conditions that violate protective labor legislation.²¹⁰ Employees also play a crucial role in exposing corporate wrongdoing, a function recognized by many whistleblower

²⁰⁶ *In Solidarity: Removing Barriers to Union Organizing: Hearing Before the H. Comm. on Educ. and Lab.*, 117th Cong. 11-13 (2022) (statement of Dr. Kate Bronfenbrenner, Dir. & Senior Lecturer, Corn. Univ. Sch. of Indus. & Lab. Rels.) (stating employer opposition to organizing has grown in intensity as companies gained access to new surveillance tools).

²⁰⁷ Hayley Peterson, *Amazon-Owned Whole Foods Is Quietly Tracking Its Employees with a Heat Map Tool That Ranks Which Stores Are Most at Risk of Unionizing*, BUS. INSIDER (Apr. 20, 2020, at 10:52 ET), <https://www.businessinsider.com/whole-foods-tracks-unionization-risk-with-heat-map-2020-1> (explaining store's individual risk score is calculated based on more than two dozen metrics, including employee turnover, racial diversity, and proximity to union office).

²⁰⁸ Jo Constantz, *"The New Pinkertons": Anti-Union Consultants and Surveillance Tech Thwart Organizing*, CUNY ACAD. WORKS, Fall 2021, at 5 (citation omitted) (stating alleged intent of browser extension installation was to spy on internal employee activity).

²⁰⁹ Bradley Wilson, *Influence the Future with Predictive Analytics in HR*, PERCEPTYX (May 8, 2019), <https://blog.perceptyx.com/predictive-analytics-hr> [<https://perma.cc/9XDA-DHHX>] ("Organizational, personal, and experimental data can be used to create a risk index and predict the number of employees who will leave with 80-85% confidence."). Firms construct comprehensive profiles to predict which workers are most likely to leave their jobs, allowing employers to strategically target those workers for pay increases, while diminishing wages for those more likely to stay or unable to easily exit. Newman, *supra* note 2, at 717-19.

²¹⁰ See, e.g., Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e-3(a) (anti-retaliation provisions); Fair Labor Standards Act of 1938, 29 U.S.C. § 215(a)(3) (same); Occupational Safety and Health Act of 1970, 29 U.S.C. § 660(c) (same).

laws.²¹¹ The risk, however, is that workplace surveillance and data collection will deter workers from coming forward with information about violations.²¹²

Privacy law scholars have long argued that awareness of surveillance alters the behavior and activity of those surveilled, creating a chilling effect.²¹³ More specifically, workplace monitoring systems can undermine workers' willingness to speak freely with one another about workplace conditions or engage in other socially valued speech, like whistleblowing.²¹⁴ Although there are legal protections from retaliation, workers cannot access those remedies until after they have experienced an adverse action. Actually receiving a remedy is highly uncertain and, if it occurs at all, will likely take years. Extensive monitoring and recording of workers' activities thus add another impediment to reporting known or suspected wrongdoing, even though the law recognizes and seeks to encourage this kind of speech. In a monitored workplace, "employees will reasonably fear that the surveillance has been implemented in order to facilitate later retaliation"²¹⁵

Systematic data collection and algorithmic management tools are profoundly reshaping the relationship between workers and firms. While it is inevitable that technological developments will shift the nature of work, what is worrisome is that many of these data-driven innovations are being deployed in ways that threaten harms far beyond traditional concerns about seclusion, dignity, and autonomy. Rather, these new technologies allow firms to collect ever-greater amounts of worker data and to leverage it in new ways that can degrade basic working conditions, undermine worker bargaining power, and worsen economic inequality.

²¹¹ See, e.g., Sarbanes-Oxley Act of 2002, 18 U.S.C. § 1514A (providing protection to whistleblower employees to effectuate their ability "to provide information, cause information to be provided, or otherwise assist in an investigation"); Affordable Care Act, 29 U.S.C. § 218c (protecting employees from being discharged for providing information relating to violations of Act); Consumer Financial Protection Act of 2010, 12 U.S.C. § 5567(a) (same).

²¹² Pauline T. Kim, *Electronic Privacy and Employee Speech*, 87 CHI.-KENT L. REV. 901, 904 (2012) (arguing lack of privacy protection discourages socially valued forms of speech by workers).

²¹³ *Id.* at 926-27 (noting arguments of privacy theorists that surveillance chills speech and exploration of ideas). See generally RICHARDS, *supra* note 118 (arguing corporate surveillance threatens core democratic values like privacy); Cohen, *Examined Lives*, *supra* note 117, at 1373 (asserting privacy is necessary for autonomy, and autonomy requires "degree of freedom from monitoring, scrutiny, and categorization by others").

²¹⁴ See Kim, *supra* note 212, at 929.

²¹⁵ Garden, *supra* note 203, at 63.

IV. THE LIMITS OF WORK LAW

Many of the harms identified in Section II.B are the subject of existing workplace regulations, which are intended to protect workers from the most extreme forms of exploitation and to ensure a minimum level of working standards. However, today's novel tech tools are undermining many of these basic labor and employment law protections.²¹⁶ Recognizing these trends, some labor law scholars have doubled down on traditional labor and employment protections, arguing for strengthening existing laws.²¹⁷ Others have gestured in the direction of data privacy laws, suggesting that including workers in those laws might provide needed protections.²¹⁸

In Part V, we examine the emerging consumer data protection model and argue that it offers only limited leverage for protecting workers' interests. But first, in this Part we describe existing workplace regulations and explain why they are inadequate to protect workers' fundamental rights in an era of algorithmic management. Conventional labor and employment laws were largely developed in the industrial era, based on certain assumptions about how workplaces are organized and managed. These assumptions no longer hold given firms' ability to engage in massive data collection and sophisticated computer analyses.

To start, traditional labor regulation assumes that the minimum standards necessary for decent work can be assured by regulating formal employment relationships.²¹⁹ Data-driven technologies have undermined that assumption by enabling fissuring of the workplace.²²⁰ Firms can now rely on labor that is

²¹⁶ Ajunwa et al., *supra* note 1, at 747-62; Newman, *supra* note 2, at 725-31; Kim, *Data-Driven Discrimination*, *supra* note 10, at 897-901; Kim, *Data Mining*, *supra* note 73, at 406.

²¹⁷ See, e.g., Bales & Stone, *supra* note 1, at 59-62; Hirsch, *supra* note 1, at 933-35; Newman, *supra* note 2, at 16.

²¹⁸ Several have argued that workers should be given data rights similar to those provided in the GDPR, without analyzing in detail how those rights might apply or their potential impact in the workplace context. See, e.g., Hirsch, *supra* note 1, at 935-37; Kim & Bodie, *supra* note 21, at 309-15; Adams-Prassl, *supra* note 130, at 140-41 ("[The] GDPR provide[s] a number of mechanisms that might be able to counterbalance some of the concerns raised in connection with the increasing spread of algorithmic management. This is not to say that it can solve all the inherent contradictions."); Bernhardt et al., *supra* note 2, at 15-16. But see Ajunwa et al., *supra* note 1, at 773-74 (dismissing possibility omnibus privacy laws could protect workers).

²¹⁹ See, e.g., Fair Labor Standards Act of 1938, 29 U.S.C. §§ 201-219; Title VII of the Civil Rights Act of 1964, 42 U.S.C. §§ 2000e-2000e17; National Labor Relations Act of 1935, 29 U.S.C. §§ 151-166.

