WHO'S GOT THE POWER ?

Restoring Worker Power in the Age of Algorithmic Unionbusting

epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

NATIONAL institute FOR WORKERS' RIGHTS

July 2026

About EPIC

The Electronic Privacy Information Center (EPIC) is a 501(c)(3) non-profit public interest research advocacy center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues.

Learn more at https://epic.org.

If you'd like to support EPIC's work, visit https://epic.org/support-epic/.

About NIWR

The National Institute for Workers' Rights (NIWR) is an advocacy organization focused on making it harder for employers to violate workers' rights and easier for workers to fight back. NIWR was founded by the National Employment Lawyers Association.

Learn more at https://niwr.org/.

If you'd like to support NIWR's work, visit https://niwr.org/support/.

Authors

Abby Frerick, NIWR Paul H. Tobias Attorney Fellow

Abigail Kunkler, EPIC Law Fellow

Mayu Tobin-Miyaji, EPIC Law Fellow

Acknowledgements

The authors would like to thank EPIC Counsel Kara Williams and Thomas McBrien, EPIC Senior Counsel Calli Schroeder, EPIC Deputy Director John Davisson, and NIWR Director Jason Solomon for their thoughtful feedback on this white paper. The authors also thank EPIC Policy and Communications Fellow Caroline Anders for designing this white paper, and EPIC IPIOP Clerks Karinna Gerhardt, Stephanie Forbes, and Naomi Bonilla Hoshikawa for their assistance, as well as Sarp Nalbantoğlu, CPSES Bingle Family and Priscilla Chan Summer Service Fellow at EPIC.

Table of Contents

Introduction

The U.S. labor movement is experiencing a renaissance driven by high-profile strikes, historic elections, and widespread popular support. Union approval is high across age, race, and political affiliation.[1] Nearly half of U.S. workers say that they would join a union—the most popular version of organizing—if given the chance,[2] and in 2025, unionization in the U.S. was at its highest levels since 2009.[3] Because of the breadth of activities that count as worker organizing, it is likely that this is underinclusive.[4] The popularity of worker organizing parallels research linking higher union density with better outcomes for individuals, communities, and even democracy, leading to improved conditions including higher wages and better benefits, reduced income inequality, and stronger voter protections.[5]

As workers organize, many employers are responding by incorporating new technologies that can undermine their efforts. Surveillance technologies, AI-powered algorithmic management, and large troves of worker data empower employers to tightly surveil workers' behavior and infer information about their organizing, lifestyle, and behaviors. This surveillance enables algorithmic unionbusting—the practice of using workplace technology to identify, coerce, or oust worker organizers. The practice can be hard to pin down. The consequences for workers are not.

---

[1] *In Solidarity: Removing Barriers to Union Organizing: Hearing Before the H. Comm. on Educ. & Lab.*, 117th Cong. (Sept. 14, 2022) (letter from Kate Bronfenbrenner, Cornell School of Industrial and Labor Relation).

[2] Frederick Reiber et al., *Surveillance, Spacing, Screaming and Scabbing: How Digital Technology Facilitates Union Busting*, Proceedings of the 2026 CHI Conf. on Hum. Factors in Computing Sys. 1 (2026).

[3] Margaret Poydock, Teke Wiggin, & Celine McNicholas, *U.S. Employers Spend More than $1.5 Billion Annually on Union Avoidance*, Econ. Pol'y Inst. 2 (May 20, 2026). We note, as well, that drops in union elections are not necessarily reflective of workers interest in organizing and may instead indicate strategic decisions to avoid elections under certain administrations.

[4] While unions are the most well-known form, worker organizing expands beyond unions. Concerted activity—the process through which workers work together to influence their pay and other workplace conditions—is protected under the National Labor Relations Act, whether or not it results in a union. National Labor Relations Act, 29 U.S.C. §§ 151–169. We note that concerted activity, the legal term of art used by the NLRA, goes by many names in colloquial discussion. Concerted activity, collective action, collective bargaining, and worker organizing, while having different boundaries, all refer to this general concept.

[5] *See generally* Celine McNicholas et al., *Unions Aren't Just Good for Workers—They Also Benefit Communities and Democracy*, Econ. Pol'y Inst. (Aug. 20, 2025).

Algorithmic unionbusting demonstrates the vital link between privacy rights and labor rights for protecting communities.[6] This whitepaper examines the ways that employers extract information from workers and weaponize it against worker organizing. We then situate the practice of algorithmic unionbusting within the failing framework of existing privacy and labor law before recommending changes policymakers at the state and federal level can make to restore worker power.

[6] *See* Brishen Rogers, *Data and Democracy at Work: Advanced Information Technologies, Labor Law, and the New Working Class* 81–103 (arguing that privacy and labor are linked by the protection of rights essential to strong community, namely association and speech).

I. Employers Are Increasingly Turning to Algorithmic Unionbusting.

Today, workers face ubiquitous surveillance and datafication throughout the employment relationship that may easily be used to attack workers' right to organize.[7] Employers' persistent and growing push to translate workers and their outputs into measurable data points has been an ongoing campaign for at least the past century.[8] The notion that an employer's economic interests are best advanced through the close monitoring of workers has come to be known as the "datafication" of workers and workplaces.[9] The modern workplace—and the vast amount of data collected about workers every day—is ripe for abuse by employers, who can easily turn data about workers against them to undermine their organizing efforts.[10]

Worker surveillance permeates all aspects of the worker's relationship with their employer. When a worker applies for an open position, employers marshal automated hiring systems outfitted with sentiment analysis and natural language processing to evaluate applicants.[11] Once on the job, workers are constantly monitored by surveillance cameras, sensors,[12] wearable technologies, engagement tools like keystroke loggers, and automated decisionmaking systems (ADS) that evaluate performance and automate consequential decisions about workers.[13] All the while, the suite of workplace surveillance tools collects

---

[7] *See generally* Aiha Nguyen, *The Constant Boss; Labor Under Digital Surveillance*, Data & Soc'y (May 19, 2021); Alexander Hertel-Fernandez, *Estimating the Prevalence of Automated Management and Surveillance Technologies at Work and Their Impact on Workers' Well-Being*, Equitable Growth (Oct. 1, 2024).

