

June 29, 2023

Office of Science and Technology Policy
The White House
1600 Pennsylvania Ave NW
Washington, DC 20500

RE: *Comment on Request for Information on Automated Worker Surveillance
and Management*

Thank you for the opportunity to comment on the widespread harms caused by using automated tools to surveil and control workers. Absent aggressive action across several agencies of the federal government, the “future of work” risks becoming a future of algorithmic manipulation and surveillance that will strip workers of dignity, power, and voice, suppress wages, and exacerbate our nationwide workplace health and safety crisis. Marginalized communities and workers of color will suffer the most. The Consumer Financial Protection Bureau (CFPB), Equal Employment Opportunity Commission (EEOC), Federal Trade Commission (FTC), Department of Justice (DOJ), Department of Labor (DOL), National Labor Relations Board (NLRB), and the Occupational Safety and Health Administration (OSHA) should act urgently and in concert to address this evolving threat to workers.

Towards Justice is a nonprofit legal organization that uses impact litigation, policy advocacy, and collaboration with workers and workers’ organizations to build worker power and advance economic justice. These comments are informed by our ongoing engagement with workers and our litigation and advocacy on behalf of workers suffering from surveillance and algorithmic control. Examples of our advocacy in this space include litigation on behalf of rideshare drivers in California alleging that Uber and Lyft cannot on the one hand deny them labor rights while on the other hand use algorithms to manipulate and control them, including by setting the prices charged to consumers, without violating California antitrust and unfair competition laws.¹ We also represent Amazon delivery drivers alleging that Amazon—in part through the use of invasive worker surveillance tactics—denies drivers reasonable access to the

¹ *Gill et al. v. Uber Technologies, Inc. et al.* 3:22-cv-04379, Complaint, Jun. 21, 2022, chrome-extension://efaidnbmnnnibpcjpcglclefindmkaj/https://towardsjustice.org/wp-content/uploads/2022/06/Uber-Lyft-Complaint-FILED.pdf; see also Kellen Browning and Noam Scheiber, *Drivers’ Lawsuit Claims Uber and Lyft Violate Antitrust Laws*, N.Y. Times, Jun. 21, 2022, <https://www.nytimes.com/2022/06/21/business/uber-lyft-antitrust-lawsuit.html>.

bathroom and creates an illegal disparate impact on people with typically female anatomy.² We have also represented workers in a variety of cases challenging unfair competition in the labor market,³ and in cases combatting the misuse of big data to harm low-wage workers.⁴ Meanwhile, we have engaged in extensive advocacy on behalf of workers harmed by employer-driven debt, including earned wage access products that may allow employers to obtain extensive information about the financial circumstances of their workers.⁵ Because harm to workers often implicates several areas of law, we strive to provide de-siloed advocacy support to our clients and often help workers and worker organizations to use labor standards laws, competition laws, and consumer protection laws to level the playing field and build worker power.

Employers have always kept tabs on worker behavior and performance and have always sought to manipulate and control workers while evading legal responsibilities to them. But in the past two decades, employers have increasingly sought to exploit technologies that allow them to obtain even more granular and real-time information about workers and to manipulate and control workers by hidden algorithms.⁶ Modern workplace surveillance is used to track productivity; monitoring the number of packages a warehouse worker scans per minute or the number of keystrokes a desk worker completes on her computer.⁷ It is used to keep tabs on worker location, eye movement, internet browsing, and electronic communications. “Now, with the advent of almost ubiquitous network records, browser history retention, phone apps,

² *Cross et. al. v. Amazon*, 2023-cv-31495, Complaint, May 22, 2023, <https://towardsjustice.org/wp-content/uploads/2023/05/2023-05-22-12-32-23-2023.5.22-DSP-complaint-for-filing.pdf>; see also Jules Roscoe, *Drivers Sue Amazon Over 'Inhumane' Conditions, Having to Pee in Bottles*, Vice, May 24, 2023, <https://www.vice.com/en/article/z3m4wa/drivers-sue-amazon-over-inhumane-conditions-having-to-pee-in-bottles>.

