POLICY BRIEF

The "Privacy" Trap:

How "Privacy-Preserving AI Techniques" Mask the New Worker Surveillance and Datafication

This brief was written by:

Minsu Longiaru, PowerSwitch Action
Wilneida Negrón, PhD, Coworker.org
Brian J. Chen, Data & Society
Aiha Nguyen, Data & Society
Seema N. Patel, University of California College of the Law, San Francisco (formerly UC Hastings Law)
Dana Calacci, PhD, Pennsylvania State University College of Information Sciences and Technology

Executive Summary

How would you feel if prompts like "speak more warmly" or "smile now," generated by emotion-tracking tools, popped up on your screen at work as you spoke with a customer or client? What if, in your interactions with coworkers, your employer was using data to predict and tamp down on any signs that your conversations could lead to workplace organizing or joining a union? And what if, in all of this, your employer was using so-called "Privacy-Preserving AI Techniques" that allowed them to truthfully say they never "touched" your or anyone else's personal data — even as they managed to analyze that data in order to do these things?

Such are the dilemmas workers increasingly face in the digital age. In response to widespread concerns about data tracking and the collection of personal information, corporations are deploying a new brand of technologies, including forms of artificial intelligence (AI), that claim to be "privacy-preserving" or "privacy-friendly" because they protect individuals' personal data. **But protecting workers' personal data does not necessarily lead to protecting workers.** Because corporations can use these Privacy-Preserving AI Techniques as workarounds to analyze data at scale and make predictions without "touching" personal data, these technologies can enable corporations to technically comply with data privacy laws while exerting control over workers in ways that should cause grave concern.

Left unchecked and absent proactive intervention, these technologies will be deployed in ways that further obscure accountability, entrench inequality, and strip workers of their voice and agency. Stronger state-level enforcement of existing laws — and most fundamentally, new workplace technology rights and standards — are necessary to protect workers from an expanding web of invisible control and digital exploitation.

In light of these emerging technologies, we propose three forward-looking design principles, developed through deep discussions with workers, academics, and technologists. Rather than finely regulating specific technologies or data inputs directly, these principles target root causes, addressing the overall deficit of worker power and autonomy that tends to worsen as employers deploy new technologies. As federal preemption increasingly threatens state and local regulation of AI technology, this approach to protecting workers may also emerge as a necessary one.

Principles

1. **Eliminate the employer surveillance prerogative** by preventing abusive surveillance from happening in the first place.
2. **Focus on worker outcomes and refuse to play cat and mouse with the tech industry** by widening the lens to target not only the boss’s tech-driven means, but their harmful ends.
3. **Prioritize policies that enhance worker autonomy and check corporate power** by rebalancing power asymmetries.

These principles — paired with concrete legislative tools, enforcement reforms, and grassroots policy change efforts already underway across the US — offer a roadmap for bold governance that provides meaningful protection to workers and positions them to be decision-makers in the digital age.

Glossary

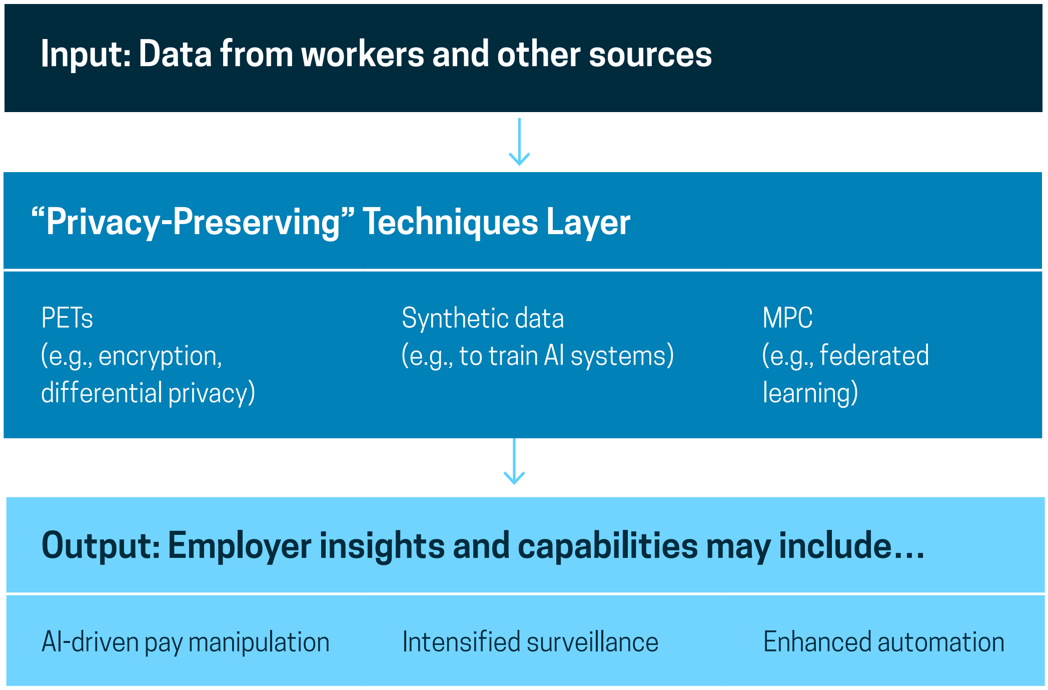
Privacy-Preserving AI Techniques: Technologies, including PETs, synthetic data, and MPC, that “protect” personal data — data that is individually identifiable or traceable to an individual — while still allowing for the collection, use, and analysis of that data.[1]

Privacy-Enhancing Technologies (PETs): Technologies, including homomorphic encryption, functional encryption, and differential privacy, that use encryption and similar techniques to allow personal data to remain “hidden” even as it is being collected, processed, and used.

Synthetic Data: A form of data built by a computing model that is used to supplement or replace “real” data, i.e., data that is based on real-world measurements.

Multi-Party Computation (MPC): Technologies that allow data from different devices or parties to be analyzed, without revealing each other’s data to one another.

How can employers use Privacy-Preserving AI Techniques to avoid “touching” personal data?



Input: Data from workers and other sources

“Privacy-Preserving” Techniques Layer

PETs (e.g., encryption, differential privacy)

Synthetic data (e.g., to train AI systems)

MPC (e.g., federated learning)

Output: Employer insights and capabilities may include…

AI-driven pay manipulation

Intensified surveillance

Enhanced automation

Introduction

Workers and advocates are racing to address the widespread use of automated management and surveillance tools in the workplace.[2] Such technologies are strongly associated with higher anxiety levels for workers, pressure to work at unsafe speeds, and higher rates of workplace injury.[3] Adding to this, corporations can use a new class of emerging Privacy-Preserving AI Techniques to further erode worker power and perpetuate new harms.

This policy brief examines three of these technologies, which are increasingly integrated into AI systems that monitor and manage work: privacy-enhancing technologies (PETs), synthetic data, and multi-party computation (MPC).

To demonstrate that these technologies are often inadequate to protect workers, we unpack two core myths about data privacy:

- The myth that data protection in the consumer marketplace functions similarly in the workplace.

- The myth that stronger data protections, particularly those focused on safeguarding personally identifying information, are sufficient to address the harms that workers suffer from data extraction.

This brief also highlights some of the most promising examples of a next generation of labor and technology protections. It provides legislators and advocates with a framework for designing policy tools to regulate emerging technologies proactively and sustainably, and advances an ambitious policy vision that focuses on worker dignity and power, not just technically narrow data privacy protections.