[8] Ifeoma Ajunwa, *Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law*, 63 St. Louis. U. L.J. 21, 23 (2018).

[9] Sam Adler-Bell & Michelle Miller, *The Datafication of Employment*, Century Found. (Dec. 19, 2018). *See also* Alexandra Mateescu, *Challenging Worker Datafication*, Data & Soc'y (Nov. 8, 2023).

[10] Letter from Serv. Emps. Int'l Union to Joel Christie, Acting Secretary, Fed. Trade Comm'n (Nov. 18, 2022).

[11] Ifeoma Ajunwa, The Quantified Worker 138–52 (2023).

[12] Letter from U.S. Chamber of Com. to Off. of Sci. and Tech. Pol'y (June 29, 2023).

[13] *See* EPIC, *Assessing the Assessments: Maximizing the Effectiveness of Algorithmic & Privacy Risk Assessments 10* (June 25, 2025); Wilneida Negrón, *Move Algorithmic-Driven Pay and Scheduling Systems From Surveillance Pay to Fair Wages*, Fed. of Am. Scientists (June 11, 2026); Miranda Bogen & Aaron Rieke, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, Upturn (Dec. 2018)

or infers staggering amounts of information about workers. How a worker performs their job, their location and movements (on and off the clock),[14] their communications with colleagues, biometric information,[15] and even emotion and sentiment[16] are carefully tracked and logged. Performance monitoring systems seek to standardize work into discrete, quantifiable tasks, imposing frequently arbitrary rules[17] on what actions or behaviors lead to compensation or discipline and undermining worker autonomy.[18]

While employers furnish various justifications for workplace surveillance, such as workplace safety and security, anti-theft measures, customer satisfaction, accurate accounting of performance, and preventing worker turnover, workplace surveillance is easily weaponized by employers against workers engaged in unionization campaigns. In a paper analyzing counter-organizing tactics used by employers, the authors identified four categories of tactics: surveillance, spacing, screaming, and scabbing.[19] We adopt this framework here to demonstrate algorithmic unionbusting.

Employers use surveillance to monitor behavior, track activities and communications, and infer and predict the behavior or personal traits of employees.[20] The workplace technologies already in use make this possible.

---

[14] Betsy Stark, *Companies Tracking Employees' Every Move*, ABC News (Jan. 4, 2001); Ceylan Yeginsu, *If Workers Slack Off, the Wristband Will Know. (And Amazon Has a Patent For It.)*, N.Y. Times (Feb. 1, 2018); Lauren Kaori Gurley, *Internal Documents Show Amazon's Dystopian System for Tracking Workers Every Minute of Their Shifts*, Vice (June 2, 2022); Ajunwa, *supra* note 8, at 26.

[15] Ajunwa, *supra* note 8, at 34–49; Tatyana Woodall, *Big Meat Companies Want to Use Smartwatches to Track Workers' Every Move*, Vice (Nov. 2, 2022).

[16] Nguyen, *supra* note 7 at 13; Josh Dzieza, *How Hard Will the Robots Make Us Work?*, The Verge (Feb. 27, 2020); Khari Johnson, *Kaiser Permanente Nurses Say Technology is Making Their Jobs—and Patient Care—Worse*, The Markup (July 9, 2026); Emma Roth, *Burger King Will Use AI to Check if Employees Say 'Please' and 'Thank You',* The Verge (Feb. 26, 2026); Lauren Kaori Gurley, *Internal Slacks Show HelloFresh is Controlling Talk of Unionization*, Vice (Nov. 19, 2021).

[17] Cella M. Sum, Caroline Shi & Sarah E. Fox, *"It's Always a Losing Game": How Workers Understand and Resist Surveillance Technologies on the Job*, Proc. ACM Hum.-Comput. Interaction 11–13 (2025); Johnson, *supra note* 16.

[18] Nguyen, *supra* note 7, at 8; Sum, Shi & Fox, *supra note* 17, at 11 (some workers reported that the monitoring systems penalized them for quick water breaks, describing the system as "psychological manipulation."); Jodi Kantor & Arya Sundaram, *The Rise of the Worker Productivity Score*, N.Y. Times (Aug. 14, 2022); Hertel-Fernandez, *supra note* 7.

[19] Reiber et al., *supra* note 2.

[20] *Id*. at § 4; In Solidarity: Removing Barriers to Union Organizing: Hearing Before the H. Comm. on Educ. & Lab., *supra* note 1, at 11–12.

For instance, HelloFresh was reportedly tracking social media posts related to its workers' unionization campaign and reporting them as spam.[21] In another example, Amazon-owned Whole Foods was reported to be tracking likelihood of unionization campaigns in their stores through a heat map using more than two dozen metrics, including employee "loyalty," turnover, and racial diversity; "tipline" calls to human resources; proximity to a union office; and violations recorded by the Occupational Safety and Health Administration.[22]

Spacing refers to employers using workplace technology and policies or rules to hinder communication and trust between workers.[23] Employers may do this through use of security cameras and management software to physically space out workers, isolating them in their work stations, or weaponizing scheduling software to shift pro-union employees to different locations.[24] Employers may also limit digital communication between workers by creating communication silos between different parts of the business or prohibiting discussion of topics such as union campaigns.[25]

Surveillance and spacing are mutually enforcing tactics. Monitoring worker behavior throughout their shifts inevitably discourages workers from interacting with each other outside of strictly necessary interactions, chilling worker conversations and diminishing the trust necessary for collective organizing.[26] Even if there is no direct spacing separating workers physically or digitally, workplace technologies may interfere with collective organizing by pitting workers against one another, intensifying work, and creating a culture of fear through surveillance. Combined, these tactics create a chilling effect. For example, some employers turn workers against one another through competitive performance metrics. A