³ See e.g., *Bautista et.al v. Carl Karcher Enterprises, LLC*, <https://towardsjustice.org/litigation/fighting-wage-suppression-in-the-fast-food-industry-bautista-et-al-v-carl-karcher-enterprises-llc/>; *Beltran v. InterExchange, Inc.*, <https://towardsjustice.org/litigation/fighting-wage-suppression-for-childcare-workers-on-au-pair-visas-beltran-et-al-v-interexchange-inc-et-al/>; *Llacua v. Western Range Association*, <https://towardsjustice.org/litigation/combating-wage-suppression-in-the-sheep-ranching-industry-llacua-et-al-v-western-range-association-et-al/>; *Cirilo Ucharima Alvarado v. Western Range Association*, <https://towardsjustice.org/2023/03/28/proposed-class-of-shepherders-vindicated-in-suit-against-western-range-association/?fbclid=IwAR1MX2FZqwiHSIBYFoXGqSgghYnwYzbwstQ6zfBmDLhJV-vuHQjTv696D5I>.

⁴ *Gambles v. Sterling Infosystems, Inc.*, <https://towardsjustice.org/litigation/preventing-careless-data-collection-from-limiting-job-prospects-gambles-merck-compo-v-sterling-infosystems-inc/>.

⁵ *Testimony of David H. Seligman Before the United States Senate Committee on Banking, Housing, and Urban Affairs On Employer-Driven Debt*, Sept. 13, 2022, chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/<https://www.banking.senate.gov/imo/media/doc/Seligman%20Testimony%209-13-22.pdf>.

⁶ Matthew T. Bodie, *The Law of Employee Data: Privacy, Property, Governance*, Indiana Law Journal, Vol. 97, 2021-2022, Saint Louis U. Legal Studies Research Paper No. 2021-14, <https://ssrn.com/abstract=3819897>; see also Alexandra Mateescu and Aihua Nguyen, *Algorithmic Management in the Workplace*, New York: Data & Society, 2019, https://datasociety.net/wp-content/uploads/2019/02/DS_Algorithmic_Management_Explainer.pdf.

⁷ *The Rise of Workplace Spying*, WEEK, Jul. 5, 2015, <http://theweek.com/articles/564263/rise-workplace-spying> (“a survey from the American Management Association, at least 66 percent of U.S. companies monitor their employees’ internet use, 45 percent log keystrokes, and 43 percent track employee emails”); see also, Annette Bernhardt, Reem Suleiman and Lisa Kresge, *Data and Algorithms at Work: The Case for Worker Technology Rights*, UC Berkeley Labor Center, Nov. 2021, <https://laborcenter.berkeley.edu/data-algorithms-at-work/>.

electronic sensors, wearable fitness trackers, thermal sensors, and facial recognition systems, there truly could be limitless worker surveillance.”⁸

Real-time surveillance of workers is often coupled with real-time control of workers whether through human managers or algorithms that can exploit detailed information about workers to manipulate their behavior and depress their wages.⁹ Because these forms of control—although often more invasive and coercive than control exercised by human bosses—are hidden some companies (especially in the so-called “gig economy”) have attempted to argue that they can exercise control over workers in this way without being accountable to them under the labor laws. In this way, workplace surveillance and algorithmic control are inextricably intertwined with misclassification.

These systems dramatically reduce worker autonomy, undermine fair competition, and disparately impact protected classes of workers in ways that reinforce historic marginalization. In addition, these technologies are often implemented without worker knowledge, and usually without full disclosure of what is being tracked, what the goalposts are, or what the consequences are if goals are not met. And once data about workers is collected, workers have limited ability to access that information or to protect it from inappropriate use or disclosure. This creates a general environment of fear that modifies worker behavior in concerning ways. It can encourage workers to work far beyond expected productivity goals, while chilling both collective action and enforcement of workplace rights.

These extensive harms cannot be resolved by one agency of government. In fact, worker surveillance and algorithmic control are often exploited by employers in an attempt to skate between various legal regimes. Control by hidden algorithm alongside misclassification, for example, may seek to evade the authority of the DOL or NLRB, but in doing so, implicate the authority of the CF PB, DOJ, and FTC. The primary goal of these comments is to highlight the authority of the CFPB, DOL, DOJ, EEOC, FTC, NLRB, and OSHA and emphasize the need for aggressive and coordinated action across the federal government to address these challenges. The comments include some specific recommendations, but they also raise many unanswered questions, questions that can only be resolved if the federal government is acting in concert to address these harms.