I. When “Privacy” Isn’t Enough: The Hidden Risks of Emerging Workplace Technologies

Until recently, most tech regulation in the United States has followed what we call a “*chase-the-data*” approach — a framework based on individual rights to access, correct, or delete personal data.[4] Key laws like the California Consumer Privacy Act (CCPA)[5] are based on this approach, mirroring elements of the European Union General Data Protection Regulation (GDPR), which is often held up as the “gold standard” of this policy model.[6] Laws like these have been groundbreaking in challenging data extraction and establishing new rights to data privacy. They offer individuals some level of control to counter corporate ownership of data.

This data protection and security model — originally aimed at regulating how tech companies like Google and Facebook collect and use data for advertising[7] — has two major characteristics. First, because it equates individual data *privacy* with *protection*, legal protections often only apply to so-called personal data that can be traced to a particular individual. Thus, data that is anonymized, de-identified, or aggregated is afforded few to no legal protections.[8] Second, because this model focuses on individual data rights, the burden of exercising those rights falls on the individual, typically through procedural rights to “know,” “delete,” and “correct” one’s own data.[9]

Such individualized approaches fall woefully short in the workplace.[10] Workers often operate under conditions of extremely unequal bargaining power, where the stakes of exercising one’s rights can be prohibitively high.[11] Even in the rare instances when employers must disclose the use of workplace technology, workers generally lack the power to perceive or control the full extent of workplace surveillance.[12] As a result, there has been an unprecedented expansion in employers’ ability to collect worker data without meaningful consent, and to use it to surveil, discipline, and intensify exploitation.[13] Employers can also profit from worker data by selling it on the open market.[14]

New advancements in AI, machine learning, and distributed computing, such as so-called **privacy-enhancing technologies, synthetic data, and multi-party computation**, offer ways for companies to comply with “chase-the-data” regulatory models and nominally claim they are protecting worker privacy. But these technologies are very unlikely to help workers — and in fact can be deployed to perpetuate or enhance worker surveillance. The following sections discuss how, without adequate safeguards, these new technologies — while superficially promising privacy — can allow employers to continue to feed worker data into machine learning models that exert ever-higher levels of control, manipulation, and extraction.

A. Obscuring the Watcher: How "Privacy-Enhancing" Technologies (PETs) Mask Employer Surveillance

> "For us drivers, a lot of it is just suspicion. They [Uber] are collecting your information and they know everything about you. They know what route you're taking, your personal information, where you are going, but when it comes to the output of the algorithm, that is all obscured. There is no way to know why the app is making these decisions for me."
>
> — Longtime Uber driver[15]

As corporations use worker data to generate detailed profiles and performance metrics, workers' experiences of employer manipulation arising from information asymmetries are becoming routine.[16] These experiences will become even more common as privacy-enhancing technologies (PETs),[17] such as *homomorphic encryption*,[18] *functional encryption*,[19] and *differential privacy*,[20] are introduced in the workplace. These types of PETs allow users to analyze a dataset without identifying the individual pieces of underlying data, much in the same way that a viewer of an impressionistic painting can, from a distance, discern the overall pattern of a field, pond, or city street, without seeing the tiny, discrete daubs of color that make up the image.

Adoption of these technologies is surging: the global PET market is on track to explode from $2.4 billion in 2023 to $25.8 billion by 2033.[21] (Privacy expert Elizabeth Renieris has noted that "companies with the historically most data-intensive practices are now among the most fervent advocates and adopters of PETs."[22]) Corporations can deploy these technologies to "preach the gospel of privacy" and legitimately claim they never saw an individual's raw data, even as they extract data-driven insights relating to people's behaviors, habits, or risks, and "continue to carry out the same activities they have always undertaken."[23] These technologies can frustrate accountability,[24] obscure bias,[25] and deepen industry control by facilitating and incentivizing more data sharing between corporations.[26] As legal scholar Michael Veale has highlighted, even without accessing any individual's personal data, new cryptographic tools and privacy technologies can be used to "spotlight the roads where a protest is planned" or identify areas or industries likely to employ migrant workers.[27]

One adopter of PETs is Uber, a company that has been dogged by allegations that they use data to lower driver pay and and keep passenger fares high.[28] In 2017, Uber announced an open-source tool that would allow it — and any other company using the tool — to gather statistical results from large datasets without seeing the personal details of any single user.[29] Uber's then head of privacy engineering reportedly explained that the company's differential privacy tool would allow its analysts to perform "statistical roll ups, sums, averages, counts, things like that, without needing to access the raw data."[30]

Uber justified these potentially problematic ends by implying the solution to privacy-related concerns was technological, i.e., "integrating differential privacy into our analytics pipeline, *ensuring we can continue to improve our business with data-driven insights* while using leading-edge privacy technology."[31] Uber's privacy principles, published in 2021, also emphasize the protection of individual-level, personal *data*: "We do the right thing with *data*" and "We safeguard personal *data*."[32] Meanwhile, the company's profit-driven data analysis and extraction appear to only deepen.[33] A recent national survey of more than 2,500 Uber drivers found that seven in ten drivers report experiences that suggest the company's AI manipulates driver pay in ways that push drivers to accept lower fares or stay on the road for longer, and that drivers commonly report serious financial hardship and psychological distress as a result of difficulty predicting their pay on the app.[34]

Unless laws and regulatory frameworks account for the impacts of these so-called privacy enhancing technologies[35] — and focus on protecting not just personal data, but also actual persons — workers will continue to remain susceptible to these unaccountable forms of data-driven control, manipulation, and exploitation.[36]

B. **Synthetic Data: A New Frontier for Worker Exploitation Without Accountability**

> "When you're out there, and you can hear them moving around, but you can't see them, it's like 'Where are they going to come from?' It's a little nerve-wracking at first."
>
> — Amazon warehouse worker, describing wheeled robots in her facility[37]

Synthetic data — or AI-generated data which can be used in robotics, computer vision, and automated decision-making systems — is rapidly becoming a popular tool. Tech industry consultant Gartner estimates that by 2030, synthetic data will "completely overshadow" real data in AI models.[38] Synthetic data is generally cheaper than collecting real world data.[39] In theory, properly designed AI models trained on synthetic data can reach conclusions statistically similar to those trained on real data.[40] Rather than collecting information directly from workers, companies can use AI-generated synthetic data to simulate and predict worker behavior, bypassing labor and data protections premised solely on regulating personal data, while claiming to protect privacy.[41] Even though synthetic data may allow companies to make predictions or decisions about workers without using personal data in the legal sense, it can still harm workers.[42]

Amazon has reported using synthetic data to simulate its warehouse operations in order to train robots in its fulfillment centers.[43] Robots play a key role in Amazon's warehouses. Over its history, the company claims to have developed, produced, and deployed over one million robots across its warehouse operations network.[44] According to Amazon Robotics' chief technologist, "[w]e're using generative AI in just about everything that we're doing inside of robotics."[45]

But all this accelerated automation may come at a human cost. There is a risk that corporations can use synthetic data to accelerate the deployment of automated systems that may displace workers, degrade their working conditions, and heighten their risk of physical injury.