²²⁰ See Goldman & Weil, *supra* note 172, at 58-60 (explaining "fissuring" phenomenon, "where employers increasingly outsource various functions to contractors and subcontractors while maintaining substantial control over most of the outcomes of that work"); Rogers, *supra* note 168, at 569-73; Jill Habig, Veena Dubal & Mishal Khan, *Unrigging the Gig Economy*, STAN. SOC. INNOVATION REV. (Sep. 27, 2023), https://ssir.org/articles/entry/unrigging_the_gig_economy [<https://perma.cc/7J6N-LFPW>] ("Gig companies like Uber . . . are having their cake and eating it too: fully controlling workers' pay and conditions while evading the cost

outsourced, contingent, or “self-employed,” thereby disclaiming an employer-employee relationship, while advanced data processing tools allow them to indirectly maintain control and still capture the value created by labor.²²¹ As a result, some of the most vulnerable workers today, such as ride hail app drivers and food delivery workers, are placed outside of the firm. They provide labor crucial to the core business operations of large companies but are held at arm’s length. The immense amount of data collected from and about workers makes these arrangements possible; however, there are few legal levers available to challenge those data practices. Instead, advocacy efforts, which have been largely unsuccessful in the United States, have focused on reclassifying these workers as employees so that they can access traditional employment law protections.²²²

Other work law protections similarly miss the data-driven source of many current workplace harms. For example, the Fair Labor Standards Act (“FLSA”) sets a minimum hourly wage and requires overtime premiums with the goal of ensuring “the minimum standard of living necessary for health, efficiency, and general well-being of workers.”²²³ The primary concerns at the time the law was passed in 1938 were low hourly wages and oppressively long hours of work.²²⁴ Congress did not anticipate the algorithmic management tools that now make irregular and unstable work schedules a significant threat to maintaining minimum standards of living. Not surprisingly, then, the FLSA does not require a minimum quantity of work or protect against unpredictable work schedules.

Similarly, the Occupational Safety and Health Act (the “OSH Act”) is intended to ensure safe and healthful workplaces but is rooted in an industrial model that focuses on “recognized hazards” that cause death or serious bodily injury.²²⁵ OSHA’s regulatory efforts have centered on identifying specific substances or physical conditions that can cause physical harm and establishing

of doing business, like paying for unemployment insurance and workers’ comp”); V.B. Dubal, *Winning the Battle, Losing the War?: Assessing the Impact of Misclassification Litigation on Workers in the Gig Economy*, 2017 WIS. L. REV. 739, 742 (“[O]n-demand workers join existing service workers not considered employees and [are] thus ineligible for basic safeguards like minimum wage, overtime, [and] workers’ compensation”).

²²¹ See Dubal, *supra* note 129, at 1933-34 (explaining how algorithmic wage discrimination, enabled by cloud computing and machine learning technologies, allows firms to exert control over nominally independent drivers); see also Janine Berg, *Protecting Workers in the Digital Age: Technology, Outsourcing, and the Growing Precariousness of Work*, 41 COMPAR. LAB. L. & POL’Y J. 69, 73, 82-83 (2019).

²²² See Dubal, *supra* note 220, at 743; *Cotter v. Lyft, Inc.*, 60 F. Supp. 3d 1067, 1070 (N.D. Cal. 2015); *O’Connor v. Uber Techs., Inc.*, 82 F. Supp. 3d 1133, 1135 (N.D. Cal. 2015).

²²³ 29 U.S.C. § 202(a).

²²⁴ See 29 U.S.C. §§ 206-207 (implementing minimum wage and maximum hour provisions to address detrimental labor conditions).

²²⁵ U.S. DEP’T OF LAB., OSHA AT-A-GLANCE (2014), <https://www.osha.gov/sites/default/files/publications/3439at-a-glance.pdf> [<https://perma.cc/7LP5-89C2>] (explaining general duty clause of OSH Act “requires employers to keep their workplaces free of serious recognized hazards”).

standards to regulate them.²²⁶ This standard-setting process proved to be notoriously slow, and rapidly evolving workplace conditions quickly outstripped the agency's capacity to regulate specific hazards.²²⁷ To the extent that it exercises its enforcement powers, the agency has largely relied on the general duty clause, which requires employers to maintain places of employment free from recognized hazards.²²⁸ OSHA recently did so when citing several Amazon warehouses for excessive injury rates.²²⁹ Although these injuries trace back to Amazon's aggressive use of worker data to ratchet up productivity standards, the citations focus on engineering controls and improved worker training, without directly addressing data collection and use.²³⁰

Title VII and other civil rights laws have long prohibited discrimination in employment, and they clearly apply when employers rely on automated decision systems. Nevertheless, there are gaps in coverage, and scholars have questioned whether they are well-suited to the challenges posed by algorithmic tools.²³¹ For example, Title VII prohibits discrimination in hiring by three types of actors—employers, unions, and employment agencies²³²—because at the time of enactment, those were the entities that controlled access to jobs. Today, however, other intermediaries, such as online advertising platforms and job matching services, also play critical roles as gatekeepers to employment opportunities, and yet it is unclear whether they are covered by anti-

²²⁶ *Id.*

²²⁷ OSHA has enacted few substantive regulations in recent years, and its years-long effort to create ergonomic standards for the workplace ended in failure after Congress voted to rescind the regulation under the Congressional Review Act. *See, e.g.,* John Howard, *OSHA Standards-Setting: Past Glory, Present Reality and Future Hope*, 14 EMP. RTS. & EMP. POL'Y J. 237, 238-42 (2010). The agency's inspection capabilities are miniscule compared to the number of American workplaces, as the agency has historically been underfunded and understaffed. *Id.* And the fact that there is no private right of action means workers must rely on agency personnel to enforce their workplace safety rights. *Id.*; *Employees' Rights Under OSHA*, WOLTERS KLUWER (Feb. 3, 2022), <https://www.wolterskluwer.com/en/expert-insights/employees-rights-under-osha> [<https://perma.cc/X43W-KEES>].

²²⁸ Occupational Safety and Health Act of 1970, 29 U.S.C. § 654.

²²⁹ News Release, OSHA, U.S. Department of Labor Finds Amazon Exposed Workers to Unsafe Conditions, Ergonomic Hazards at Three More Warehouses in Colorado, Idaho, New York (Feb. 1, 2023), <https://web.archive.org/web/20260113101817/https://www.osha.gov/news/newsreleases/national/02012023> [<https://perma.cc/EXT4-7V4B>].

²³⁰ *See* Letter from David G. Kearns, Area Dir., OSHA, to Amazon.com Services LLC (Jan. 31, 2023), https://www.dol.gov/sites/dolgov/files/OPA/newsreleases/2023/02/23-359-NAT_OSHA_AmazonCitation_02132023151256.pdf.

²³¹ *See* Ajunwa, *supra* note 125, at 1690-92; Matthew U. Scherer, Allan G. King & Marko J. Mrkonich, *Applying Old Rules to New Tools: Employment Discrimination Law in the Age of Algorithms*, 71 S.C. L. REV. 449, 477-78 (2019); Kim, *Data-Driven Discrimination*, *supra* note 10, at 933. *But see* Keith E. Sonderling, Bradford J. Kelley & Lance Casimir, *The Promise and the Peril: Artificial Intelligence and Employment Discrimination*, 77 U. MIA. L. REV. 1, 21-28 (2022); Michael Selmi, *Algorithms, Discrimination and the Law*, 82 OHIO ST. L.J. 611, 618, 634-51 (2021).