1. The Federal Trade Commission and Department of Justice

Employers’ use of workplace surveillance and the related automated management of workers implicates antitrust and competition laws and laws prohibiting unfair and deceptive acts and practices within the jurisdiction of the FTC and the DOJ.

⁸ Ifeoma Ajunwa et. al., *Limitless Worker Surveillance*, California Law Review 105, no.3, 2017, <https://mronline.org/wp-content/uploads/2017/12/3Ajunwa-Schultz-Crawford-36.pdf>.

⁹ See, e.g., Veena Dubal, *The House Always Wins: The Algorithmic Gambification of Work*, Jan. 23, 2023, <https://lpeproject.org/blog/the-house-always-wins-the-algorithmic-gambification-of-work/>; Noam Scheiber, *How Uber Uses Psychological Tricks to Push Its Drivers’ Buttons*, N.Y. Times, Apr. 2, 2017, <https://www.nytimes.com/interactive/2017/04/02/technology/uber-driverspsychological-tricks.html>.

While competition laws regulating conduct involving multiple firms may not apply directly to employers' exercise of workplace surveillance and automated management over employees *within* the firm,¹⁰ firms that classify their workers as independent contractors are subject to such regulations when they use surveillance technologies and algorithms to exercise control over workers that are purportedly *outside* the firm. The so-called gig economy provides a clear example. The use of surveillance and algorithmic control to engage in “wage discrimination”¹¹ and set prices charged to customers at optimal amounts for the companies, provides powerful evidence of the control that app-based delivery and rideshare companies exercise over their drivers—evidence relevant to the question whether the companies owe those drivers labor rights. But if those workers are properly classified as independent contractors, then their use of surveillance and automated management in these ways implicate antitrust and competition laws governing vertical price restraints and wage and price discrimination. Even if such conduct does not violate the Sherman or Clayton Acts in some circumstances, the FTC has highlighted how such conduct may be an unfair method of competition under Section 5 of the FTC Act.¹²

Gig companies often also use surveillance and algorithmic management technologies to develop pay models that can make it impossible for workers to make ends meet unless they work exclusively for a single company, thus effectively preventing workers from moving between employers.¹³ Again, these payment models are powerful evidence of misclassification, but they can also be understood as restraints on worker mobility that may violate antitrust and unfair competition laws, especially when coupled with the companies' extensive market power. Put bluntly, the gig companies cannot have it both ways. They cannot deny workers labor rights without the control they exercise over those workers being subject to laws governing vertical restraints and unfair competition.

Workplace surveillance across purportedly independent firms may implicate unfair competition and antitrust laws even when workers are properly classified as employees. This may arise where powerful firms seek to use labor market intermediaries to avoid accountability to workers while simultaneously exercising control over workers and the intermediary firms. For example, Amazon's extensive surveillance of its delivery drivers, which it claims not to employ, and who are employed directly by Amazon's Delivery Service Partners (DSPs), is powerful evidence that Amazon in fact employs those workers. But surveillance also exacerbates the

¹⁰ See, e.g., *Copperweld Corp. v. Independence Tube Corp.*, 469 U.S. 927 (1984).

¹¹ Dubal, *supra* n. 9.

¹² *Policy Statement Regarding the Scope of Unfair Methods of Competition Under Section 5 of the Federal Trade Commission Act*, Commission File No. P221202, Federal Trade Commission, Nov. 10, 2022, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ftc.gov/system/files/ftc_gov/pdf/P221202Section5PolicyStatement.pdf (Section 5 prohibits “unfair methods of competition in or affecting commerce”, which “reaches beyond the Sherman and Clayton Acts to encompass various types of unfair conduct that tend to negatively affect competitive conditions” or “violate[] the spirit of the antitrust laws”, including price discrimination.).