Since 2019, investigative reports have identified a correlation between Amazon's adoption of robotics technology and worker health and safety problems.[46] Further, according to a *Wall Street Journal* analysis of Amazon's warehouse workforce, "[r]obots are also supplanting some employees, helping the company to slow hiring," and the "average number of employees Amazon had per facility last year, roughly 670, was the lowest recorded in the past 16 years."[47]

Rather than enhancing privacy in any meaningful way, synthetic data can open the door to new forms of evasion and exploitation. These include:

- **Regulatory evasion and limits to enforcement:** Laws regulating personal data may not apply to synthetic data.[48] Even when such laws do apply, an enforcer may not be able to tell whether synthetic or personal data was used, incentivizing companies to falsely claim compliance by masking real data use behind synthetic generation.[49]

- **Deepening black-box decision-making:** Synthetic data can undermine legal requirements of explainability and interpretability. Generally, the more sophisticated the synthetic data generator, the more difficult it becomes to explain correlations and — even more strongly — causality, in the data generated.[50]

- **Even more invasive profiling:** By filling gaps that exist in real-world data, synthetic data can increase the quality of a data set. But excessively high correctness and precision of factual and predictive data carries its own risks.[51] Technology ethicists warn of the possibility that forms of facial recognition and computer vision technologies, which are fueled by synthetic data to analyze crowds and predict unrest, could be adapted to predict and quell worker organizing.[52]

- **Undermining accountability:** Because synthetic data adopts the rhetorical mantle of privacy and artificiality, harmful practices might attract less legal or ethical scrutiny when synthetic data is used than when real worker data is used.[53]

Unless regulation evolves to recognize and address the use of synthetic data, workers will continue to face digital profiling, discipline, and job displacement without legal recourse.

C. How Multi-Party Computation and Federated Learning Enable Invisible Surveillance

> "If you want to ask me a question, and I choose to answer it, that's fine. But to... basically put me under a microscope and see how I'm writing things, or how my body's responding to different things [to infer that information]... [that] I don't like."
>
> — Social worker, describing an employer's use of emotion AI to infer what she is feeling[54]

Techniques like multi-party computation (MPC) and federated learning (FL) enable corporations to collaboratively analyze data or train models without directly sharing their underlying datasets. MPC allows multiple parties to jointly compute results while keeping their data encrypted.[55] FL enables multiple devices to jointly train a machine learning model by processing data locally so that it does not need to be transferred to a central server; the result is that one party can analyze another party's personal data without being in actual possession of it.[56] This can confound enforcement under legal frameworks that attribute harm to the person or entity who "touched" (or collected and processed) the personal data.[57] On paper, MPC technology looks privacy-enhancing, but in practice, corporations can wield it to coordinate data consolidation and surveillance while evading accountability.[58]

One active application of FL is in wearable devices.[59] FL can be used to assist in "emotion AI" and "affect detection," computation that is designed to detect a person's mental and emotional state via physiological signals.[60] Despite concerns about accuracy and bias,[61] the market size of emotion AI technologies is expected to grow to nearly $450 billion by 2032.[62] Decentralized FL techniques can serve as a tool for industry to deploy emotion AI while avoiding many of the organizational risks of running afoul of data protection laws.[63] For example, FL is among the tools recommended on a Cogito Tech blog that companies can use to "safeguard data from unauthorized access or breaches *while preserving the utility.*"[64]

Regardless of whether FL is used to protect worker *data,* harms to the *worker* remain.[65] In a 2023 research study:

- A custodian described emotion AI inferring their "deeper" felt emotions as akin to "spying" that crosses "a huge privacy boundary."[66]
- A social worker worried her emotion data would lead to a poor performance review on the grounds that "I wasn't necessarily happy or something like that."[67]
- A customer service representative described the distress of having to provide support to customers who, upon recognizing her identity as a Black woman, met her with disdain.[68] She "shared how difficult it was to maintain positivity 'when your insides are crying …,' knowing that [her] emotions were monitored to make sure of it."[69]

These harms are unlikely to be prevented through "technical solutions or the governance of emotion data."[70] Rather, they require more direct policy interventions.

II. Forward-Looking Design Principles for Labor and Technology Policy

As new technologies facilitate the widespread processing of aggregated, anonymized, and de-identified data, the limits of "chase-the-data" regulatory strategies may soon entirely overwhelm their merits.[71] Without proactive safeguards to regulate labor outcomes, innovation will continue to be leveraged as a tool for exploitation. To reverse this trajectory, we need policies that put worker dignity, autonomy, and collective power at the center. Below are three policy design principles that can guide regulation that is more durable and just. These principles are not a litmus test. Rather, they are core values that stakeholders and policymakers can consider when developing worker protections that will endure through the rapid technological changes on the near horizon. They are intended to be read in tandem with other tech policy recommendations advanced by unions, worker centers, and labor advocates.[72]

A. **Eliminate the employer surveillance prerogative and stop harm at the source** by preventing abusive surveillance from happening in the first place.

Policymakers should place bright-line rules on the act of "datafication,"[73] or on the collection or generation of worker data itself, and not only on the post-hoc use of data. Businesses use an array of workplace technologies to capture and analyze data, ranging from obvious tactics, such as directly surveying workers, to more hidden ones, such as embedding microphones in worker badges.[74] The problem is not only the use of such data; the harm also often arises at the point of data collection.[75] Data is slippery. Once created, it can be anonymized, aggregated, synthesized, de-identified, confidentially computed, stored, sold, shared, and more. A first step in interrupting this cycle of harm is to close the spigot: we must end what legal scholar Ifeoma Ajunwa and her co-authors have described as "limitless worker surveillance."[76]

At the root of this worker datafication problem are default legal rules that, apart from extremely limited legal protections that may prevent surveillance in break rooms and bathrooms, generally allow employers to collect and use worker data however they want.[77] The advent of increasingly invasive, low-cost workplace monitoring technology requires us to rethink these default rules.

Stronger workplace technology laws should aim to break, as appropriate, what we call "the employer surveillance prerogative."[78] In other words, policymakers should ban electronic monitoring of workers outright, especially mass, continuous surveillance. When intermittent electronic workplace monitoring is permitted, it should follow strict minimization principles. Specifically, it should only be allowed when it is strictly necessary (such as for legal compliance), affects the smallest number of workers, collects the least amount of necessary data, and is narrowly tailored to use the least invasive means.[79] Additionally, businesses should be required to notify workers of the use of electronic monitoring as well as its intended purpose. Laws that prevent the sale and repurposing of any worker data that has been collected are also critical for interrupting the business imperative to collect and exploit as much data as possible.

There are signs that state and local lawmakers are starting to push for setting boundaries on employer surveillance and datafication. One example is Massachusetts' **Fostering Artificial Intelligence Responsibility (FAIR) Act**,[80] proposed in 2025, which would strictly prohibit electronic monitoring that includes facial recognition, gait analysis, or emotion recognition technologies.[81] The bill would also bar audio or visual surveillance in private spaces, such as bathrooms, prayer rooms, break areas, and workers' homes and personal vehicles — a necessary protection in a world of hybrid and remote work.[82] California's **Assembly Bill 1331**, proposed in 2025, also takes steps to advance worker autonomy.[83] The bill would prohibit companies from requiring workers to physically implant tracking devices[84] or wear always-on surveillance tech.[85] It would also give workers the right to leave behind monitoring tools during off-duty hours and in personal or private spaces, including during rest periods and meal breaks.[86]

Together, these bills reflect a critical turning point in labor-tech regulation. They recognize that protecting worker data is no substitute for protecting workers' space, time, and autonomy.

B. **Focus on worker outcomes and refuse to play cat and mouse with the tech industry** by widening the lens to target not only the boss's tech-driven means, but their harmful ends.

Legal frameworks that focus on technicalities tend to disadvantage workers, exacerbating power asymmetries and information imbalances. This is all the more true in recent years, as rapid advancements in technology have made it increasingly challenging for workers and regulators to accurately determine the precise data inputs or processes of a given machine learning model or AI technique. This can trap policymakers in a cat-and-mouse game, in which they enact laws that only apply based on exactly how a particular problematic technology is built or the specific invasive data inputs it uses, only to have corporations leapfrog over the law by deploying new technologies that bypass its reach while still achieving the same harmful ends.