²³² 42 U.S.C. § 2000e-2(a)-(c).

discrimination law.²³³ Even apart from doctrinal fit, practical obstacles make it difficult to enforce anti-discrimination laws in the absence of data rights. Workers who may have been disadvantaged by a discriminatory algorithm are unlikely to have access to information about the model or the underlying data that is necessary to challenge it or even to detect its discriminatory effects.

Workers' rights to organize and engage in concerted activity are clearly protected under Section 7 of the National Labor Relations Act ("NLRA"),²³⁴ and established precedents hold that pervasive monitoring and surveillance is unlawful when it chills the exercise of those rights.²³⁵ Recognizing the potential impact of new data-driven technologies, Jennifer Abruzzo, General Counsel of the NLRB under President Biden, issued a memorandum in 2022 urging enforcement actions against employers whose algorithmic management practices interfere with protected concerted activity.²³⁶ The memo also asserted that when workers are represented by a union, employers must "provide information about, and bargain over, the implementation of tracking technologies and their use of the data they accumulate."²³⁷ General Counsel Abruzzo signaled her intention to leverage existing law to the fullest extent possible to address algorithmic threats to collective worker activity. Those efforts came to halt when President Trump fired her upon taking office.²³⁸ However, even if NLRA protections were fully leveraged, any challenges would have to be tied specifically to the exercise of Section 7 rights, and the duty to bargain only applies where the workplace is unionized. Given low unionization rates and lack of knowledge about the law, even robust enforcement of Section 7 rights would be unlikely alone to significantly regulate or constrain firms' data practices.

Across multiple substantive laws, work law protections are typically retrospective in orientation.²³⁹ Workplace regulation in the United States

²³³ See Kim, *supra* note 140, at 869-74.

²³⁴ 29 U.S.C. § 157.

²³⁵ See, e.g., Nat'l Captioning Inst., 368 NLRB No. 105 (Oct. 29, 2019) (holding institute violated National Labor Relations Act ("NLRA") by "[e]ngaging in surveillance of employees' Union and other protected activities in emails, chat room logs and other electronic communications"); Brasfield & Gorrie, LLC, 366 NLRB No. 82 (May 8, 2018) (finding project manager's taking of photos and video of picketers blocking employees from entering jobsite was not unlawful surveillance); F.W. Woolworth Co., 310 NLRB 1197, 1197-98 (Apr. 27, 1993).

²³⁶ Memorandum from Jennifer A. Abruzzo, Gen. Couns., NLRB, to All Reg'l Dirs., Offs.-in-Charge & Resident Offs., NLRB 6 (Oct. 31, 2022).

²³⁷ *Id.* at 5.

²³⁸ Andrea Hsu, *Trump Fires EEOC and Labor Board Officials, Setting Up Legal Fight*, NPR (Jan. 28, 2025, at 18:07 ET), <https://www.npr.org/2025/01/28/nx-s1-5277103/nlr-trump-wilcox-abruzzo-democrats-labor> [<https://perma.cc/ZK79-9QTG>].

²³⁹ The central exception to the individual, retrospective liability model is the NLRA, which relies not on government regulatory action, but rather was intended to empower workers to form unions and through collective bargaining set appropriate workplace standards. While union voice can influence wages and working conditions, the current reality

typically focuses on past conduct, imposing liability when it causes covered harms to individual workers. Thus, workers who have not received minimum wage or overtime premiums in violation of the FLSA can sue for back wages.²⁴⁰ Workers who suffer workplace injuries can recover compensation for medical expenses and lost earning capacity.²⁴¹ Workers who have been discriminated against can sue for backpay and damages.²⁴² And so on. Retrospective liability, however, is inadequate to protect workers from algorithmic harms. Litigation focuses narrowly on questions of causation in individual cases rather than examining the broader systems that shift power to employers and undermine workers' rights. Data practices in particular are likely to be sticky. Once established, widespread data collection becomes normalized, making it more difficult to challenge or displace.

To address algorithmic harms, then, labor law needs to be updated, but not just by amending or adjusting individual substantive laws. Laws regulating the workplace focus on specific harms, but firms' data practices operate comprehensively, affecting how work is structured and power is distributed across the workplace. A common set of data collection practices can affect multiple substantive rights. Thus, in an era of big data and algorithmic management, setting minimum standards for labor is not enough, because this approach fails to address a central cause of workers' relative disempowerment: the largely unrestrained collection and exploitation of their data by firms.

V. THE LIMITS OF DATA PROTECTION MODELS

If current labor and employment laws are inadequate to protect workers' rights in a data-driven workplace, what about data protection laws? Including workers in data protection legislation would give them rights they currently lack, providing an important complement to minimum labor standards. However, the regulatory model represented by the current wave of data protection statutes is inadequate to protect workers' interests. On a conceptual level, the consumer model of data protection is a poor fit, obscuring important characteristics of the work relationship that shape workers' interests in their data. On a more practical level, the rights currently provided in the consumer privacy laws are weak and generally ill-suited to address data harms in the workplace. We explore each of these challenges in turn.

is that unions only represent a fraction of the workforce in the United States. *See* 29 U.S.C. § 158; Zachary Schaller, *Decomposing the Decline of Unions: Revisiting Sectoral and Regional Shifts*, 76 INDUS. & LAB. RELS. REV. 387, 387 (2023) (“[O]nly approximately 6% of workers in the nation’s private sector now belong to a labor union . . .”).

²⁴⁰ 29 U.S.C. § 216.

²⁴¹ 1 LEX K. LARSON, LARSON’S WORKERS’ COMPENSATION LAW § 1.01 (Matthew Bender rev. ed. 2025).

²⁴² 42 U.S.C. § 2000e-5(g)(1); Age Discrimination in Employment Act of 1967, 29 U.S.C. § 626(b); Americans with Disabilities Act of 1990, 42 U.S.C. § 12117(a).

A. *Conceptual Limits of the Consumer Model*

As described in Part I, the current data protection framework largely evolved with the consumer in mind, which likely accounts for the widespread exclusion of workers. To push for greater protection, workers could argue that collection and processing of their personal data threaten the same harms that motivate consumer privacy laws. Like consumers, workers are subject to extensive surveillance and data gathering by firms, much of it opaque and obtained without any real consent on the part of the data subject. Firms then use the extensive data collected to build individual profiles and influence the behavior of the consumer or worker to extract surplus value. Making an analogy to consumers would be a way of arguing for greater data protection for workers; however, this strategy has significant drawbacks. There are fundamental differences in the two types of relationships, making the consumer-worker analogy an uneasy fit. More to the point, relying on the consumer model overlooks workers' unique vulnerability to exploitation of their data and risks adopting a model that is not only inapt but inadequate in the workplace context.