¹³ *Gill et al. v. Uber Technologies, Inc. et al.* 3:22-cv-04379, Complaint, ¶¶ 62-77, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://towardsjustice.org/wp-content/uploads/2022/06/Uber-Lyft-Complaint-FILED.pdf.

vertical restraints that Amazon exercises over its DSPs. It is much harder for DSPs to provide services to firms besides Amazon when Amazon’s surveillance and management technology has constant eyes on DSPs and delivery drivers—including through video cameras inside DSP vans. As a consequence, Amazon DSPs may be captive to Amazon, which can exploit its market power to set prices and wages in ways that undermine worker bargaining power.¹⁴

Together, the FTC’s unfair method of competition authority and its unfair and deceptive act and practices (UDAP) authority can be used to attack the ways in which worker surveillance and algorithmic management can deceive and manipulate workers. The Commission’s 2021 case against Amazon for misappropriating driver tips provides a blueprint. The FTC explained how Amazon “mislead its drivers and conceal[ed] its theft,” which made it “less likely that drivers would seek better opportunities elsewhere, helping Amazon attract and retain workers in its quest to dominate.”¹⁵ Unfortunately, “[u]nder its status quo approach, the FTC [did] not seek civil penalties for this type of abuse.”¹⁶ The agency should use all its authority under Section 5 of the FTC Act and all the tools at its disposal to attack the ways in which workers are harmed by worker surveillance and algorithmic management and control.

2. Occupational Safety and Health Administration (OSHA)

Living in a proverbial panopticon with the constant threat and possibility not only of surveillance, but of losing your livelihood if you fail to meet unknown standards, creates extraordinary physical and mental strain for many workers. This is particularly so as technology makes surveillance easier and cheaper for employers. Much thoughtful work has been done to document the physical and mental health impacts of workplace surveillance. We know that the need to meet efficiency goals—known and unknown to the worker—encourages workers to push themselves in ways that too often result in injury. Amazon’s injury rates, driven by minute-by-minute tracking of warehouse workers, have become particularly infamous.¹⁷

Pervasive workplace monitoring has had disturbing implications for workers’ ability to take care of basic bodily functions. In a report from *The New York Times*, “workers across a variety of jobs—pharmaceutical assistants, insurance underwriters, employees of e-commerce companies—. . . said productivity pressure had led to problems with bathroom breaks.”¹⁸ Towards Justice is now litigating a case in which Amazon delivery drivers allege that invasive

¹⁴ For more about abuses of Amazon DSPs, see: Lauren Kaori Gurley, *‘I Had Nothing to My Name’: Amazon Delivery Companies Are Being Crushed by Debt*, Mar. 7, 2022, <https://www.vice.com/en/article/wxdbnw/i-had-nothing-to-my-name-amazon-delivery-companies-are-being-crushed-by-debt>.

¹⁵ Statement of Commissioner Rohit Chopra, Federal Trade Commission, Feb. 2, 2021, https://www.ftc.gov/system/files/documents/public_statements/1587003/20200102_final_rchopra_statement_v2.pdf.

¹⁶ *Id.* at 2 n.12.

¹⁷ Will Evans, *Ruthless Quotas at Amazon Are Maiming Employees*, *The Atlantic*, Nov. 25, 2019, <https://www.theatlantic.com/technology/archive/2019/11/amazon-warehouse-reports-show-worker-injuries/602530/>; see also Daniel A. Hanley and Sally Hubbard, *Eyes Everywhere: Amazon’s Surveillance Infrastructure and Revitalizing Worker Power*, *Open Markets*, Sept. 2020, <https://www.openmarketsinstitute.org/publications/eyes-everywhere-amazons-surveillance-infrastructure-and-revitalizing-worker-power>.

¹⁸ Jodi Kantor and 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>.

monitoring by Amazon forced them to pee in bottles or defecate in bags to meet their metrics.¹⁹ Even in the at-home work context, metrics requiring workers to answer phone calls within a certain number of seconds, move their mouse with particular frequency, or meet keystroke goals can keep workers tied to their desks. At Towards Justice, we met with a worker who was so constrained by at-home monitoring that she peed herself in her own bedroom because she couldn't get up from her desk.

Such dystopian examples underscore the health impacts of workplace surveillance, as well as the extraordinary imbalance of power in the modern workplace. In workplaces where employers do not extensively surveil and manipulate workers, workers are more likely to be able to work at a healthy and safe pace and meet basic bodily functions like accessing the bathroom. But as more and more workers are governed by technologies that strip them of autonomy, we should ensure that OSHA has the resources and support to use regulation, guidance, and aggressive enforcement under the general duty provision²⁰ to protect workers.