To ensure that worker protections sufficiently address real-world impacts, policymakers should go beyond merely regulating technical inputs, such as how data is collected or anonymized, and also focus on the intended and unintended real-world outcomes these systems produce for workers. A new generation of laws that guarantees workers digital rights for the 21st century should focus on addressing and preventing tangible harms like scheduling instability, unfair discipline, surveillance-based stress, dangerous work speed quotas, health and safety risks from automated decision-making, and job precarity, regardless of the type of technology used or whether companies technically comply with privacy standards.

One way to accomplish this is to establish bright-line rules prohibiting the use of automated decision-making technologies in certain situations.[87] Another is to evaluate how technologies may harm workers, and to address or prevent those harms. For example, the federal **Warehouse**

Worker Protection Act, proposed in 2024,[88] prohibits dangerous work speed quotas that interfere with workers' ability to use the bathroom and take guaranteed breaks, or that are set in time increments shorter than one day.[89] Following years of reported high injury rates among warehouse workers due to technology-enabled monitoring,[90] the bill directs the Occupational Safety and Health Administration (OSHA) to create an ergonomic management standard for warehouse workers.[91] This mandate also reflects a need to authorize existing regulatory agencies to update and advance protections for the new challenges of data-driven workplaces.

In the specific instances when worker data collection is permitted, a policy focus on worker outcomes should also create clear liability and consequences for any harms that result. **New York City's Secure Jobs Act**, which was introduced in 2024, would establish a just-cause standard that, in essence, shifts the burden of proof to an employer to justify a worker's termination.[92] The proposed bill also specifically prohibits employers from firing workers based on data from biometric technologies, geofencing technologies (location tracking), apps installed on personal devices, and recordings taken within the private homes of employees.[93]

One advantage of policy approaches that plainly restrict certain employer practices is their legibility: they do not require workers or regulators to decipher black-box systems. Such laws better enable workers to recognize when their rights have been violated. One early and instructive example is **fair workweek laws**, which protect workers from scheduling changes without notice or remuneration.[94] A number of states and localities have enacted these laws in response to the rise of just-in-time scheduling practices, in which employers, often using data-driven software, attempt to "optimize" labor costs via highly unpredictable worker scheduling changes. Fair workweek protections do not regulate technicalities, like what data is fed into the algorithm; rather, they disincentivize the problem itself by requiring employers to compensate workers financially for last-minute scheduling changes.

Both fair scheduling and warehouse quota laws are examples of how regulators can create new substantive rights for workers by designing new workplace regulations for emerging technology-induced harms that were not previously recognized under law. These types of policies are readily enforceable and have a concrete, direct impact on working conditions.[95]

C. **Prioritize policies that enhance worker autonomy and check corporate power** by rebalancing power asymmetries**.**

To advance worker power in the age of AI, policymakers must recognize that the core problem is not the protection of particular pieces of data, but how emerging workplace technologies can exacerbate power asymmetries and structural exploitation.[96] Now is the time for state and local legislators to move beyond a narrow focus on individual privacy and take steps to legislate with clear standards that enhance worker power.

First, policymakers should support mechanisms that bolster workers' collective participation throughout all stages of the development and deployment of workplace technology.[97] Foundationally, it is critical for policymakers to support workers' rights to collectively bargain,[98] as unions and other worker associations have quickly proven to be among the most impactful stakeholders in incorporating worker expertise in new tech deployments.[99] Even when unions or organized worker centers are not present in a particular workplace, there are still opportunities to ensure meaningful worker input. These include: incorporating worker participation in all stages of AI development, deployment, and redesign; treating worker participation as work and compensating workers for their time; and designing high-quality engagement methods, such as prioritizing workers as the key source of knowledge to identify problems and respecting workers' rights throughout the process.[100]

Second, policymakers should apply this brief's analysis to ensure that the public and private enforcement provisions in new labor-tech laws match the scale and sophistication of emerging Privacy-Preserving AI Techniques like synthetic data and multiparty computation. Legislators should strengthen the investigative authority and internal capacity of labor agencies, state attorneys general, and local enforcement authorities to conduct public hearings, compel transparency, and scrutinize employer practices even when data is anonymized or decentralized.[101] Recognizing the tremendous consolidation of corporate power behind AI,[102] legislators should also ensure that penalties are scaled to deter abuse, so that even the biggest corporations take the law seriously. This may include profit disgorgement and executive- or investor-level sanctions that hold decision-makers personally accountable, not just their firms.[103]

Steps to strengthen private enforcement are equally important, given that under-resourced government agencies will not have the capacity to vindicate workers' rights violations on their own. As a starting point, new workplace technology rights should always include a private right of action (PRA), or the right of a private individual or organization (not just the government) to sue an employer or business in court, either individually or in a class action. Business lobbies have vigorously resisted the inclusion of PRAs in tech related legislation,[104] even though PRAs are the standard legal mechanism for workers and consumers to enforce their rights,[105] and offer the most direct access point for creating accountability in the private sphere.[106] Relatedly, in cases involving algorithmic decision-making or surveillance, the burden of proof should rest with employers, e.g., to demonstrate that their use of such technology fits specific categories of permissible use, or to show that they have chosen the narrowest version of electronic monitoring available.

Third, given the secrecy that pervades the tech sector, enacting strong whistleblower protections is also essential.[107] Whistleblowers are why we know about technology controversies involving companies ranging from Facebook to Instagram to Uber.[108] Strong whistleblower laws that cover workplace technology developers as well as both worker and supervisor users of these technologies can encourage insider disclosures that may uncover violations, inform public discussion, and spur action by consumers and policymakers.[109]

Last, strengthening anti-retaliation laws helps to protect line-level workers' ability to individually and collectively address the new forms of injustice arising from electronic surveillance, monitoring, and control.[110] Front-line workers will be the first ones to identify the harms from these technologies. We all benefit when they have the protections they need to step forward.

Conclusion

The design principles in this brief offer a path to move beyond the narrow frameworks of data protection that have dominated tech policymaking for decades. In our conversations with workers, academics, and technologists, an overriding theme was that Privacy-Preserving AI Techniques are, in essence, the newest face of an age-old problem: corporations putting profits over people. The stakes are high: dignity, fairness, and voice on the job. To advance durable protections for workers, it is critical to eliminate the employer surveillance prerogative, focus on worker outcomes, and prioritize worker autonomy and check corporate power. We need safeguards rooted in collective rights, structural accountability, and democratic participation. Across the country, a growing coalition of labor leaders, civil society organizations, technologists, and policymakers is rising to meet this challenge. Together, we are forging new regulatory models — ones that treat workers not as data points, but as decision-makers.

Acknowledgments

This brief would have not been possible without the remarkable contributions of Research, Worker, and Policy Council members.

A special thanks to Iretiolu Akinrinade, Ben Beach, Lindsey Cameron, Adam Cantwell-Corn, Sergio Di Martino, Melodi Dincer, Sharon DuChessi, Elizabeth Epstein, Nell Geiser, Ryan Gerety, Tara Jeane, Michelle Miller, Mariah Montgomery, Mary Mueller-Reich, Sarah Myers West, Timothy Newman, Maya Pinto, Gabrielle Rejouis, and Sophie Song. All errors are the authors’ own.

Endnotes

[1] We derive the term "Privacy-Preserving AI Techniques" from the research of Yew, et al., which focuses on how "the cover of compliance with data protection and privacy laws can enable the use of [privacy-preserving AI] PPAI to increase data consolidation and surveillance." Yew, Rui-Jie, et al. "You Still See Me: How Data Protection Supports the Architecture of AI Surveillance." *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, vol. 7, 2024, p. 1710.