Consumer law is animated by an image of consumers as "autonomous individuals engaged in arms-length solitary transactions with firms."²⁴³ Its focus is transactional, centering on representations and promises made in the market for goods and services. Consumers are assumed to know their own best interests, but they sometimes need legal protection to redress fraud or deception, or to overcome a lack of information that hinders pursuit of their best interests and distorts the operation of the market.²⁴⁴ Because the central concern is disadvantage in market transactions, the harms are conceptualized primarily in financial terms. Some legal scholars have strongly criticized this conception;²⁴⁵ however, the law largely reflects a transactional approach. This framing can exert a gravitational pull, shaping how legal protections are defined. As a result, leaning heavily on the consumer model to define workers' data rights risks obscuring other important characteristics of the work relationship.

Workers are situated differently from consumers in several critical ways that matter in thinking about their data rights. First, as Jonathan Harris describes it,

²⁴³ Jonathan F. Harris, *Consumer Law as Work Law*, 112 CALIF. L. REV. 1, 43 (2024).

²⁴⁴ See, e.g., Amelia Fletcher et al., *Consumer Protection for Online Markets and Large Digital Platforms*, 40 YALE J. ON REGUL. 875, 881-84 (2023); Victor E. Schwartz & Cary Silverman, *Common-Sense Construction of Consumer Protection Acts*, 54 U. KAN. L. REV. 1, 9 (2005); Luke Herrine, *What Is Consumer Protection For?*, 34 LOY. CONSUMER L. REV. 1, 18 (2022); Dee Pridgen, *The Dynamic Duo of Consumer Protection: State and Private Enforcement of Unfair and Deceptive Trade Practices Laws*, 81 ANTITRUST L.J. 911, 917 (2017).

²⁴⁵ Critics have argued the goals of consumer law ought to be more capacious and have pointed to ways in which it can or should provide more substantive protections. See, e.g., Luke Herrine, *At the Nexus of Antitrust & Consumer Protection*, 2023 UTAH L. REV. 849, 851-53; Rory Van Loo, *Broadening Consumer Law: Competition, Protection, and Distribution*, 95 NOTRE DAME L. REV. 211, 218 (2019).

employment is more “relational.”²⁴⁶ Because labor is an integral part of producing goods and services, workers often have enduring relationships with firms. The human capital they develop may be firm-specific, making it difficult to move easily to another firm. Work relationships are often much thicker than consumer transactions, involving coordination of effort and collaboration that extends beyond a simple exchange.

The implications of these thicker relational ties cut both ways. On the one hand, the fact that workers are an integral part of firms’ production processes means that firms have legitimate interests in accessing and controlling some forms of worker-related data. Even though linked to individual workers, data generated in the creation of goods or services are integral for the firm to conduct its business. Workers can also directly affect firms’ interests in ways that consumers cannot. For example, they can take actions that legally bind the firm or subject it to liability. As argued below, workers’ countervailing interests should limit firms’ *carte blanche* in their data practices. However, firms also have legitimate interests in their workers’ activities, justifying certain forms of data collection and use.

On the other hand, the relational nature of employment renders workers more vulnerable to abusive data practices than consumers. For most people, work is not a simple, one-off economic exchange, but rather a substantial and ongoing personal investment in order to secure the basic necessities of life. In that sense, work is foundational and prior to exercising one’s rights as a consumer. In the United States, employment also provides access to critical benefits, such as health insurance and retirement income. Employees are thus in a position of heightened dependence upon the firm—so much so that the law has at times identified economic dependence as the touchstone for determining whether an employment relationship exists.²⁴⁷ That economic dependence, in turn, renders workers more vulnerable to firms’ efforts to collect and exploit their data. And the harms to workers from firms’ data practices are potentially more pervasive, extending beyond a financially disadvantageous transaction.

Of course, some work relationships are becoming more short-term and transactional as technological tools have allowed the fissuring of work.²⁴⁸ Work

²⁴⁶ Harris, *supra* note 243, at 43.

²⁴⁷ See *Usery v. Pilgrim Equip. Co.*, 527 F.2d 1308, 1310 (5th Cir. 1976) (finding lower court failed to put sufficient emphasis on “the all-pervasive determinant economic dependence” factor); *Scantland v. Jeffery Knight, Inc.*, 721 F.3d 1308, 1312 (11th Cir. 2013) (stating focus of economic reality inquiry used to determine employment status is economic dependence); *Hanson v. Trop, Inc.*, 167 F. Supp. 3d 1324, 1328 (N.D. Ga. 2016) (asserting employment status determination must be viewed through lens of economic dependence).

²⁴⁸ See Goldman & Weil, *supra* note 172, at 66; Mark Anner, Matthew Fischer-Daly & Michael Maffie, *Fissured Employment and Network Bargaining: Emerging Employment Relations Dynamics in a Contingent World of Work*, 74 INDUS. & LAB. RELS. REV.: J. WORK & POL’Y 689, 699 (2021); Richard Blum, *Worker Collective Action in the Time of Fissuring: Independent Contractor Labor Boycotts, the Thirteenth Amendment, and Antitrust Law*, 19 NEV. L.J. 365, 372-77 (2018).

arrangements in the gig economy look more like consumer relationships, when they focus on discrete tasks, resembling isolated, arms-lengths transactions. While these work arrangements may lack the thicker relational ties of the standard employment relationship, their very contingency imposes a different form of vulnerability on workers. Precisely because of the vast amounts of data that can be collected about their activities, workers can be subjected to strict control and potential manipulation without the firm needing to create a more enduring relationship.

Workers differ from consumers in a second fundamental way. Unlike the imagined autonomous consumer, workers are embedded in a relationship that is explicitly hierarchical. Employment law has its roots in the common law of masters and servants, and that sense of hierarchy and subordination continues to permeate the law today.²⁴⁹ Implicit in many legal doctrines is the assumption that workers must subordinate their interests to those of their employers. For example, under the common law, employees owe a “duty of loyalty” not to act contrary to the interests of their employers.²⁵⁰ When on the job, workers are subject to employer control and discipline. There is no pretense that they have rights to self-expression or self-actualization at work. Rather, the expectation is that they will conform to any work requirements imposed by the employer, limited only by the minimum substantive guarantees provided in various labor laws.

Companies that rely on gig workers point to their ostensible lack of control over those workers in order to disclaim the existence of an employment relationship.²⁵¹ This strategy rests on the proposition that employment inherently entails a high level of control over workers. No analogous assumption attaches to the consumer relationship. Far from being subordinate, the “consumer is king.” Consumer law purports to protect the autonomy of the consumer, however short it falls of that goal. Workplace laws, by contrast, do not aim to protect workers’ autonomy, but assume employers’ right to direct and discipline labor. This power in turn facilitates firms’ ability to extract data from their workers, and to leverage such data to further tighten control, thereby enhancing their power over workers.

Workers are also situated differently from consumers regarding their long-term position in the firm. Companies have an interest in extracting surplus from consumers, but to remain viable in the long term, they need to maintain those

²⁴⁹ Matthew T. Bodie, *Employment as Fiduciary Relationship*, 105 GEO. L.J. 819, 820 (2017) (explaining under settled doctrine, employees owe fiduciary duties of loyalty to their employers).

²⁵⁰ STEVEN J. GOLDSMITH & LOUIS SHUMAN, 9 LABOR AND EMPLOYMENT LAW § 232.04 (2025) (LEXIS).