[21] Gurley, *supra* note 14.
[22] Reiber et al., *supra* note 2, at § 4. *See also H&M Fined for Breaking GDPR Over Employee Surveillance, BBC* (Oct. 5, 2020); Annie Palmer, *How Amazon Keeps a Close Eye on Employee Activism to Head Off Unions*, CNBC (Oct. 24, 2020).
[23] Reiber et al., *supra* note 2, at § 4.
[24] *Id*.
[25] *Id*.; Ken Klippenstein, *Leaked: New Amazon Worker Chat App Would Ban Words Like "Union," "Restrooms," "Pay Raise," and "Plantation",* The Intercept (Apr. 4, 2022), (Amazon was reportedly considering automated system that would flag and automatically block employees from sending a message based on keywords, which included many relevant to organized labor, including "union," "grievance," "pay raise," and "compensation.").
[26] Gurley, *supra* note 14.

worker interested in unionizing may be discouraged to organize because they fear detection through surveillance and the prospect of retaliation.[27]

While screaming and scabbing have less direct privacy harms, workplace technology aids employers to engage in both of these tactics as well. Screaming refers to employers pushing anti-union messaging through means of communication required for work, such as emails, internal messaging platforms, or mobile apps required for scheduling and clocking in and out.[28] Such messaging through communications platforms that workers are required to check creates a digital captive audience where employers can overwhelm workers with anti-union messaging at any time, during work hours or outside of them.[29] Scabbing, the use of technologies to facilitate the replacement of union labor, is made easier by workplaces mediated by ADS that automate finding and interviewing candidates and training, scheduling, and assigning tasks to replacement workers.[30]

The wide latitude employers enjoy to collect worker data and deploy workplace technologies[31] has allowed employers to abuse such systems to detect, preempt, and interfere with workplace organizing. As workplace surveillance technologies and AI systems become more affordable and accessible, employers have introduced more intrusive forms of surveillance, including an assemblage of networked devices to continuously collect granular data about workers.[32] In fact, surveys of union organizers have found that employer use of electronic worker surveillance during union elections more than doubled between 1999 and 2021, rising from 14 percent to 32 percent of all elections.[33] Workers seeking to organize in today's workplaces thus must contend with employers who have every incentive—and dozens of technologies—to surveil workers as closely as possible.

---

[27] Indeed, retaliation has never been easier for employers to justify as it is in an algorithmically managed workplace, where employers can simply check their monitoring systems for perceived infractions that may mask retaliation.
[28] Reiber et al., *supra* note 2, at § 4.1.3.
[29] *Id*.
[30] *Id*.
[31] See, e.g., Rogers, *supra* note 6, at 60–63.
[32] Sum, Shi & Fox, *supra* note 17, at 3.
[33] *In Solidarity: Removing Barriers to Union Organizing: Hearing Before the H. Comm. on Educ. & Lab.*, *supra* note 1, at 11–12.

II. The Union Avoidance Industry Weaponizes Worker Data.

When feeling threatened by possible worker organization efforts, employers frequently turn to union avoidance consultants, also known as labor persuaders or union busters.[34] In 2022, the Cornell School of Industrial and Labor Relation found that employers opposing unionization hired third-party consultants in nearly three out of four elections.[35] In the United States alone, employers spend roughly $1.7 billion a year on union avoidance consultants and law firms to keep their workers from organizing.[36]

Like employers, union avoidance consultants use worker information to target organizing efforts.[37] In 2021, IRI Consultants[38] gathered immensely personal details about hospital employees and their social and financial positions.[39] This included information on a worker's personality, temperament, motivations, ethnicity, family background, spouse's employment, finances, health data, work ethic, job performance, disciplinary history, and involvement in union activity.[40] This information was used to score workers on their likelihood to organize or vote for unionization.[41] This same information could be used to target workers that the consultant believes are easy to persuade against unionizing due to their financial or social positions, opening up workers to increased privacy violations, manipulation, or intimidation.

IRI is far from the only consultant utilizing data analytics to disrupt organizing. The notorious anti-union law firm Littler Mendelson has been vocal about its interest in turning data against workers to predict and stamp out unionizing.[42] Indeed, the

---

[34] *Id*. at 9–10.
[35] *Id*.
[36] Margaret Poydock, Teke Wiggin & Celine McNicholas, *U.S. employers spend more than $1.5 billion annually on union avoidance*, Econ. Pol'y Inst. (May 20, 2026).
[37] See, e.g., Sarah Kessler, *Companies are Using Employee Survey Data to Predict—and Squash—Union Organizing*, OneZero, Medium (July 30, 2020); Susanna Vogel, *How Companies Use Predictive Analytics to Get Ahead of Union Drives*, HR Brew (Nov. 3, 2021).
[38] IRI Consultants appears to have rebranded to People Results. When you visit IRI's website, it redirects to peopleresults.com.
[39] Lauren Kaori Gurley, *'Lazy,' 'Money-Oriented,' 'Single Mother': How Union-Busting Firms Compile Dossiers on Employees*, Vice (Jan. 5, 2021).
[40] *Id*.
[41] *Id*.
[42] *See* Kessler, *supra note* 37; Jarod Facundo, *Lawyers, Not Persuaders*, The Am. Prospect (Oct. 5, 2023).

firm has used data-driven union vulnerability heat maps and anti-union computer monitoring software in this pursuit.[43] Another employer-side law firm, Jackson Lewis, similarly touts its data analytics group and its “data-driven decisions.”[44] While much of the information analyzed comes from the employers themselves, it also comes from public sources like social media and, very likely, data brokers.[45]

Despite the prevalence of these third-party union avoidance consultants, employers have a strong incentive to ditch them or, at least, to offset their cost. Notably, LaborLab and the Economic Policy Institute have estimated that employers across the U.S. spend an incredible $1.7 billion annually on third-party avoidance consultants.[46] In one recent example, Iowa hospital UnityPoint spent between $20,600 and $34,000 on consultants *every day* when faced with demands for more staff and better safety measures from overloaded and imperiled hospital staff.[47] With such a high price tag, employers are increasingly incentivized to repurpose the worker data they already hold to offset the time and cost of third-party consultants.