3. The National Labor Relations Board

The decline in unionization over the last half century has undermined workers' ability to negotiate and combat invasive surveillance and monitoring. And now, constant surveillance can effectively deter or prevent unionization and other collective action.²¹ Pace of work requirements keep workers too busy to engage with one another. Knowing they are being watched chills worker behavior and makes them fear retaliation. Surveillance technology can be used to spread workers out or otherwise reduce opportunities for collective action. And technology can help employers identify workers suspected of or engaged in organizing.²² Although electronic micromanagement may inspire workers to fight back, and "[s]ome of the most closely monitored employees in the country have become some of the most restive",²³ it still "seems unimaginable that unlimited employer scrutiny of employees' collective action could be consistent with the core of the National Labor Relations Act's (NLRA's) protections."²⁴

It is crucial to safeguard workers from unlawful retaliation based on information gathered through workplace surveillance as well as employer surveillance of non-workplace activities. For example, during the COVID-19 pandemic, a Colorado-based paramedic participated in an interview for public radio that explained some of the workplace difficulties medical care

¹⁹ Matt Bloom, *Amazon Delivery Drivers in Colorado Peed in Bottles, Pooped in Bags to Keep Jobs, Lawsuit Says*, Colorado Public Radio, May 23, 2023, <https://www.cpr.org/2023/05/23/amazon-lawsuit-delivery-drivers-quotas/>.

²⁰ 29 U.S.C. § 654, 5(a) and (b).

²¹ See generally, Jo Constantz, *"They Were Spying On Us": Amazon, Walmart, Use Surveillance Technology to Bust Unions*, Newsweek, Dec. 13, 2021, <https://www.newsweek.com/they-were-spying-us-amazon-walmart-use-surveillancetechnology-bust-unions-1658603>; Charlotte Garden, *Labor Organizing in the Age of Surveillance*, St. Louis University Law Journal 55, 2018, <https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=1817&context=faculty>.

²² Sarah Kessler, *Companies Are Using Employee Survey Data to Predict — and Squash — Union Organizing*, OneZero, Jul. 30, 2020, <https://onezero.medium.com/companies-are-using-employee-survey-data-to-predict-and-squash-union-organizing-a7e28a8c2158>.

²³ Kantor and Sundaram, *supra* n. 18.

²⁴ Garden, *supra* n. 21.

professionals faced during the pandemic. The paramedic’s employer immediately reprimanded him even though he was off duty and speaking about the terms and conditions of employment that undeniably impacted his coworkers.²⁵

The National Labor Relations Board (NLRB) should use regulation and case decision-making to guide employers about how the NLRA constrains workplace surveillance. This guidance must reflect the challenges created by corporate coupling of labor market fissuring—the offloading of the costs and liabilities inherent to being an employer—with the simultaneous use of surveillance technologies designed to ensure corporate control over workers.²⁶ As General Counsel Jennifer Abruzzo explained, these changes in workplace organization require a “new framework for protecting employees from intrusive or abusive forms of electronic monitoring and automated management that interfere with Section 7 activity.”²⁷

4. The Consumer Financial Protection Board

The Consumer Financial Protection Board (CFPB) has an important role to play in protecting workers against the inappropriate use of their personal data.²⁸ We appreciate the CFPB’s scrutiny of data brokers that obtain information about consumers through workplace surveillance.²⁹ In 2019, Towards Justice represented a class of workers concerned that careless data sharing by a large background check services company was limiting their job prospects in violation of the Fair Credit Reporting Act (FCRA), and in 2021, Towards Justice represented clients alleging that use of criminal history on background checks to automatically bar drivers from a rideshare app ran afoul of New York’s Fair Chance Act. As the CFPB has articulated, the FCRA is not only relevant to the use of background checks in employment decisions, but also to combating unauthorized or inappropriate use of data gathered about workers. Both the dissemination of inaccurate information, and the misuse of accurate information, may constitute a violation.