²⁵¹ See, e.g., Dubal, *supra* note 220, at 741-42 (describing spread of business model where platforms like Uber treat workers as independent contractors rather than employees); Orly Lobel, *The Gig Economy & the Future of Employment and Labor Law*, 51 U.S.F. L. REV. 51, 58 (2017) (highlighting Uber’s characterization of its drivers as “partners” free from company control).

relationships. Thus, their data practices will be geared not solely toward extracting surplus, but also toward strengthening consumers' ties to the firm. By contrast, many firms would be happy to reduce their workforces in order to cut labor costs. Put simply, firms can benefit from having fewer (or no) workers, but they can never do without consumers. As a result, firms' incentives around how to use data will differ in the two contexts, and reputational concerns are likely to have less force in restraining exploitative data practices when it comes to workers.

In other contexts, scholars have argued that firms' practices are blurring the lines between workers and consumers.²⁵² For example, Marion Crain describes internal marketing efforts whereby firms encourage employees to "buy into the brand" in order to induce greater loyalty and extra-role effort, even though the employers do not incur any greater reciprocal obligations.²⁵³ Jonathan Harris has explored how firms treat workers like consumers when they offer services and credit products incidental to the work relationship.²⁵⁴ And others have pointed out that firms' efforts to restrict labor mobility represent anti-competitive conduct that harms workers in ways similar to collusive or monopolistic behavior in consumer markets.²⁵⁵ The goal of these scholars has been to leverage sources of protection outside of work law, such as implied contract, consumer, and antitrust laws, in order to bolster worker protections.

These strategies may hold promise in areas where work law falls short; however, they also carry risks. Considering exploitative credit products offered by employers, Harris identified two potential problems with relying on a "workers as consumers" framework. First, conceptualizing workers as consumers rather than producers feeds into a narrative of "individualism, autonomy, freedom of contract, and self-betterment" that detracts from class-identity formation.²⁵⁶ Second, Harris noted that the "workers as consumers" framework is limited because the protections offered to consumers against unfair financial products is quite weak.²⁵⁷

Similar concerns caution against relying too heavily on a consumer model for establishing workers' data rights. As explained in Part VI below, workers have strong *collective* interests in how their data is used. The consumer model of data protection obscures the interdependence of workers' interests. The second

²⁵² See, e.g., Harris, *supra* note 243, at 44 (describing how firms offer credit products to workers as part of labor contract, blurring line between workers and consumers); Marion Crain, *Managing Identity: Buying into the Brand at Work*, 95 IOWA L. REV. 1179, 1183-84 (2010) (explaining internal marketing campaigns that treat employees as if they are consumers).

²⁵³ Crain, *supra* note 252, at 1183-84.

²⁵⁴ Harris, *supra* note 243, at 3 (arguing workers who receive services and credit products from firm are entitled to protections of consumer law).

²⁵⁵ See, e.g., Hiba Hafiz & Ioana Marinescu, *Labor Market Regulation and Worker Power*, 90 U. CHI. L. REV. 469 (2023).

²⁵⁶ Harris, *supra* note 243, at 41-42.

²⁵⁷ *Id.* at 44.

concern identified by Harris also obtains because the recently enacted consumer privacy laws are arguably quite anemic. They rely heavily on procedural rights, such as those articulated in the original FIPs, and provide few legally enforceable standards to limit data collection and use. As discussed in the next Part, this model of consumer data privacy offers few meaningful legal protections for workers' interests in their data.

B. *Practical Limits of Data Protection*

As seen in Part I, all but one of the recent data protection bills in the United States excludes workers. Putting aside the question of conceptual fit, this Part explores what it would mean practically if workers *were* covered by these statutes, and the extent to which doing so would protect their interests. There are significant variations among the nineteen state data protection laws now on the books, but they follow a similar overall structure. Each provides consumers with a set of individual rights, and each imposes some obligations on entities that process personal data. These rights and obligations would offer some new protections for workers but fall far short of adequately protecting them against the kinds of harms discussed above.

Some scholars have criticized the reliance on individual rights to protect consumer privacy as ineffectual,²⁵⁸ and those concerns are particularly true in the workplace. Among the rights most commonly provided in the state statutes are rights to access and correct one's personal information. These rights were part of the original FIPs and have long been included in data protection regulations. The Fair Credit Reporting Act, passed in 1970, gave people the right to receive a copy of their consumer reports and to request correction of any errors.²⁵⁹ By accessing their consumer reports, individuals might discover erroneous information—say, a bankruptcy or eviction that never happened—that harmed their reputation and unfairly deprived them of opportunities. With the right to seek correction of errors, their reputations could be restored and opportunities expanded.

Rights of access and correction are less useful in an era of big data. For one thing, the amount of data that can be captured digitally is so voluminous, and the information it captures so granular, that individual data points may not have much meaning upon casual inspection. Consider, for example, an online assessment administered to applicants that collects information about their response times when performing certain tasks. From a simple review of the data,

²⁵⁸ Many scholars have criticized reliance on individual rights to protecting consumer privacy as ineffectual. *See, e.g.*, Ari Ezra Waldman, *Privacy's Rights Trap*, 117 NW. U. L. REV. ONLINE 88, 88 (2022); Julie E. Cohen, *How (Not) to Write a Privacy Law*, KNIGHT FIRST AMEND. INST. COLUM. U., Mar. 23, 2021, at 4; Solove, *supra* note 103, at 1881-83. Others have pushed back, arguing that these rights are necessary, even if not sufficient by themselves. *See, e.g.*, Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529, 1533 (2019); Kaminski, *supra* note 103, at 390, 395.

²⁵⁹ 15 U.S.C. §§ 1681, 1681b(b), 1681i.

it may be difficult to know if any measurements are erroneous. Moreover, the *meaning* of each piece of data, or the inferences drawn from it, often will not be apparent simply by viewing it in isolation. The value for the firm comes when it is aggregated across many other data points, and with the data of many other workers. Even if individuals could detect and correct errors in their own data, such changes are unlikely to affect outcomes when aggregated data is used to establish system-wide conditions—such as setting performance standards or identifying organizing hot spots.

Other individual rights created by the recent data protection laws are also difficult to operationalize in the workplace context.²⁶⁰ For example, a robust right of deletion would run up against employers' legitimate interests in retaining many types of data about workers. In the consumer context, firms generally have no ongoing need for an individual's data after a transaction has been completed. By contrast, employers may be required legally or practically to maintain information about workers relating to the firm's operations or its employment practices, even after the employment relationship has ended.²⁶¹ Imagine, for example, a firm that investigates allegations that an employee engaged in sexual harassment. Giving the employee a robust right of deletion in such a situation would prevent the employer from maintaining complete personnel records, as well as potentially undermine enforcement of anti-harassment law. Data linked to individual workers will also often be enmeshed in information about a firm's business activities, such that a blanket right of deletion would be unworkably broad.²⁶² Because employers have legitimate interests in retaining many types of worker data, a different sort of balancing is required than for consumer data.

As explained in Part I, most of the state data protection statutes appear intended to grant workers the right to opt-out of automated decision systems, even as they exclude them from all other protections. If an opt-out right is available, its usefulness depends upon the type of decision at stake. Such a right is most critical for workers when they are subject to decisions with serious consequences—such as termination—that rest on information with a high risk of error, misinterpretation, or bias. For example, automated discharge of drivers after a fixed number of customer complaints creates a significant risk of arbitrary or discriminatory terminations, given the inconsistency and known biases in

²⁶⁰ Rights of data portability are also common, intended to enable consumers to easily switch to competing digital services. *See, e.g.*, Utah Consumer Privacy Act, UTAH CODE ANN. § 13-61-201 (West 2025). It is difficult to give this right meaning in the context of work relationships.