The union avoidance industry knows this. Companies like Perceptyx have taken old union-buster methods, including union vulnerability audits that evaluate the likelihood that a workplace or group is “at risk” of unionizing, and created proprietary software products to replicate and supplement these methods

[43] John Logan, *Not Your Father’s Anti-Union Movement: Ten Key Facts About Starbucks’ Union Avoidance Law Firm, Littler Mendelson, Labor and Working-Class History Association* (Mar. 7, 2022).

[44] Kessler, *supra* note 37 (preserving JacksonLewis’ webpage stating that it “leverages employers’ rich workforce datasets to enable effective data-driven decisions for workforce-related issues. . .”).

[45] Although there is no definitive connection between union avoidance consultants and data brokers, data brokers collect vast amounts of data about individuals including their financial status, lifestyle, health information or political affiliation, to inform their union avoidance strategy, allowing employers and union avoidance consultants to easily purchase such data about workers. Further, employers do purchase information from data brokers for a variety of purposes, including background checks. Notably, data broker registries maintained by California and Texas shows that many data brokers sell information on union activity. For more information about data brokers, *see Data Brokers*, EPIC.org.

[46] See Poydock, Wiggin, & McNicholas, *supra* note 36.

[47] Emma Janssen, *Nurses in Iowa Are Fighting an Unprecedented Anti-Union Campaign*, The Am. Prospect (Sept. 22, 2025). LaborLab has filed complaints with the Department of Labor against several consultants involved in the UnityPoint campaign for failing to adequately report their involvement, including attorneys at Littler Mendelson. *See Watchdog Files Complaint Against UnityPoint’s Union-Busting Campaign as Nurses Fight for Patient Safety*, LaborLab (Sept. 8, 2025).

at a lower cost. Now frequently branded as “employee listening” or “people analytics,” tools like those made by Perceptyx use AI “listening agents” and compile employee survey data, sales data, financial metrics, ethnicity, productivity information, and “internal research” to predict locations, teams, and individuals that are more likely to organize.[48] Another example is HireRight, a company that developed a product to predict the likelihood that a job applicant would be a whistleblower by mining social media.[49] Existing consultants are getting in on the game as well. For example, Littler Mendelson has developed Littler OnDemand, a platform that Littler’s clients can use to perform data analytics and receive predictions and recommendations.[50]

Consultant activity is shrouded from the view of workers and the public. As discussed further in Section IV of this whitepaper, union avoidance consultants are required to submit publicly available reports when they are hired to obstruct unionization, including through surveillance.[51] Unfortunately, that requirement has large carveouts for consultants who render “advice” to companies but do not have direct contact with workers.[52] Most consultants operate within this loophole.[53] Delaying or denying transparency is a key tactic for obstructing organizers and enforcers.

[48] Kessler, *supra* note 37; Bradley Wilson, *Influence the Future with Predictive Analytics in HR*, Perceptyx (May 8, 2019).
[49] Annette Bernhardt, Lisa Kresge & Reem Suleiman, *The Data-Driven Workplace and the Case for Worker Technology Rights*, 76 ILR Rev. 3, 12 (2023).
[50] Littler, *Littler onDemand*.
[51] Office of Labor-Management Standards, *Employer and Consultant Reporting*, Dep’t Lab. (July 3, 2025).
[52] 29 U.S.C. § 433(c).
[53] Econ. Pol’y Inst. & LaborLab, *Busting the Union Busters: The Need to Improve Transparency Around Union-busting Activity*, 3–4 (Nov. 13, 2024).

III. Algorithmic unionbusting chills worker organizing, hinders enforcement, and harms workers.

The surveillance that powers algorithmic unionbusting is categorically different than the surveillance faced by workers at the time workers' rights were enshrined by law in the U.S. What used to be a man with binoculars is now an interconnected network of entities, data, and mass-market algorithmic tools. Increasingly, these tools utilize machine learning or other forms of AI-enabled data analysis to easily derive insights. More information, more kinds of information, and more granular information is taken in, processed, generated, bought, and sold than ever before.[54] The National Labor Relations Act of 1935 (NLRA) was created to deal with individual instances of problematic employer practices, not networked surveillance. And as the surveillance industry increasingly turns toward making inferences about individuals from pools of consolidated and analyzed information,[55] technology skirts any privacy protections for consumer data by porting it into the underregulated workplace as data about workers, taking advantage of the false separation between worker and consumer. In and out of the workplace, legal doctrine is failing to defend against pernicious, continuous, and granular datafication. Like the broader union avoidance industry, algorithmic unionbusting thrives in the loopholes.

Within the permissive bounds of existing law,[56] employers are now incentivized to surveil workers as much as possible and collect as much information as possible from workers, workplaces, data brokers, algorithmically generated inferences, and other sources. As a result, more than two-thirds of U.S. workers (disproportionately workers of color) are now subjected to at least one form of electronic monitoring.[57] Workers rarely have the means to avoid it.[58] Under the pervasive regime of

---

[54] Julie E. Cohen, *How (Not) to Write a Privacy Law*, Knight First Amend. Inst. at Colum. U. (Mar. 23, 2021); Sum, Shi & Fox, *supra* note 17 at 3.

[55] *See generally* Minsu Longiaru et al., *The "Privacy" Trap: How "Privacy-Preserving AI Techniques" Mask the New Worker Surveillance and Datafication*, Data & Soc'y (June 2026); Rogers, supra note 6, at 57–80.