[2] Negrón, Wilneida. *Little Tech is Coming for Workers: A Field Guide to the Technologies Being Used to Manage Workers Today*. Coworker.org, Nov. 2021; Hertel-Fernandez, Alexander. *Estimating the Prevalence of Automated Management and Surveillance Technologies*. Washington Center for Equitable Growth, 1 Oct. 2024.

[3] Hertel-Fernandez, *supra*. *See also* Patel, Seema N. "Governance & Guardrails: Artificial Intelligence and Low-Wage Workers." 85 *Maryland Law Review* 1 (forthcoming Nov. 2025) (documenting how AI-powered technologies harm workers in low-wage industries); Gutelius, Beth, et al. *Pain Points*. University of Illinois Chicago, Center for Urban Economic Development, 2023 (describing toll of electronic monitoring and surveillance on Amazon warehouse worker health and well-being).

[4] Kaal, Wulf A. "Dynamic Regulation for Innovation." *Perspectives in Law, Business & Innovation* (Mark Fenwick, Wulf A. Kaal, Toshiyuki Kono & Erik P.M. Vermeulen eds.), New York Springer, 2016, U of St. Thomas (Minnesota) Legal Studies Research Paper No. 16-22; Gal, Mishal, et al. "Synthetic Data: Legal Implications of the Data-Generation Revolution." 109 *Iowa Law Review* 1087, 2024, pp. 1139, 1147.

[5] California's CCPA (Cal. Civ. Code §§ 1798.100 et seq.) remains the only comprehensive statewide data privacy law that does *not* generally exclude employee data from its protections. The law has been described as "an important first step in making sure that workers have the tools necessary to advocate for their rights in the 21st century data-driven workplace." Technology and Work Program at the UC Berkeley Labor Center. *Summary: Worker Rights Under the CCPA/CPRA*. UC Berkeley Labor Center, 21 Nov. 2023.

[6] Buttarelli, Giovanni. "The EU GDPR as a Clarion Call for a New Digital Global Standard." *International Data Privacy Law*, vol. 6, issue 2, 2016; Andrew, Jane, et al. "The General Data Protection Regulation in the Age of Surveillance Capitalism." *Journal of Business Ethics*, 2021, p. 565; Zanker, Marek, et al. "The GDPR at the Organizational Level." *E&M Economics and Management*, 2021, p. 207.

[7] Keogh, Brian. "50 Attorneys General Investigate Google: Surveillance Capitalism and Legal Privacy Frameworks." 30 *Transnational Law & Contemporary Problems* 267, pp. 273–276; Meaker, Morgan. "The Slow Death of Surveillance Capitalism Has Begun." *Wired*, 5 Jan. 2023; Zard, Lex, et al. "Targeted Advertising and Consumer Protection Law in the European Union." 56 *Vanderbilt Journal of Transnational Law* 799, pp. 802–803.

[8] Yew, *supra*, at p. 1712. Moreover, the rise of publicly available information online as well as increasingly sophisticated computing hardware has made it possible to re-identify "anonymized" data. "Re-identification of anonymized data has grave privacy and policy implications as regulators, businesses, and consumers struggle to define privacy in the modern permanently-recorded age." Lubarsky, Boris. "Re-Identification of 'Anonymized' Data." *Georgetown Law and Technology Review*, vol. 1, 2017, p. 202. *See generally* Ohm, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." 57 *UCLA Law Review* 1701, 2010.

[9] Susser, Daniel. "From Procedural Rights to Political Economy: New Horizons for Regulating Online Privacy." *The Routledge Handbook of Privacy and Social Media*. Routledge, 2023, p. 283; Solove, Daniel. "The Limitations of Privacy Rights." 98 *Notre Dame Law Review* 975, 2023, pp. 977, 982–983, 994, 1015.

[10] Nguyen, Aiha. "A Collective Work Agenda for the Digital Economy." *Friedrich Ebert Stiftung Briefing*, Apr. 2024.

[11] Patel, "Governance and Guardrails," *supra*; Ruckelshaus, Catherine K. "Labor's Wage War." 35 *Fordham Urban Law Journal* 373, 2008, p. 384.

[12] Sum, Cella, M., et al. "'It's Always a Losing Game': How Workers Understand and Resist Surveillance Technologies on the Job." *arXiv preprint arXiv:2412.06945*, 2024.

[13] Zickuhr, Kathryn. "Workplace surveillance is becoming the new normal for U.S. workers." *Washington Center for Equitable Growth*, 18 Aug. 2021; Rogers, Brishen. "Workplace Data and Workplace Democracy." 6 *Georgetown Law Technology Review* 454, 2022; Bodie, Matthew, "Beyond Privacy." *The Law and Political Economy Project*, 7 Feb 2023. *See also* Andrew, Jane, et al. "The General Data Protection Regulation in the Age of Surveillance Capitalism." *Journal of Business Ethics*, vol. 168, 2021, pp. 565–578. Laidler, John. "High Tech is Watching You." *The Harvard Gazette*, 4 Mar. 2019.

[14] *See generally* Adler-Bell, Sam, et al. *The Datafication of Employment.* The Century Foundation, 19 Dec. 2018 (noting how "corporate surveillance enable[s] a pernicious form of rent-seeking — in which companies generate huge profits by packaging and selling worker data in marketplace [sic] hidden from workers' eyes"); Mateescu, Alexandra. "Explainer: Challenging Worker Datafication." *Data & Society*, Nov. 2023, pp. 2–3.

[15] Tobias, longtime Uber driver, interview, in Dubal, Veena. "On Algorithmic Wage Discrimination." 123 *Columbia Law Review* 1929, 2024, p. 1972.

[16] Alacovska, Ana, et al. "Algorithmic Paranoia: Gig Workers' Affective Experience of Abusive Algorithmic Management." *New Technology, Work, and Employment*, 2024, pp. 1, 13; Todolí-Signes, Adrián. "Making Algorithms Safe for Workers: Occupational Risks Associated with Work Managed by Artificial Intelligence." *Transfer: European Review of Labour and Research*, vol. 27, no. 4, 2021, pp. 433–452, pp. 8–10 (pre-print); Korogodsky, Alexander. "Recursive Impacts of Algorithmic Management on Trust and Employee Productivity in Professional Work Settings." *Proceedings of the 58th Hawaii International Conference on System Sciences*, 2025, pp. 5424–5425; *Uber's Inequality Machine*. PowerSwitch Action, et al. Jun. 2025, p. 5 (finding, in a national survey of more than 2,500 Uber drivers, that 78% of drivers reported that driving on the Uber app feels like gambling — the occasional good fare keeps them going).

[17] Synthetic data and MPC, including federated learning, may also be categorized as PETs. We address these techniques in Sections B and C, *infra*. In this Section, we focus on homomorphic encryption, functional encryption, and differential privacy.

[18] Homomorphic encryption allows companies to analyze encrypted data and decrypt the result, without ever seeing the underlying unencrypted data. *See* Armknecht, Frederik, et al. "A Guide to Fully Homomorphic Encryption." *Cryptology ePrint Archive*, 2015, p. 1.

[19] Functional encryption allows certain questions to be asked of encrypted data. *See* Veale, Michael. "Rights for Those Who Unwillingly, Unknowingly and Unidentifiably Compute!" 2023, p. 5, to appear in Micklitz, Hans W., et al. eds. *The Future of the Person in Private Law.* Bloomsbury Press, 2025.

[20] Differential privacy allows a party to introduce random "noise" into a dataset, thus allowing analysis of the dataset, even as individual data points are no longer easily identifiable. *See* Ebadi, Hamid, et al. "Differential Privacy: Now It's Getting Personal." *ACM Sigplan Notices*, vol. 50, no. 1, 2015, pp. 69–81.