²⁶¹ For an example, see 29 C.F.R. § 1602.14 (2024), regarding employers' record-keeping requirements under anti-discrimination laws. Employers may also be required to preserve information when there are allegations of wrongdoing or violations of the law.

²⁶² For example, some types of employee information will be impossible to separate from records regarding a firm's operations, such as payroll records or information about an employee's work product.

customer reviews.²⁶³ Having a right to opt-out of automated terminations could be highly valuable to workers in such contexts.

The right to opt-out, however, is less useful in the absence of other individual data rights. If a worker opts out, presumably the decision will be made by a human supervisor who will likely rely on the same information. Unless the worker is informed about the basis for the decision and has an opportunity to review and, if necessary, challenge the data on which the decision is made, the right to opt-out of automated decisions may be a hollow one.

An individual right to opt-out of automated decisions is also less useful when the harms to workers are systemic. For example, if worker data is used to ratchet up performance metrics, or to target organizing hot spots, an individual's decision to opt out is unlikely to affect how algorithmic management tools operate systemically. Individual rights are also inadequate to address systemic discrimination. If a hiring system has discriminatory effects by disproportionately screening out members of disadvantaged groups, individual decisions to opt out will not make the system operate in a less biased way. To the contrary, significant numbers of opt-outs could make it more difficult to detect discriminatory patterns. Furthermore, if some subpopulations opt out at significantly higher rates, the tested population may become less representative, further contributing to biased outcomes.

Recent data protection statutes also impose a number of obligations on entities that process personal data. These obligations might offer some protection if they applied to worker data. For example, all of the statutes mandate transparency in some form, requiring data controllers and processors to provide consumers with information about the categories of personal data they collect and their purposes in processing that data.²⁶⁴ Privacy law scholars have long criticized the inadequacy of privacy notices, complaining that they are long, difficult to understand, and therefore rarely actually read.²⁶⁵ Nevertheless, for workers, receiving notice about what personal data is collected and how it is used in algorithmic management tools would provide an important first step. Of course, a good deal depends on how this information is provided, but as discussed below, unions or other worker representatives could play a role in analyzing this

²⁶³ See Keith Cunningham-Parmeter, *Discrimination by Algorithm: Employer Accountability for Biased Customer Reviews*, 70 UCLA L. REV. 92 (2023); see also Seb Murray, *Ratings Systems Amplify Racial Bias on Gig-Economy Platforms*, YALE INSIGHTS (Aug. 14, 2023), <https://insights.som.yale.edu/insights/ratings-systems-amplify-racial-bias-on-gig-economy-platforms> [<https://perma.cc/2TLT-JYXN>].

²⁶⁴ See, e.g., Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-578(C) (2025).

²⁶⁵ See, e.g., RICHARDS, *supra* note 75, at 54, 94 (remarking such “‘notice’ . . . is little more than vague terms hidden in the bewildering fine print of privacy policies”); Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74, 76-80, 102-06 (2018) (describing privacy policies as “confusing, inconspicuous, and inscrutable” forms of notice designed so no one reads them); Elvy, *supra* note 111, at 442-45; Calo, *supra* note 106, at 1030.

information and making its salience for workers' rights clear. While notice alone will never be sufficient, workers cannot even begin to challenge unfair data practices without basic knowledge about what they are.

A number of the state statutes also obligate entities to specify the purposes for which they are collecting data, and to minimize collection and processing to what is necessary for the stated purpose.²⁶⁶ In theory, these obligations of purpose specification and data minimization could be helpful in mitigating workplace harms if applied to worker data. As a practical matter, however, the obligations imposed by recent data protection laws are largely ineffectual because they do not articulate any clear standards for determining what legitimate purposes are, nor how to determine what is "necessary" for a given purpose.²⁶⁷ In addition, most lack any clear enforcement mechanisms for entities that violate these obligations.²⁶⁸

The current data protection laws are limited in another way, because they protect only "personal data"—which is linked or linkable to an identified person—and not "de-identified data"—which cannot reasonably be linked to an identified person.²⁶⁹ As many scholars have noted, the line between personally identifiable and anonymized data is vanishingly thin, especially given advances in computing techniques that permit re-identification.²⁷⁰ Not only is re-identification of data often possible, but many of the potential harms to workers

²⁶⁶ See, e.g., CAL. CIV. CODE § 1798.100(c) (2018); Maryland Online Data Privacy Act of 2024, H.B. 567, § 14-4607(B)(1) (2024); VA. CODE ANN. § 59.1-578(A) (2025).

²⁶⁷ Cf. Ari Ezra Waldman, *Civil Society and the Crisis of Privacy Law*, 74 EMORY L.J. 1079, 1092 (2025) (arguing data minimization provision of ADPPA offered little protection because it was "a vague commitment with no way to enforce it"). Many of the state laws requiring data minimization are similarly vague or even less detailed than the ADPPA's data minimization provisions. See *supra* note 266.

²⁶⁸ See, e.g., Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-584 (2025); COLO. REV. STAT. § 6-1-1311 (2025).

²⁶⁹ See, e.g., California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100-140(m), (v) (West 2025); Colorado Privacy Act, COLO. REV. STAT. §§ 6-1-1303(11), (17), -1306 (2025); Virginia Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575, -577 (2025); Utah Consumer Privacy Act, UTAH CODE ANN. §§ 13-61-101(14), (24), -201 (West 2025).

²⁷⁰ See, e.g., Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1742-43 (2010) (explaining anonymization cannot guarantee privacy); Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703, 710-11 (2016) (discussing how deidentified data sets do not protect identity given risk of reidentification); Frederik Zuiderveen Borgesius, Jonathan Gray & Mireille van Eechoud, *Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework*, 30 BERKELEY TECH. L.J. 2073, 2116-20 (2016) (detailing instance of pseudonymized data being linked to users, even without advanced re-identification techniques); Stacey A. Tovino, *Not So Private*, 71 DUKE L.J. 985, 999-1005 (2022) (highlighting examples of anonymous health data being reidentified to expose data subjects). But see, e.g., Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1, 5 (2011) (arguing "concerns over anonymized data have all the characteristics of a moral panic and are out of proportion to the actual threat posed by data dissemination").

from data processing do not even require personally identifiable information. Aggregated, anonymized data can be used, for example, to predict organizing “hot spots” and suppress workers’ collective activity. Similarly, algorithms that optimize labor cost savings when building staffing schedules, or that set plant-wide performance standards, do not require personally identifiable data, even though they can significantly worsen conditions experienced by individual workers.²⁷¹

Thus, even if recently enacted statutes were expanded to include workers, they would have only a minimal impact mitigating the types of harms outlined in Section III.B. The individual rights and new obligations might benefit workers in marginal cases. As a whole, however, these statutes would do little or nothing to limit firms’ extensive data gathering practices, or to constrain them from leveraging that data in ways that undermine workers’ interests. Thus, while inclusion in current data protection laws could be helpful on the margins, these rights alone are unlikely to meaningfully improve basic work conditions.