[56] *See* Section IV, *infra*.

[57] Alexander Hertel-Fernandez, *How Union Contracts Are Protecting U.S. Workers from Automated Management and Surveillance in the Workplace*, Wash. Ctr. For Equitable Growth (Mar. 12, 2026).

[58] Reiber et al., *supra* note 2, at § 6.1.1 (arguing that digital technologies embed unionbusting within the labor process).

employment-at-will, employers may penalize or dismiss workers for even trying to protect themselves from constant surveillance. Indeed, consent to surveillance was likely a condition of the worker's employment.

Perhaps by now obvious, algorithmic unionbusting works to chill worker organizing. Simply put, workers, often in precarious positions, fear retaliation for speaking out about their working conditions. Algorithmic unionbusting makes it easy for employers to dig through data to find any small infraction they may weaponize against organizers. Further, algorithmic unionbusting chills organizing by siloing workers with monitoring, warnings, intensified work, and trackers. Algorithmic unionbusting makes it dangerous or impossible to form the trust and community identity that successful organizing campaigns require.[59]

If workers do manage to overcome the chilling effect, algorithmic unionbusting continues to undermine their positions during the campaign and at the bargaining table.[60] The scale and scope of information that employers, consultants, and software companies may access allows for unprecedented insights into workers' lives. The information asymmetry gives employers incredible power to identify, predict, and exploit pressure points individual workers may have in an attempt to break ranks or morale and drive down bargaining over key issues like wages. Further, algorithmic unionbusting turns nuanced jobs into quantified tasks, increasing the ability for employers to seek cheaper labor elsewhere[61] and weakening the value of workers' expertise.

Unionization is an essential pathway for workers to reject unreasonable workplace technology and negotiate strong guardrails around what remains.[62] To empower workers' voices, we must shut down algorithmic unionbusting.

[59] *See* Rogers, *supra* note 6, at 81–103.
[60] This is true both for first and future contracts.
[61] *See* Brishen Rogers, The Law and Political Economy of Workplace Technological Change, 55 Harv. Civ. Rights-Civ. Lib. L. Rev. 531, 562–573 (2020).
[62] Lisa Kresge, *Negotiating Tech: An Inventory of U.S. Union Contract Provisions for the Digital Age*, U.C. Berkeley Lab. Ctr. (2026).

IV. Existing Law Isn't Meeting the Demands of Algorithmic Unionbusting.

Our existing legal framework cannot effectively safeguard against algorithmic unionbusting. The National Labor Relations Act of 1935, designed for the more limited surveillance that existed at its inception and made weaker over time, cannot adequately protect worker organizing from the perils of algorithmic unionbusting. Attempts to impose oversight on the union avoidance industry have failed to provide adequate transparency into the ways the industry invades worker privacy. Similarly, existing privacy protections largely exclude workers or provide narrow protections that cannot adequately defend the right to organize against the misuse and abuse of data that is now commonplace.

A. Federal Labor Laws Do Not Adequately Guard Against Algorithmic Unionbusting.

1. The National Labor Relations Act

The National Labor Relations Act (NLRA) gives private sector workers the right to act together to improve their wages and working conditions, whether or not they belong to a union.[63] Section 7 of the NLRA covers organizing, bargaining, and any other concerted activity undertaken for mutual aid or protection.[64] This Section of the NLRA is broad by design; it extends coverage to informal worker conversations and collective action that occur outside of any union campaign. This means the protection attaches the moment workers begin talking to each other about their conditions of employment—two warehouse workers talking about their pay and retail workers using a group chat to discuss a scheduling policy are all protected.[65] The NLRA is enforced by the National Labor Relations Board (the Board).[66] As discussed below, however, the Board's surveillance doctrine was designed for an earlier generation of union-busting tactics, leaving significant gaps that employers now exploit through data-driven (and often covert) monitoring and prediction tools.

[63] 29 U.S.C. § 157.

[64] While the Act's coverage is broad, it does not cover all workers. Agricultural workers, domestic workers, independent contractors, and supervisors are excluded. 29 U.S.C. § 152(3).

[65] *Id*. § 153.

[66] 29 U.S.C. § 153. See also National Institute for Workers' Rights, *The Right to Talk to Co-Workers and Management About Working Conditions: A Study of Enforcement at the NLRB* 8 (2024) (providing examples of the right to "engage in other concerted activities" for "mutual aid or protection.").

According to the NLRA, it is an unfair labor practice for an employer to interfere with, restrain, or coerce workers in the exercise of their protected activity, and violations are referred to as unfair labor practices.[67] However, the text of Section 7 does not address workers' privacy nor employer surveillance explicitly, and doctrine around the concept has developed over time in ways that are often unhelpful to workers. For example, the NLRB only finds that surveillance was an unfair labor practice if it was more than an employer happening to see concerted activity taking place.[68]

Data shows that employer surveillance during union election campaigns increased from 14% to 32% from 1999 to 2021, and to 36% when the employer mounted an anti-union campaign.[69] Examples of surveillance that the NLRB has held to violate the NLRA include management watching workers with binoculars, observing union activity on a daily basis for hours at a time, posting guards in previously unguarded areas, photographing workers in response to union activity, and starting a new practice of sitting with workers during breaks during an ongoing campaign.[70]

Employer surveillance violates the NLRA when it is out of the ordinary in a way that would tend to interfere with, restrain, or coerce workers' concerted activity.[71] An employer can also violate the law by creating the impression that protected activity is under surveillance, even when no actual monitoring occurred.[72] However, this doctrine is constrained significantly by its permissive approach to existing and overt surveillance. Employers may continue practices adopted before workers began to engage in concerted activity, even if those practices

---

[67] *Id*. § 158(a).