Additionally, the increased use of consumer financial products and services within the employment relationship—an issue clearly within the CFPB’s authority—creates new forms of worker surveillance and automated management. Through our own litigation and advocacy, we

²⁵ *Complaint alleges Denver Health Prevented Employees from Speaking Out Against Racism*, 9 News, Nov. 24, 2020, <https://www.9news.com/article/news/health/coronavirus/denver-health-systemic-racism-covid-19-whistleblower-complaint/73-057d1e8a-df65-420d-a04d-096c7b41f0ff>.

²⁶ Reed Shaw, *Amazon, Surveillance, and the NLRB’s Joint Employer Rule*, OnLabor, May 30, 2023, <https://onlabor.org/amazon-surveillance-and-the-nlrbs-joint-employer-rule/>.

²⁷ Jennifer Abruzzo, *Electronic Monitoring and Algorithmic Management of Employees Interfering with the Exercise of Section 7 Rights*, Memo. GC 23-02, Oct. 31, 2022, <https://www.nlr.gov/news-outreach/news-story/nlr-general-counsel-issues-memo-on-unlawful-electronic-surveillance-and>

²⁸ 12 U.S.C. § 5511 et sec.

²⁹ See, Emma Oppenheim, *Worker Surveillance Poses Potential Privacy Harms*, CFPB, Jun. 20, 2023, <https://www.consumerfinance.gov/about-us/blog/worker-surveillance-poses-potential-privacy-harms/>.

have seen how employers operating as creditors can exploit their power to exercise even more control over workers.³⁰

Furthermore, employers may exploit financial information about workers obtained through their role as creditors providing employer-driven debt to further exploit and control those workers. As just one example, rideshare companies offer workers earned wage access products that may allow “early” access to wages. For example, Uber’s “Instant Pay” service allows drivers to immediately claim earnings from each ride, although they must pay a fee, ranging from \$2.99 to \$4.99.³¹ Uber of course knows how often a driver uses Instant Pay, which may offer insight into that worker’s financial desperation. Can Uber access that information when deciding how much to pay that worker? That is, can Uber add that information to the algorithm that determines worker pay and engages in so-called “wage discrimination”³² in order to pay more desperate workers less? Because the gig companies keep their algorithms hidden, it is not clear whether information gathered through consumer-creditor relationships may be used to control and manipulate workers, but this is a question that falls within the CFPB’s jurisdiction.

5. The Equal Employment Opportunity Commission

Our antidiscrimination laws (including Title VII of the U.S. Civil Rights Act of 1964, the Age Discrimination in Employment Act, the Equal Pay Act, and the Americans with Disabilities Act) prohibit discrimination on the basis of race, color, religion, sex, national origin, age, or disability. These laws not only protect against intentional discrimination based on protected characteristics, but also against policies or practices that have a disparate impact on protected groups. The Equal Employment Opportunity Commission should aggressively combat workplace surveillance techniques and data usage policies that harm marginalized communities.

Our anti-discrimination laws should already bar the use of workplace surveillance tools to purposefully discriminate. But further clarification could help protect workers from the use of invasive technologies to find out about individual protected characteristics, even where the purposes of worker surveillance are general or opaque. For example, can a facially neutral wellness program gather information about worker health that reveals their ethnicity – like genetic information unique to individuals of Ashkenazi Jewish descent? Or that reveals health conditions unique to members of our trans community? If so, having gathered that information, how may an employer use it?

³⁰ See e.g., Seligman Testimony, *supra* n. 5; see also, Dave Jamieson, *When This Pilot Quit Her Job, Her Employer Billed Her \$20,000*, Huffington Post, Jan. 21, 2023, https://www.huffpost.com/entry/ameriflight-pilot-training-repayment-provisions_n_63a2214ee4b04414304bc464#:~:text=When%20This%20Pilot%20Quit%20Her,soon%20came%20to%20regret%20it; Taylor Telford, *PetSmart offered free training. But it saddled employees with debt.*, Wash. Post, Aug. 4, 2022, <https://www.washingtonpost.com/business/2022/08/04/petsmart-dog-grooming-traininglabor-lawsuit/>.

³¹ Caitlin Mullen, *Branch Draws Uber, Others into Fold*, Payments Dive, Feb. 16, 2023, <https://www.paymentsdive.com/news/uber-partnership-a-boon-for-branch-payments-ewa/642898/>.

³² Dubal, *supra* n. 9.