VI. WORKERS’ COLLECTIVE INTERESTS IN DATA

Algorithmic management tools can undermine basic workers’ rights in a number of ways, yet existing regulatory models that focus on minimum labor standards or data protection are insufficient to protect those rights. What is missing is recognition of workers’ *collective* interests in determining how their data is used to manage the workplace. In this Part, we argue that the law should explicitly recognize those interests and provide robust channels for workers to exercise their rights on a collective basis.

A number of scholars have criticized the individual rights model of data protection for failing to recognize the relational nature of data.²⁷² Data does not just affect the individual from whom it is collected; rather, as Viljoen and others point out, that data can reveal information about another, potentially affecting the second person’s rights.²⁷³ It is this relational quality of data—its ability to provide insights about related populations or groups, not just the individual from whom it was collected, that makes data valuable to commercial entities.²⁷⁴ Thus, it is a mistake to think that individual data rights can mediate the relationship between an isolated data subject and a data collector.²⁷⁵

²⁷¹ Another example is when an employer uses workforce-wide data to anticipate future benefits costs—say, the predicted number of pregnancies in the workforce—and adjusts its benefits coverage or leave policies in order to minimize those anticipated costs.

²⁷² See generally Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573 (2021).

²⁷³ *Id.* at 605 & n.89.

²⁷⁴ Individual data is of marginal utility, but when aggregated with data about many others, it can be mined for patterns and inferences, allowing an entity to make predictions about people other than the individual from whom the data was collected. See *id.* at 611-12.

²⁷⁵ See *id.* at 578.

The observation that data is relational certainly holds true for workers' data. However, this view overlooks another important dimension of data for workers—namely, that they have *collective* interests in firms' data practices. The relational view foregrounds how person A's data can result in harms to person B. In contrast, a collective perspective emphasizes that workers' data interests are not only related, they are entwined—they rise and fall together. Workers do not just have similar interests as individuals; they have joint interests *as a group* in how their data is used. Data practices that harm one worker inherently affect all. In this way, their interests cannot be separated; workers share the *same* interest collectively.

The collective nature of workplace data is illustrated by the inadequacy of individual data rights. As discussed in Section VI.B, even if workers had rights of access and correction, such rights would offer little protection. Exercising those rights on an individual basis is difficult, and receiving data about a single person provides little insight into how the system as whole works.²⁷⁶ Moreover, individually correcting or deleting a data record is unlikely to affect the overall operation of algorithmic management systems, because the impact of any single piece of data is usually quite marginal.

In this sense, data practices in the workplace are, like many workplace conditions, “local public goods.”²⁷⁷ A public good is a benefit that, once provided, inherently benefits everyone in the community; no one can be excluded even if they object or refuse to contribute.²⁷⁸ National defense is commonly provided as an example at the state level.²⁷⁹ Many conditions of work have the characteristics of local public goods because they either affect all workers alike or none at all. For example, if an employer provides air conditioning, everyone who works in that space benefits; it cannot be provided to just a subset of workers. Algorithmic management practices are local public goods because decisions about data collection and use will be implemented across the workforce. Tools such as scheduling software or productivity monitoring would not be useful to firms if they could only be applied to some, but not all, of the relevant workforce. Because these tools are intended to operate systemwide, decisions about their deployment will benefit or harm all workers alike.

²⁷⁶ See generally Kim, *Data Mining*, *supra* note 73 (explaining data mining allows companies to make inferences about personal characteristics that go beyond information actually collected); see also generally Viljoen, *supra* note 272 (describing how digital economy derives value not so much from individual-level information but from population-level insights).

²⁷⁷ See Pauline T. Kim, *Collective and Individual Approaches to Protecting Employee Privacy: The Experience with Workplace Drug Testing*, 66 LA. L. REV. 1009, 1027 (2006) (characterizing employees' interest in privacy as type of “local public good”).

²⁷⁸ See generally Julian Reiss, *Public Goods*, STAN. ENCYCLOPEDIA PHIL., Fall 2021, at 1, <https://plato.stanford.edu/archives/fall2021/entries/public-goods> [[https:// perma.cc/5SMY-MB38](https://perma.cc/5SMY-MB38)] (defining public goods and providing examples).

²⁷⁹ *Id.*

Individual bargaining over local public goods is likely to lead to failure. Individuals have insufficient incentives to bargain for improvements; although a change will benefit everyone, the individual bears the full cost of bargaining. Even if the total benefit for all workers would exceed the cost to the employer of providing the good, the good will not be provided if bargaining occurs only on an individual basis. For these reasons, individual workers have little incentive to resist collection and processing of their data. If they refuse to consent, they risk retaliation, yet they would gain little in the way of benefit if they succeed. Even if their information was excluded, data collected from other workers would be sufficient to fuel algorithmic management tools. Only when workers can negotiate collectively, taking into account the interests of the group as a whole, is the provision of local public goods likely to occur.

What would protecting workers' collective interests in their data look like practically? Foremost, it would require data rights that could be asserted on a collective basis, by a union or other worker representative. Section 7 of the NLRA already protects workers' rights to exercise voice collectively to address workplace issues.²⁸⁰ Because firms' data practices increasingly shape working conditions, worker representatives should also have the right to request collective data where necessary to enforce existing labor rights. For example, where automated systems are used to impose discipline or set wages, worker representatives should have access to the data necessary to determine whether rights are being violated.

Recognizing workers' collective interest would also mean that the individual rights created by data protection laws should be granted to workers collectively, rather than individually. Access to aggregated data could offer workers real insights into questions like how employers set performance standards or whether they are determining compensation fairly. Unions or other worker representatives could provide technical expertise and infrastructure, educating workers about how firms' data collection affects their working conditions, and helping them access and interpret complex, aggregated worker data.

In addition, this information could empower worker representatives to enforce firms' obligations under data protection laws, prompting firms to clearly articulate the reasons for collecting personal data (purpose specification) and ensuring that they only collect and use data necessary for those purposes (data minimization). For example, if an employer chose to deploy a surveillance system, it would have to identify its reason for doing so and limit how it used the collected data. If the stated reason was to maintain security, worker representatives could challenge the use of that system to collect biometric data about workers, impose discipline, or monitor organizing activity.

In addition to data rights, many recently proposed governance regimes call for stakeholder involvement in the design and development of algorithms or AI

²⁸⁰ See *supra* note 234 and accompanying text.

systems.²⁸¹ Often these proposals are quite vague as to how the relevant stakeholders should be identified and what their participation should look like.²⁸² Creating meaningful avenues for participation is challenging when algorithms are used in contexts such as criminal law enforcement, where their effects are broadly felt across a diffuse public.²⁸³ The workplace, however, is a setting in which these challenges are more tractable. Workers' status as stakeholders is obvious because the way data is deployed directly determines the conditions under which they work. And affected workers are usually easily identified because the employing firm must collect basic information about their identity and contact information in order to employ them. Moreover, in some workplaces, existing labor organizations provide vehicles for exercising collective worker voice.

Regulatory frameworks that focus on procedural requirements risk becoming box-checking exercises in the absence of substantive standards. However, the speed of technological evolution and the vast array of possible use cases make it difficult to rely on legislatures to enact specific standards. Given the inevitable regulatory gaps, worker groups are in the best position to identify and assess risks of data technologies in the workplace, and to help determine when and how potential harms should be mitigated or eliminated altogether.