[68] Charlotte Garden, *Labor Organizing in the Age of Surveillance*, 63 St. Louis U. L.J. 55, 62 (2018).

[69] *See In Solidarity: Removing Barriers to Union Organizing: Hearing Before the H. Comm. on Educ. & Lab.*, *supra* note 1, at 11–12.

[70] Garden, *supra* note 68, at 61 (citing Cook Family Foods, Ltd., 311 N.L.R.B. 1299, 1301 (1993); NLRB v. Collins & Aikman Corp., 146 F.2d 454, 455 (4th Cir. 1944); S.J.P.R., Inc., 306 N.L.R.B. 172, 189 (1992); Aladdin Gaming, 345 N.L.R.B. 585, 586–87 (2005)). *See also* Starbucks Corp., 374 N.L.R.B. 10, 11 (2024).

[71] 29 U.S.C. § 158(a)(1); Metal Industries Inc., 251 N.L.R.B. 1523, 1523 (1980) (affirming that routine or casual observation of workplace activity does not rise to the level of unlawful surveillance).

[72] Flexsteel Industries, Inc., 311 N.L.R.B. 257, 257–58 (1993); Garden, *supra* note 68, at 63 (citing Cal. Acrylic Indus., 322 N.L.R.B. 41, 59 (1996) ("[W]hether a video tape was actually in Saldana's video camera or whether he actually pressed down on the record button … the 'chilling effect' of such on Respondent's employees' Section 7 rights was the same.")).

later allow the employer to observe the activity.[73] This means employers may implement surveillance technology for purposes like promoting productivity or maintaining security without those tools being automatically unlawful. However, an employer who uses tools like a pre-existing security camera system or email monitoring software cannot then direct those systems specifically to target workers engaged in protected activity. Even so, this doctrine incentivizes early and invasive workplace surveillance.

Because the Board does not generally find obvious or pre-existing surveillance problematic, workers run into proof problems when enforcing their rights. When an employer takes adverse action against a worker for engaging in protected activity, such as termination, schedule changes, or quota increases, workers have to show that protected activity occurred, that the employer knew about it, and that the employer's response was motivated in part by hostility toward that activity.[74] Once those elements are established, the employer must show that it would have taken the same action regardless of the worker's activity.[75]

Yet covert surveillance creates compounding proof problems for workers. They do not know they have been surveilled, nor what data has been collected about them. Federal laws do not require that employers disclose their surveillance to workers. These proof problems compound further where the automated tool itself, rather than an individual manager's discretionary use of it, is calibrated in a way that tends to suppress protected activity. Imagine, for example, that a scheduling or productivity algorithm happens to penalize the informal conversations and shift overlaps through which organizing typically occurs. As the design choices behind these systems are opaque and rarely, if ever, subject to any external audit, a worker would face the difficult task of proving not just that they were targeted, but that the tool itself was shaped in a way that structurally disadvantages protected activity.

Board law around algorithmic performance management is underdeveloped. ADSs that track performance against quotas or compliance metrics generate a continuous stream of seemingly neutral, data-backed justifications an employer can invoke when it wants to discipline a particular worker. Existing precedent would suggest that using such tools selectively against workers engaged in protected activity is unlawful. But because these systems flag technical rule

[73] Garden, *supra* note 68, at 62.
[74] 29 U.S.C. § 158(a); Wright Line, 251 N.L.R.B. 1083, 1083 (1980).
[75] Wright Line, 251 N.L.R.B. 1083, 1083 (1980).

violations or quota shortfalls that many workers will commit at some point, they hand employers a legitimate-sounding rationale to single out an organizer while leaving the underlying motive obscured. This dynamic makes the discriminatory use of a facially neutral tool difficult for workers to uncover and even harder to prove.

The Biden-era General Counsel's office at the Board proposed a framework in October 2022 that would have addressed this opacity directly.[76] The General Counsel urged the Board to find that electronic monitoring and algorithmic management practices that interfere with Section 7 rights would be presumptively unlawful, with employers required to justify them by demonstrating a legitimate business need that cannot be met through less intrusive means.[77] Ultimately, that memorandum was withdrawn in February 2025 following the inauguration of President Trump.

2. The Labor-Management Reporting and Disclosure Act

In 1959, Congress sought to mandate transparency in the organizing process with the Labor-Management Reporting and Disclosure Act (LMRDA).[78] Under the LMRDA, employers and union avoidance consultants are required to create reports when they contract to persuade employees on whether and how to exercise their right to organize. These reports, known as "persuader reports," are filed with the Office of Labor-Management Standards (OLMS), an office of the Department of Labor, and made available to the public. Of particular interest to this white paper, the LMRDA requires consultants and employers to detail their surveillance activities in their reports.

However, many companies and consultants avoid reporting by exploiting the carveouts for consultants acting as attorneys[79] for or rendering "advice" to the employer.[80] In fact, the Department of Labor has estimated that closing the advice loophole would mean that consultant reports would increase tenfold,

[76] Memorandum GC 23-02 from Jennifer A. Abruzzo, General Counsel, NLRB, *Electronic Monitoring and Algorithmic Management of Employees Interfering with the Exercise of Section 7 Rights* 6–8 (Oct. 31, 2022).
[77] *Id*.
[78] 29 U.S.C. §§ 431 et seq.
[79] *Id*.. § 434.
[80] *Id*. § 433(c). *See* Econ. Pol'y Inst. & LaborLab, *supra* note 53, at 3–4.

and employer reports would double.[81] While the OLMS has worked to improve reporting in recent years,[82] compliance is low. Even those who must report regularly fail to do so.[83] Of those who do, reports are delayed, meager, and unhelpful.[84] The disregard for reporting is incentivized by the lack of financial penalties and lackluster enforcement.[85] In the end, exploitable loopholes and toothless enforcement leave workers in the dark and widen information and power asymmetries between workers and employers.