[21] Jacobson, Jon. "The impact of privacy-enhancing technologies (PETs) on business, individuals, and society." *World Economic Forum*, 25 Oct. 2023.

[22] Renieris, Elizabeth. Beyond Data. The MIT Press, 2023, p. 85.

[23] *Id.*, pp. 78, 88, 94 (explaining that "big tech's rhetorical shift and strategic adoption of PETs and other measures taken in the name of 'privacy' are actually helping it preserve and consolidate power in the face of a governance crackdown narrowly focused on data."); Veale, "Rights for Those Who Unwillingly, Unknowingly and Unidentifiably Compute!" *supra*, at p. 5; Veale, Michael. "Privacy Is Not the Problem with the Google-Apple Contact Tracing Toolkit." *The Guardian*, 1 Jul. 2020.

[24] Renieris, *supra*, at p. 85 (stating that "PETs can be notoriously difficult for lawmakers and policymakers to audit or govern").

25 *Id.*, pp. 86–87 (noting that PETs "can legitimize activities that many would otherwise find objectionable," with resulting harms that can include "discrimination, harassment, exclusion, and exploitation").

26 *Id.*, p. 88.

27 Veale, *supra*, "Privacy Is Not the Problem."

28 Dubal, "On Algorithmic Wage Discrimination," *supra*, at pp. 1961–1976 (describing how algorithms can be used to make worker pay opaque and unpredictable); Kloczko, Justin. *Surveillance Price Gouging*. Consumer Watchdog, Dec. 2024; Simonite, Tom. "When Your Boss Is an Uber Algorithm." *MIT Technology Review*, 1 Dec. 2015; *Driven Out By AI*. Action Center on Race and the Economy, Spring 2025; Sherman, Len. "The Inconvenient Truths Uber's CEO Does Not Want You to Know." *Medium*, 12 Aug. 2024. *See also* Sherman, Len. "Uber's CEO Hides Driver Pay Cuts to Boost Profits." *Forbes*, 15 Dec. 2023.

29 Greenberg, Andy. "Uber's New Tool Lets Its Staff Know Less About You." *Wired*, 13 Jul. 2017; Tezapsidis, Katie. "Uber Releases Open Source Project for Differential Privacy." *Medium*, 13 Jul. 2017.

30 Greenberg, *supra*.

31 Tezapsidis, *supra* (emphasis added).

32 Uber Technologies, Inc. "Schedule 14-A 2021," *Securities and Exchange Commission EDGAR Online*. Securities and Exchange Commission, 29 Mar. 2021 (emphasis added); *Business Conduct Guide*. Uber, 2021, p. 30 (emphasis added). *See also* Renieris, *supra*, at p. 82.

33 "Uber's Profit, Power, and Problems with CEO Dara K." *Podcast Episode - On with Kara Swisher*, 30 Oct. 2023 (Uber CEO Dara Khosrowshahi stating, "We use AI when you get quoted a price for an Uber, when a driver gets an offer for a particular ride, when we route you, when you open up Uber Eats. All of it is powered by AI. So AI is intermingled and every single part of our service at this point and these algorithms are superior to the technology that we had 5 to 10 years ago because they learn a skill in a personalized way. It's pretty powerful tech out there."); Sherman, "The Inconvenient Truths Uber's CEO Does Not Want You to Know," *supra*; Sherman, "Uber's CEO Hides Driver Pay Cuts to Boost Profits," *supra*. *See generally* Dubal, "On Algorithmic Wage Discrimination," *supra*.

34 PowerSwitch Action, *supra*, at p. 3. *See generally* Dubal, Veena and Wilneida Negrón, "How Artificial Intelligence Uncouples Hard Work from Fair Wages Through 'Surveillance Pay' Practices – and How To Fix It." *Washington Center for Equitable Growth*, 21 Aug. 2025 (describing a first-of-a-kind audit of AI labor management vendors suggesting that traditional employers are now also using automated surveillance and decision-making systems to set compensation structures and to calculate individual wages); Wells, Katie and Funda Ustek Spilda, "Uber for Nursing," *Roosevelt Institute*, 17 Dec. 2024 (finding, through original interviews with "gig" nurses and assistants, that the gig economy's labor model and its algorithmic management technologies have a foothold in the healthcare sector).

35 Confidential computing technologies may be covered under broader definitions of “processing” personal data, although coverage may depend on the exact nature of the dataset and how it was processed, inviting potential litigation, questions of proof and room for interpretation by the relevant legal authorities. Inverarity, Calum. *Modern PETs and Confidential Computing: No Way Out from GDPR Obligations*. Open Data Institute, 8 Sep. 2023. *See also* Patel, “Governance and Guardrails,” *supra*.

36 *See generally* Renieris, *supra*, at p. 91.

37 O’Brien, Matt. “As Robots Take Over Warehousing, Workers Pushed to Adapt.” *Associated Press*, 30 Dec. 2019.

38 *Is Synthetic Data the Future of AI? Q & A with Alexander Linden*. Gartner, 22 Jun 2022.

39 Wiehn, Tanja. “Synthetic Data: From Data Scarcity to Data Pollution.” *Surveillance & Society,* vol. 22, no. 4, 2024, p. 472. For a description of various ways synthetic data is produced, *see* Steinhoff, James. “Toward a Political Economy of Synthetic Data: A Data-Intensive Capitalism That Is Not a Surveillance Capitalism?” *New Media & Society*, vol. 26, no. 6, pp. 3296–3298.

40 Steinhoff, *supra*, at p. 3296. Synthetic data, however, does not eliminate the need for data quality. For example, the performance of large-scale models trained successively on synthetic data will degrade over time. Shumailov, Ilia, et al. “AI Models Collapse When Trained on Recursively Generated Data.” *Nature*, vol. 631, 2024, pp. 755–759.

41 Jayashankar, Rakshitha, et al. “Advancing Employee Behavior Analysis Through Synthetic Data.” *arXiv preprint arXiv:2409.14197*, 2024; Sakka, Fadi. “Harnessing Structural Equation Modelling Based Synthetic Data with Artificial Intelligence on Employee Performance Prediction Model in Multinational Organisations.” *International Research Journal of Multidisciplinary Scope*, vol. 6, no. 2, 2025, pp. 71–80; Wiehn, *supra*, at pp. 472–473.

42 Gal, *supra*, at p. 1137.

43 *5 Ways Amazon is Using AI to Improve Your Holiday Shopping and Deliver Your Package Faster.* Amazon, 22 Nov. 2024, www.aboutamazon.com/news/operations/amazon-uses-ai-to-improve-shopping. *See also* Bosset, Pierre. *Amazon Robotics Combines the Power of NVIDIA Omniverse and Adobe Substance 3D to Simulate Warehouse Operations*. Adobe Blog, 30 Nov. 2023, https://blog.adobe.com/ en/publish/2023/11/30/amazon-robotics-combines-power-nvidia-omniverse-adobe-substance-3d-simulate-warehouse-operations; Andrews, Gerard, Sr. “From Virtual to Reality: How Synthetic Data Will Train Smarter Robots for Industrial Applications.” *Medium*, 9 Nov. 2023.

44 *Amazon Has More than 750,000 Robots that Sort, Lift, and Carry Packages — See Them in Action.* Amazon, 3 Mar. 2025, https://www.aboutamazon.com/news/operations/amazon-robotics- robots- fulfillment-center; *Amazon Launches a New AI Foundation Model to Power Its Robotic Fleet and Deploys Its 1 Millionth Robot*. Amazon, 30 Jun. 2025, https://www.aboutamazon.com/news/operations/ amazon-million-robots-ai-foundation-model.