Requiring worker bargaining or consultation around data practices in the workplace need not block technological innovation. Rather, it would help direct that innovation in ways that benefit workers and firms alike. Some forms of technology are productivity-enhancing because they complement human skills to make workers more productive. New tools can also improve workers' lives by mitigating hazards or performing the most dangerous tasks. However, other applications of technology operate primarily to the benefit of firms by allowing them to capture more of the surplus value without improving productivity. Many monitoring and surveillance tools fall into this category.²⁸⁴ As Brishen Rogers argues, mandated bargaining around data uses would "incentivize employers to adopt productivity-enhancing rather than power-augmenting technologies."²⁸⁵ Collective data rights would give workers leverage to redirect innovation from uses that merely redistribute power toward applications that create greater shared benefits.

Unions have already focused attention on data rights in recent labor actions. One of the central issues in the recent strike by actors in Hollywood was control

²⁸¹ See Margot E. Kaminski & Gianclaudio Malgieri, *Impacted Stakeholder Participation in AI and Data Governance*, 27 YALE J.L. & TECH. 247, 251-70 (2025) (describing shift toward promoting stakeholder participation in data protection and AI regulation).

²⁸² *Id.* at 294-99.

²⁸³ See Ngozi Okidegbe, *To Democratize Algorithms*, 69 UCLA L. REV. 1688, 1712 (2023).

²⁸⁴ ACEMOGLU & JOHNSON, *supra* note 24, at 16-20; ROGERS, *supra* note 1, at 25-27; see also Erik Brynjolfsson, *The Turing Trap: The Promise and Peril of Human-Like Artificial Intelligence*, 151 DAEDALUS 272, 273-74 (2022).

²⁸⁵ ROGERS, *supra* note 1, at 143.

over the use of data capturing their appearance and bodies, which could be used to generate AI images or video content.²⁸⁶ The Writers Guild of America was similarly concerned about how data generated by its members in the form of past writings might be used to train models to replace their labor.²⁸⁷ Both strikes were only resolved by providing the workers a greater measure of control over their data and the use of AI tools in work processes.²⁸⁸ Other unions have sought to bargain over monitoring tools that collect data used to set performance standards or impose discipline.²⁸⁹ Labor advocates have been pressing state legislatures to enact protections against abusive use of digital technologies. Worker organizations have also developed policy statements and principles regarding the use of digital technologies in the workplace, emphasizing core themes of ensuring accountability, improving jobs, centering workers, and advancing the public good.²⁹⁰

As these developments illustrate, worker organizations already recognize the significance of data in shaping working conditions, as well as the need to address data use from a collective perspective. However, most workplaces lack formal labor representation, posing challenges. Relying on collective rights is complicated in the United States, given low union density, NLRA preemption, and the prohibition on employer-sponsored worker organizations.²⁹¹ Giving workers a meaningful voice will require innovating methods for worker participation and making legal changes. What exactly that might look like is beyond the scope of this Article; nevertheless, it is useful to note that many possible models exist. In Germany, for example, companies are required to consult with workers before implementing significant technological changes, and studies suggest that workplace automation has taken a different path there—benefiting both workers and firms—rather than shifting wealth and power to

²⁸⁶ Winter, *supra* note 18.

²⁸⁷ Arkin, *supra* note 159.

²⁸⁸ Jake Coyle, *In Hollywood Writers' Battle Against AI, Humans Win (For Now)*, AP NEWS (Sep. 27, 2023, at 17:35 ET), <https://apnews.com/article/hollywood-ai-strike-wga-artificial-intelligence-39ab72582c3a15f77510c9c30a45ffc8> [<https://perma.cc/6CZ5-9UBR>]; Andrew Dalton, *The Hollywood Writers Strike Is Over After Guild Leaders Approve Contract with Studios*, AP NEWS (Sep. 26, 2023, at 23:54 ET), <https://apnews.com/article/writers-strike-deal-hollywood-vote-actors-d3119d670a4fd3449773bf8f4026fb2b> [<https://perma.cc/H2JQ-DLHW>]; see also *Summary of the 2023 WGA MBA*, WRITERS GUILD AM. CONT. 2023, <https://www.wgacontract2023.org/the-campaign/summary-of-the-2023-wga-mba> [<https://perma.cc/SF9R-NCWU>] (last visited May 1, 2026).

²⁸⁹ ROGERS, *supra* note 1; Lisa Kresge, *Negotiating Workers' Rights at the Frontier of Digital Workplace Technologies in 2023*, UNIV. OF CAL. BERKELEY LAB. CTR. (Dec. 18, 2023), <https://laborcenter.berkeley.edu/negotiating-workers-rights-at-the-frontier-of-digital-workplace-technologies-in-2023> [<https://perma.cc/6W84-552W>].

²⁹⁰ See generally KHAN & FENG, *supra* note 19.

²⁹¹ See Cynthia L. Estlund, *The Ossification of American Labor Law*, 102 COLUM. L. REV. 1527, 1529-30 (2002).

firms and worsening working conditions.²⁹² A report by the Labor and Worklife Program at Harvard Law School sets forth a number of recommendations for reforming labor law that would allow workers to build collective power and increase worker voice and representation.²⁹³ And recently, some states have begun experimenting with workers' councils that have the authority to review working conditions within a particular industry, such as fast food. These types of innovations might provide effective models for worker consultation on data practices, without depending upon the lengthy and complex process of union organizing.

CONCLUSION

Despite their near total exclusion from recent data protection laws, workers have strong interests in their personal data—interests as compelling, if not more so, than that of consumers. Firms increasingly rely on algorithmic management tools that extract and analyze worker data and then leverage it to shape the production process. These tools can threaten basic workers' rights, undermining long-established guarantees of minimum working standards and fair treatment. Consumer-focused data protection regimes might offer some benefits on the margins, but they are far from adequate to address potential harms to workers from firms' data practices. And even if existing labor standards were updated to address data-driven workplaces, it would be difficult for minimum standards legislation to keep up with constantly evolving technology.

Recognizing workers' collective interests is crucial to protecting against exploitative data practices. Collective data rights could more effectively safeguard workers' substantive rights than a framework relying on individual rights alone. Rather than setting uniform requirements for all workplaces, empowering collective worker voice allows more flexibility in considering the varying needs of different industries and workplaces. Importantly, the harms to workers from technological advances are not inevitable. Firms can use tools to increase control and extract more surplus from workers, or they can choose to adopt digital technologies that enhance human capabilities, increase productivity and spread the gains more broadly. Strengthening worker voice will help prioritize the latter, so that technology produces widely distributed benefits, rather than further concentrating power and undermining working conditions.

²⁹² Anna Waldman-Brown, *Automation Isn't the Biggest Threat to US Factory Jobs*, WIRED (May 1, 2022, at 07:00 ET), <https://www.wired.com/story/robots-automation-jobs-manufacturing-labor-germany-us> [<https://perma.cc/XL8W-KTJ5>].

²⁹³ See generally SHARON BLOCK & BENJAMIN SACHS, CLEAN SLATE FOR WORKER POWER: BUILDING A JUST ECONOMY AND DEMOCRACY (2020), <https://clje.law.harvard.edu/app/uploads/2020/01/Clean-Slate-for-Worker-Power.pdf> [<https://perma.cc/A55A-MS9D>] (proposing reforms around fostering inclusion, transforming representation rights, fortifying organizing rights, reimagining collective action rights, expanding bargaining rights, reforming corporate law, reforming rules of democratic participation, and allowing state and local labor law experimentation).