Our anti-discrimination laws also should already bar the use of workplace surveillance that has a disparate impact on protected groups. For example, Towards Justice’s clients allege that Amazon’s monitoring and automated delivery performance metrics has a disparate impact on workers with typically female anatomy.³³ In essence, by refusing to allow adequate bathroom access, Amazon has transformed urinating in a bottle into a job requirement, thus making it much more difficult for anyone who cannot easily urinate in a bottle to do the job.

The disparate impacts of surveillance may arise in other contexts as well. Pace of work requirements may inadequately accommodate disabled workers. Incorporating consumer ratings into worker surveillance—a common practice among rideshare companies and chain restaurants – may become a vehicle for consumer bias that disparately impacts traditionally marginalized workers.³⁴ And worker surveillance combined with other problematic practices—like algorithmic wage discrimination – may cause a disparate impact, like the known gender disparity in earnings among Uber drivers.³⁵ Finally, the hiring algorithms used by many employers – although marketed to reduce intrinsic bias—may cause discriminatory outcomes.³⁶

Our anti-discrimination laws also protect workers from hostile work environments. Constant monitoring or fear of people watching you could create a hostile work environment based on gender or gender identity. Or the fact that “[l]ow-wage workers are traditionally more likely to be surveilled, and workers of color and immigrants are most likely to be working in many of the low-wage jobs with immediate and severe consequences of surveillance,”³⁷ could create a hostile work environment for these protected classes of workers.

To ensure our anti-discrimination laws can be brought to bear in these instances, we must consider the relationship between the worker and the employer, and between the surveillance technology provider and both the hiring entity and the worker. Our laws must ensure that companies that exert power over workers do not achieve free reign to discriminate against them by modifying or re-naming the employment relationship. Similarly, our laws must not exempt

³³ *Cross et. al, v. Amazon*, Complaint, 2023CV31495, May 22, 2023, <https://towardsjustice.org/wp-content/uploads/2023/05/2023-05-22-12-32-23-2023.5.22-DSP-complaint-for-filing.pdf>.

³⁴ Mateescu and Nguyen, *supra* n. 6; Rosenblat, Alex, Karen Levy, Solon Barocas, and Tim Hwang, *Discriminating Tastes: Customer Ratings as Vehicles for Bias*, Data & Society, Oct. 2016, https://datasociety.net/pubs/ia/Discriminating_Tastes_Customer_Ratings_as_Vehicles_for_Bias.pdf.

³⁵ Cody Cook et al., *The Gender Earnings Gap in the Gig Economy: Evidence from over a Million Rideshare Drivers*, The Review of Economic Studies 88, no. 5, Oct. 1, 2021: 2210–38, <https://doi.org/10.1093/restud/rdaa081>.

³⁶ Gideon Mann and Cathy O’Neil, *Hiring Algorithms Are Not Neutral*, Harvard Business Review, Dec. 9, 2016, <https://hbr.org/2016/12/hiring-algorithms-are-not-neutral>; See also, Alex Engler, *Auditing Employment Algorithms for Discrimination*, The Brookings Institution, Mar. 12, 2021, <https://www.brookings.edu/research/auditing-employment-algorithms-for-discrimination/>.

³⁷ Kathryn Zickuhr, *Workplace Surveillance is Becoming the New Normal for U.S. Workers*, Washington Center for Equitable Growth, Aug. 18, 2021, <https://equitablegrowth.org/research-paper/workplace-surveillance-is-becoming-the-new-normal-for-u-s-workers/>.

surveillance technology providers from repercussions for knowingly perpetuating systemic bias regardless of the relationship they purport to maintain with either employers or workers.³⁸

The Equal Employment Opportunity Commission should take on each of these fights, first to clarify the law and then to enforce it vigorously to prevent the perpetuation of systemic bias in the modern workplace.