[45] Kell, John. “Amazon’s Big Bet on Warehouse Robots is Already Getting a Boost From Generative AI.” *Fortune*, 19 Feb. 2025.

[46] Anway, Nicholas. “Amazon’s Approach to Robotics Is Seriously Injuring Warehouse Workers.” *On Labor*, 5 May 2022; *The Injury Machine: How Amazon’s Production System Hurts Workers.* Strategic Organizing Center, Apr. 2022.

[47] Herrera, Sebastian. “Amazon Is on the Cusp of Using More Humans Than Workers in Its Warehouses.” *Wall Street Journal*, 30 Jun. 2025.

[48] Gal, *supra*, at p. 1147.

[49] *Id.*, at p. 1148.

[50] *Id.*, at p. 1149.

[51] Chen, Jia Hong. “The Dangers of Accuracy: Exploring the Other Side of the Data Quality Principle.” *European Data Protection Law Review*, vol. 36, 2018, pp. 40–42 (warning of new forms of discrimination and loss of maneuvering space for individual self-determination).

[52] Susser, Daniel and Jeremy Seeman. “Critical Provocations for Synthetic Data.” *Surveillance and Society*, vol. 22, no. 4, 4 Nov. 2024, p. 455.

[53] *Ibid.*

[54] Interview in Roemmich, Kat, et al. “Emotion AI at Work: Implications for Workplace Surveillance, Emotional Labor, and Emotional Privacy.” *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 2023, pp. 5, 7.

[55] Yew, *supra*, at p. 1710.

[56] *Id.*, at pp. 1710, 1712; Renieris, *supra*, at p. 82.

[57] Yew, *supra*, at p. 1714.

[58] *Id.*, at p. 1710.

[59] Wang, Wenshou, et al. “A Privacy Preserving Framework for Federated Learning in Smart Healthcare Systems.” *Information Processing & Management*, vol. 60, no. 1, Jan. 2023.

[60] Saylam, Berrenur, et al. “Federated learning on Edge Sensing Devices: A Review.” *arXiv preprint arXiv:2311.01201*, 2023, p. 19, citing Can, Yekta Said, et al. “Privacy-Preserving Federated Deep Learning for Wearable Iot-Based Biomedical Monitoring.” *ACM Transactions on Internet Technology (TOIT)*, vol. 21, issue 1, 2021, pp. 1–17; Feng, Jie, et al. “A Privacy-Preserving Human Mobility Prediction Framework via Federated Learning.” *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4, 2020, pp. 1–21; Sozinov, Konstantin, et al. “Human Activity Recognition Using Federated Learning.” *2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications* 33 (ISPA/IUCC/BDCloud/SocialCom/SustainCom), IEEE, 2018, pp. 1103–1111; Ek, Sannara, et al. “Evaluation of Federated Learning Aggregation Algorithms: Application to Human Activity Recognition.” *Adjunct Proceedings of the 2020 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2020 ACM International Symposium on Wearable Computers*, 2020, pp. 638–643.

61 Barrett, Lisa. "Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements." *Psychological Science in the Public Interest*, 2019.

62 Andalibi, Nazanin. "Emotion AI Will Not Fix the Workplace." *Interactions*, vol. 32, no. 2, Mar.–Apr. 2025.

63 Roemmich, *supra*, at pp. 14–15.

64 *Navigating the Challenges of Multimodal AI Regulation*. Cogito Tech, 10 Sept. 2024 (emphasis added). *See also* De La Garza, Alejandro. "This AI Software Is 'Coaching' Customer Service Workers. Soon It Could Be Bossing You Around, Too." *Time*, 8 Jul. 2019 (describing Cogito, an artificial intelligence program that displays a notification on customer service agents' computers telling them "to slow down, speed up, stop talking, start talking or try to sound more sympathetic").

65 Roemmich, *supra*, at pp. 14–15 (noting that "[p]rivacy enhancement, regulation, and risk mitigation all have limits; a failure to consider at a more fundamental level whether it is just to develop, design, and implement systems that implicate the privacy of our inner, emotional lives can expose and exacerbate social injustices for all").

66 *Id.*, at pp. 5, 7 (interview in study).

67 *Id.* at pp. 5, 9 (interview in study).

68 *Id.* at pp. 5, 12 (interview in study).

69 *Ibid.*

70 *Id.*, at p. 15.

71 Viljoen, Salomé. "A Relational Theory of Data Governance." 131 *Yale Law Journal* 573, 2021, p. 613; Renieris, *supra*, at pp. 120–121. *See also* Negrón, Wilneida. *The Changing Landscape of Temporary Work: From Agencies, Apps, to AI*. Coworker, 2024, p. 6 (warning that "technological advancements have been insidiously linked to labor deregulation, contributing to the fragility of labor markets")

72 *See, e.g.*, Bernhardt, Annette, et al. *Data and Algorithms at Work: The Case for Worker Technology Rights*. The UC Berkeley Labor Center, 3 Nov. 2021; Boosting Worker Power and Voice in the AI Response. Center for Labor and a Just Economy, 24 Jan. 2024; Doellgast, Virginia, et al. *Boosting US Worker Power and Voice in the AI Economy.* Washington Center for Equitable Growth, 19 Feb. 2025.

73 Adler-Bell, *supra*.

74 Bernhardt, Annette, et al. "The Data-Driven Workplace and the Case for Worker Technology Rights." *ILR Review*, vol 76, no. 1, 2023, pp. 3–29.

75 Renieris, *supra*, at p. 133 (explaining that "by the time something has been datafied, it is often too late to negotiate on the grounds of power, inclusion, equity, or fairness")

76 Ajunwa, Ifeoma, et al. "Limitless Worker Surveillance." 105 *California Law Review* 735, 2017.

77 *Id.*, at pp. 747–748; Bodie, Matthew. "The Law of Employee Data." 97 *Indiana Law Journal* 707, 2022, p. 733; Wilborn, S. Elizabeth. "Revisiting the Public Private Distinction: Employee Monitoring in the Workplace." 32 *Georgia Law Review* 825, 1998, pp. 872–873 & n. 180. *See also* Patel, "Governance and Guardrails," *supra*.

78 We are indebted to Gali Racabi's analysis of the "employer prerogative" and how default workplace laws that favor the employer can both entrench deeply unequal power relations at work and limit our political imagination to change them. Such rules set a high legal bar for courts to displace them and weaken workers' bargaining power to negotiate for contractual changes. They also operate under the shadow of at-will employment and weak worker rights enforcement generally — both of which undermine workers' ability to make any of the changes that workers achieve to the default rule, real. As Racabi highlights, "Where you end up often depends on where you begin." *See* Racabi, Gali. "Abolish the Employer Prerogative, Unleash Work Law." *Berkeley Journal of Employment & Labor Law*, vol. 43, 2022, pp. 79, 85–87.

79 Bernhardt, Annette, et al. "The Data-Driven Workplace and the Case for Worker Technology Rights," *supra*.

80 2025–2026 Mass. Senate Bill 35 (Mass. S.B. 35); 2025–2026 Mass. House Bill 77 (Mass. S.B. 77). Accessed 25 Aug. 2025.

81 Mass S.B. 35 (as introduced), *supra*, at § 2(d)(ix); Mass. H.B. 77, *supra*, at § 2(d)(ix).

82 Mass S.B. 35 (as introduced), *supra*, at § 2(d)(vi)–(vii); Mass. H.B. 77, *supra*, at § 2(d)(vi)–(vii).

83 2025–2026 Cal. Assem. Bill 1331 (Cal. A.B. 1331). Accessed 25 Aug. 2025.