B. State and Federal Privacy Laws Often Fail to Protect Worker Privacy.

Privacy laws today are wholly insufficient to protect the rights of workers to engage in concerted activity. The United States has no federal comprehensive privacy law, let alone one that includes workers within its protections. The narrow federal privacy laws that do apply to workers, including the Electronic Communications Privacy Act and Stored Communications Act, have become outdated and defanged over time in the workplace context. Across the country, however, some states have adopted privacy laws to counter this federal gap, ranging from "comprehensive" privacy laws to sector- or data-specific laws. While this section will not exhaustively review all state laws that may be characterized as privacy laws, our survey of major state privacy laws clearly shows that worker interests are most often excluded entirely from such laws.

1. The Electronic Communications Privacy Act and the Stored Communications Act

Enacted in 1986, the federal Electronic Communications Privacy Act (ECPA)[86] offer some privacy protections for worker communications, including protections for stored communications and data.[87] Title I of ECPA prohibits any person from

[81] Interpretation of the "Advice" Exemption in Section 203(c) of the Labor-Management Reporting and Disclosure Act, 81 Fed. Reg. 15929 (Mar. 24, 2016). OLMS estimated that the number of employer LM-10 reports would increase to 2,777 from 957, and the number of LM-20 reports would increase to 4,194 from 387.
[82] *See* Econ. Pol'y Inst. & LaborLab, *supra* note 53, at 6.
[83] *Id*. at 4–5.
[84] *Id*.
[85] *Id*. See also Reed Shaw & Will Dobbs-Allsopp, *Ending Special Treatment for Union Busters*, OnLabor (Nov. 8, 2023).
[86] Pub. L. 99-508, 100 Stat. 1848 (codified as amended in various sections of 18 U.S.C.).
[87] *See* EPIC, *Electronic Communications Privacy Act (ECPA)* (2026).

using an electronic device to intentionally intercept the wire, oral, or electronic communications of another person while that communication is in transit.[88]

Title II of ECPA, commonly referred to as the Stored Communications Act (SCA), prohibits a person from accessing communications that are stored remotely by a provider without (or in excess of) authorization.[89] The law also prohibits providers from disclosing the stored communications of their customers without consent or other specific legal authorization. These laws, in general, prohibit employers from gaining access to a worker's private conversations and emails without their consent. However, when employers act as the provider of communications (e.g. by hosting e-mail or chat services or providing phone lines) or when they have contractual authorization to access that data (e.g. as specified in an employment contract) a worker's privacy rights can be limited. ECPA and the SCA are commonly implicated in criminal investigations but often provide little relief to workers facing surveillance by their employer.

Workers must overcome several hurdles when challenging surveillance under ECPA. First, a worker must show that the employer intercepted their communications while they were happening.[90] For example, an employer cannot record worker conversations with a hidden tape recorder under ECPA.[91] Second, ECPA only applies to a narrow band of surveillance, excluding common methods like video-only surveillance (i.e. recordings without audio).[92] It also only prohibits employers from intentionally intercepting communications, incentivizing passive and continuous workplace surveillance.[93]

Further, employers can skirt ECPA's protections on worker communications by taking advantage of two exceptions. First, employers can utilize worker consent.

---

[88] 18 U.S.C. § 2511(1).
[89] *Id*. § 2701(a); United States v. Councilman, 418 F.3d 67, 81 (1st Cir. 2005).
[90] Boudreau v. Lussier, 901 F.3d 65, 78 (1st Cir. 2018).
[91] *Walston v. United Parcel Serv., Inc.,* No. 2:07-CV-525 TS, 2008 WL 5191710, at *2 (D. Utah Dec. 10, 2008).
[92] *Williams v. City of Tulsa*, 393 F. Supp. 2d 1124, 1132 (N.D. Okla. 2005) ("The Act does not prohibit silent video surveillance, only interception of communication.").
[93] *Mousavi v. John Christner Trucking, LLC*, 487 F. Supp. 3d 1194, 1201 (N.D. Okla. 2020); *Sunbelt Rentals, Inc. v. Victo*r, 43 F. Supp. 3d 1026, 1030–31 (N.D. Cal. 2014).

ECPA will not apply to surveillance if the worker knowingly[94] and expressly[95] consented to the surveillance. Even so, express consent is not necessarily required. Courts will imply it if the worker is aware of a general monitoring program and uses a monitored work device for non-work reasons.[96] Second, employers that control the means of communication may still listen in on wire eavesdropping when doing so in the "ordinary course of business."[97] This means that employers may monitor calls to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not (if the call is personal, they may not continue intercepting once the personal nature is determined).[98] However, it is unclear whether workers' communications about engaging in concerted activity would clearly fall under a "personal" or "business" call.[99]

Given all of this, employers are incentivized to notify workers that work devices are monitored and gather workers' written consent to the monitoring. By taking these simple steps and implementing policies limiting the use of workplace devices to workplace communications, employers can sidestep the privacy protections created by ECPA. In addition, as described earlier, employers offer various legitimate business interests to maintain systems that surveil workers, such as maintaining safety and security of the workplace, assessing worker performance, or preventing theft, which creates barriers for challenging continuous surveillance. Unless employers are intercepting communications