6. The Department of Labor Wage and Hour Division

Workplace surveillance and control also implicates the wage and hour laws. First, it is critical that the Department of Labor address misclassification by employers that exploit workplace surveillance to control and manipulate workers, especially via hidden algorithm, while also seeking to avoid accountability to those workers under the minimum wage and overtime laws.³⁹

Workplace surveillance also raises distinct challenges for properly classified employees that may implicate wage and hour protections. For example, a time tracking software that rounds worker time to the nearest 15-minute interval, or automatically accounts for mandated breaks, could result in time shaving in violation of wage and hour protections.⁴⁰ Worker surveillance that extends beyond the temporal confines of assigned working hours also raises challenging questions: Can you be off duty while being surveilled? Or is all time when a worker is surveilled compensable work time? Meanwhile, the blending of public and private personas on social media raises new questions about compensable work. Under what circumstances does posting on a personal profile become compensable work?

Also, the DOL should consider the extent to which employers who profit off the information gathered from workers have violated anti-kickback provisions by taking a thing of value from workers that belongs to workers and exploiting it for the employer's own profits.⁴¹ The DOL Wage and Hour Division should be on the cutting edge of defining and addressing these challenges to ensure that workplace surveillance does not become a tool for cheating workers out of legally earned wages.

³⁸ Miranda Bogen and Aaron Rieke, *An Examination of Hiring Algorithms, Equity, and Bias*, Upturn, Dec. 2018, <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf>.

³⁹ See discussion of worker misclassification in Section 1, above.

⁴⁰ Elizabeth Tippet, *How Employers Profit from Digital Wage Theft Under the FLSA*, American Business Law Journal 55 (2), 2018, 315–401, <https://doi.org/10.1111/ablj.12122>; Rachel Feintzeig, *Employees Say Time-Tracking Systems Chip Away at Their Paychecks*, The Wall Street Journal, May 20, 2018, <https://www.wsj.com/articles/employees-say-time-tracking-systems-chip-away-at-their-paychecks-1526821201>; see also Elizabeth Tippet, Charlotte S. Alexander, and Zev J. Eigen, *When Timekeeping Software Undermines Compliance*, Yale Journal of Law and Technology 19 (1), 2018, <https://digitalcommons.law.yale.edu/yjolt/vol19/iss1/1/>.

⁴¹ 29 CFR § 531.35.

7. The White House Office of Science and Technology Policy

The White House Office of Science and Technology Policy is uniquely positioned to bring agency leaders together to define a proactive, de-siloed approach to the extraordinary increase in workplace surveillance and automated management. Traditionally, competition, workplace health and safety, labor relations, anti-discrimination, wage and hour, and privacy laws have been viewed as separate spheres that address separate problems and provide separate solutions. But worker surveillance blurs these lines, and we must ensure a coordinated response to this new challenge.

The White House should convene representatives of the FTC, DOJ, NLRB, CFPB, DOL (OSHA and Wage and Hour), and EEOC to develop a coordinated response to the exponential increase in worker surveillance and monitoring in the marketplace. This type of coordinated oversight is essential in an economy where the imbalance of power between workers and hiring entities is so skewed.

This response should include agency-level rulemaking to clarify how relevant legal frameworks constrain the use of worker surveillance and joint enforcement. We also recommend that the federal government require review of worker surveillance plans and affirmative disclosure of such plans to workers. Workers should know how they are being surveilled, what metrics their performance is measured against, what data is collected, who can access it, and how it is used. Workers should also have access to their own data. This effort could take a cue from the draft Worker Privacy Act developed by the Center on Privacy & Technology at Georgetown Law⁴² and New York's worker surveillance disclosure requirements⁴³.

At the end of the day, workers do not care if their problems are characterized as antitrust violations, discrimination, health and safety concerns, or some other label. What matters is that the government is there to police abuses of corporate power that make work stressful, invasive, hostile, unhealthy, and demoralizing. Our government must protect workers not only from employers, but from all the powerful entities that impose the threat of surveillance on workers in ways that undermine competition, endanger privacy, cause injury, and chill the exercise of workplace rights.

⁴² Gabrielle Rejouis, *A Solution to Extensive Workplace Surveillance*, Center on Privacy & Technology at Georgetown Law, Nov. 7, 2019, <https://medium.com/center-on-privacy-technology/a-solution-to-extensive-workplace-surveillance-8f5ab4e28b4d>.

⁴³ *New York Employers Required to Notify Employees of Electronic Monitoring*, National Law Review, May 5, 2022, <https://www.natlawreview.com/article/new-york-employers-required-to-notify-employees-electronic-monitoring>.