84 *Id.* (as introduced), § 1561, subd. (c).

85 *Id.* (as introduced), § 1561, subds. (a), (b).

86 *Id.* (as introduced), § 1561, subd. (b).

87 *Algorithmic Management: Restraining Workplace Surveillance.* AI Now Institute, 11 Apr. 2023.

88 *Sens. Markey, Smith, Casey Introduce Warehouse Worker Protection Act*, Ed Markey, United States Senator for Massachusetts, 2 May 2024.

89 United States, Congress, Senate. Warehouse Worker Protection Act of 2024. 118th Congress, Senate Bill 5208, Introduced 2 May 2024 ("Warehouse Worker Protection Act") (as introduced), Title I, § 8, subds. (c)(1)(A)(i), (c)(1)(A)(ii), (c)(1)(B), (c)(1)(C).

90 Tung, Irene, et al. *Amazon's Outsized Role: The Injury Crisis in US Warehouses and a Policy Roadmap to Protect Workers*. National Employment Law Project, 2 May 2024.

91 Warehouse Worker Protection Act (as introduced), *supra*, Title III, § 301.

92 New York City Council, Int. 0909-2024 (2024) (as introduced), § 20-1272.a. The opposite of a "just cause" standard is an "at-will" standard, in which an employer has free rein to fire a worker for any reason at all, unless the employer's justification is not otherwise prohibited by law. The "at-will" standard is currently the default rule for nonunion, private-sector businesses in every state except Montana. Andrias, Kate, et al. *Ending At Will Employment*. Roosevelt Institute, Jan. 2021, at p. 4.

93 New York City Council, Int. 0909-2024 (2024) (as introduced), § 20-1272.1(c). *See also* Tung, Irene, et al. *'Just Cause' Job Protections*. National Employment Law Project, 2021; Tung, Irene, et al. *Fired Without Warning or Reason.* Data for Progress, Jan. 2023.

94 For a general inventory of these laws, *see* State and Local Laws Advancing Fair Work Schedules, Fact Sheet. National Women's Law Center, Sept. 2023.

95 *See, e.g.*, Harknett, Kristen, et al. *Seattle's Secure Scheduling Ordinance, Year 2 Worker Impact Report*. SHIFT Project, Feb. 2021, p. 16 (finding that Seattle fair scheduling ordinance provisions that required advance notice and extra pay to workers for last-minute scheduling changes led to greater scheduling predictability and stability).

96 Adler-Bell, *supra*. Gutelius, Beth. "Good Labor Policy Is Good Technology Policy." Roosevelt Institute, Feb. 2024, p. 3 ("Workplace technology is best dealt with by strengthening worker power across the economy.").

97 *See generally* Gilman, Michele. "Beyond Window Dressing: Public Participation for Marginalized Communities in the Datafied Society." 91 *Fordham Law Review* 503, 2022.

98 Center for Labor and a Just Economy, *supra*. *See generally* Gerstein, Terri. "How State and Local Government Can Support Workers' Rights to Join Unions." *NYU Wagner Labor Initiative*, 22 Apr. 2025.

99 *See, e.g., AI's Impact on Nursing and Health Care*, National Nurses United. Retrieved 2 Sept. 2025, from https://www.nationalnursesunited.org/artificial-intelligence; *Artificial Intelligence and Academic Professions.* American Association of University Professors, Jul. 2025.

100 Gilman, Michele. "Democratizing AI: Principles for Meaningful Public Participation." *Data & Society Research Institute*, Sept. 2023 (listing these and additional principles); Ballantyne, Amanda, et al. "A Vision for Centering Workers in Technology Development." *Issues in Science and Technology*, vol. XLI, no. 1, Fall 2024; Young, Meg, et al. "Gear Shift: Driving Change in Public Sector Technology through Community Input." *Data & Society Research Institute*, Jun. 2025. DOI: 10.69985/JPTW3751; "Take the Mic: How Worker Voice Shapes Workplace Technology." *Tech Equity*, Jul. 2025. *See also Guidance for Inclusive AI: Practicing Participatory Engagement.* Partnership on AI, May 2025.

101 Patel, Seema N., et al. "California Co-Enforcement Initiatives That Facilitate Worker Organizing." *Harvard Law & Policy Review: Labor Law Reform Symposium*, 2018.

102 *See generally* Brennan, Kate, et al. *Artificial Power: AI Now 2025 Landscape.* AI Now Institute, 3 Jun. 2025.

103 Cohen, Julie. "How (Not) to Write a Privacy Law." *Knight First Amendment Institute*, 23 Mar. 2021.

104 "U.S. Chamber Warns It Will Oppose Any Privacy Legislation That Creates a Blanket Private Right of Action." *US Chamber of Commerce*, 31 May 2022; Bordelon, Brendan. "Tech Lobbyists Are Running the Table on State Privacy Laws." *Politico*, 16 Aug. 2023; Smalley, Suzanne. "In Patchwork of State Privacy Legislation, Tech Lobby Sees a Single Battlefield." *The Record from Recorded Future News*, 30 Jan. 2024.

105 Wage and hour and workplace anti-discrimination laws typically contain a private right of action. Such private rights of action are crucial for workers' ability to enforce their rights, and are particularly so for workers in low-wage industries. *See, e.g.*, Ruan, Nantiya. "What's Left to Remedy Wage Theft?" 2012 *Michigan State Law Review* 1103, 2012, pp. 1115–1124. Similarly, private rights of action are standard in state consumer protection laws. "Consumer Protection Laws: 50-State Survey." *Justia,* Consumer Protection Laws: 50-State Survey, JUSTIA, Oct. 2023.

106 Henry Scholz, Lauren. "Private Rights of Action in Privacy Law." 63 *William and Mary Law Review* 1639, 2022, p. 1639.

107 Bloch-Wehba, Hannah. "The Promise and Perils of Tech Whistleblowing." 118 *Northwestern University Law Review* 1504, 2024, at pp. 1506–1510.

108 *Id.,* at pp. 1504–1505; Carole Cadwalladr. "I Made Steve Bannon's Psychological Warfare Tool." *Guardian*, 18 Mar. 2018 (describing Cambridge Analytica's harvesting of Facebook user data); Wells, Georgia, et al. "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show," *Wall Street Journal*, 14 Sept. 2021 (describing Instagram's effects on teen girls' mental health); Alecci, Scilla. "Uber Shifted Scrutiny to Drivers as It Dodged Tens of Millions in Taxes," *International Consortium of Investigative Journalists,* 11 Jul. 2022 (describing Uber's aggressive tax avoidance strategy in dealing with European authorities).

109 Bloch-Wehba, *supra*, at pp. 1506, 1553.

110 "At a Glance: Anti-Retaliation Legislation to Protect Workers and the Rule of Law." *Workplace Justice Lab at Rutgers University*, 1 Sept. 2022; Huizar, Laura. "Retaliation Funds: A New Tool to Tackle Wage Theft." *National Employment Law Project*, 21 Apr. 2021; "Fact Sheet: Adopt 'Just Cause' Job Protections Against Unfair Firings." *National Employment Law Project*, 11 Jul. 2024.

Data & Society is an independent nonprofit research and policy institute, studying the social implications of data-centric technologies and automation. We recognize that the same innovative technologies that may benefit society can also be abused to invade privacy, provide new tools of discrimination, foreclose opportunity and harm individuals and communities. We believe that technology policy must be grounded in empirical evidence, and serve the public.

www.datasociety.net

Layout by Gloria Mendoza

OCTOBER 2025