[94] *Anderson v. City of Columbus,* 374 F. Supp. 2d 1240, 1250 (M.D. Ga. 2005).
[95] Generally, courts will not find implied consent. *See Watkins v. L.M. Berry & Co*., 704 F. 2d 577 (11th Cir. 1983) (knowledge of the capability of monitoring alone will not substitute for actual consent); *Anderson*, 374 F. Supp. 2d at 1250. Further, courts closely scrutinize notices given to workers about the nature of the monitoring. *Dukes v. ADS All. Data Sys., Inc.*, No. 2:03-CV-00784, 2006 WL 3366308, at *12–13 (S.D. Ohio Nov. 20, 2006).
[96] *See Simmons v. Southwestern Bell Tel. Co.*, 452 F. Supp. 392 (W.D. Okla. 1978), aff'd, 611 F 2d 342 (10th Cir. 1979) (consent will be implied where the employee is aware of a general monitoring program and uses a business-only phone to make a personal call when other phones are provided for that purpose).
[97] *Anderson*, 374 F. Supp. 2d at 1250 (an employer may not, in the ordinary course of business, surreptitiously intercept everything an employee says while at his desk).
[98] *Ali v. Douglas Cable Commc'ns*, 929 F. Supp. 1362, 1380 (D. Kan. 1996); *Smith v. Devers*, No. CIV.A. 01-T-551-N, 2002 WL 75803, at *3 (M.D. Ala. Jan. 17, 2002) ("It is quite apparent that the complete interception of personal phone calls of an employee is not and can never be protected behavior under the business-extension exemption.").
[99] *See*, e.g., *Hay v. Burns Cascade Co.*, No. 5:06-CV-0137 NAM/DEP, 2009 WL 414117, at *15 (N.D.N.Y. Feb. 18, 2009).

done clearly outside of the work setting through workers' personal devices, ECPA offers little for workers seeking to challenge employer surveillance.

The SCA offers little more than ECPA to workers seeking to challenge workplace surveillance. The SCA prohibits employers from intentionally accessing workers' stored communications without permission.[100] But the scope of protection provided by the SCA is subject to debate over many of the statutory terms dating back to the 1980s, including what constitutes "electronic storage."[101] Employers also typically control the means of storing communications. For this reason, courts generally allow employers to access them. Thus, unless employers are accessing workers' personal accounts protected by passwords, the SCA offers little protection to workers, cementing the ubiquitous control that employers enjoy over workplace surveillance and the resulting data.

2. The Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) was enacted in 1970 to promote the accuracy, fairness, and privacy of personal information assembled by credit reporting agencies (CRAs) that assemble consumer reports on individuals for sale to companies, including employers.[102] FCRA, which includes workers in its definition of consumer,[103] operates on a hybrid enforcement model. While the Consumer Financial Protection Bureau (CFPB) creates regulations to implement FCRA's protections and shares public authority with the Federal Trade Commission and state Attorneys General to enforce FCRA, individuals may also enforce their rights under FCRA by filing civil actions in court, including their right to know when employers use their consumer information in employment decisions and to obtain a copy of the report the employer purchased.

For the purposes of FCRA, consumer reports are defined broadly to include "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purposes of serving as a factor in establishing the consumer's eligibility for"

100 18 U.S.C. § 2701(a).
101 *Id*. § 2510(17). See Rigby v. Longleaf Machining, LLC, No. CV 1:24-CV-88-TFM-M, 2026 WL 1228464, at *7 (S.D. Ala. May 4, 2026).
102 15 U.S.C. §§ 1681 et seq. See also EPIC, *The Fair Credit Reporting Act (FCRA)*.
103 Indeed, FCRA simply defines a "consumer" as "an individual." 15 U.S.C. § 1681a(c).

purposes that include employment.[104] Background dossiers that are compiled from public records, employment records, collective-bargaining activity, or other information about a worker are considered consumer reports under FCRA.[105]

Employers often purchase consumer reports to use when making employment decisions about workers, including viewing an applicant's criminal background before hiring and investigating a worker's compliance with workplace policies.[106] Increasingly, CRAs offer a range of reports to employers that may include information on workers' activities, attributes, productivity, and more.[107] Employers may purchase this information from CRAs and use this information to make prediction related to worker behavior. Although the NLRA prohibits employers from discriminating based on previous union activity or sympathies, CRAs do offer information on individuals' union organizing activity, which could factor into employers' predictions.[108]

FCRA constrains employers' use of credit reports by mandating that these records can only be used for a limited set of purposes[109] and requiring that their use conform with FCRA, including by requiring employers to obtain a worker's permission to purchase a consumer report.[110] If an employer is taking an adverse action against a worker, such as termination or demotion, it must provide notice to the worker that a consumer report was used and provide a copy of the report before the action is taken.[111] CRAs also have obligations to workers under FCRA, including a duty to follow reasonable procedures to assure the maximum possible accuracy of its information, to disclose information in a worker's file to the worker upon request,[112] and to investigate allegations that the information is incorrect.[113] CRAs must also disclose the identity of anyone who has used a

[104] 15 U.S.C. § 1681(d)(1)(B). FCRA excludes from its definition communications made to employers in connection to misconduct investigations. § 1681a(d)(2)(D).
[105] CFPB, *Background Dossiers and Algorithmic Scores for Hiring, Promotion, and Other Employment Decisions*, Consumer Financial Protection Circular 2024-06 1 (Oct. 24, 2024).
[106] *Id*. at 2.
[107] *See id*.
[108] *Id*. at 3.
[109] FCRA defines employment purposes as "evaluating a consumer for employment, promotion, reassignment or retention as an employee." 15 U.S.C. § 1681a(b).
[110] *Id*. § 1681b(b)(1)–(2).
[111] *Id*. § 1681b(3)(A). There are some exceptions to this requirement for transportation industry workers and national security investigations. *Id*. § 1681b(b)(3)(B)–(C), (4).
[112] *Id*. § 1681g(a)(2).
[113] *Id*. § 1681i(a)(1)(3).

consumer report for employment purposes within two years prior to the date a worker requests such information.[114]

In 2024, the CFPB issued landmark guidance explaining that employers making employment decisions using background dossiers, algorithmic scores, and other third-party consumer reports about workers must adhere to FCRA.[115] While the circular was rescinded by the current administration, it lays out a crucial understanding of FCRA's privacy protections that workers may still adapt for their own litigation.[116] Under that framework, any entities that collect consumer data from sources other than the client-employer and use that information to train an algorithm that assesses workers would be covered by FCRA in addition to traditional CRAs that collect and sell information.[117] As discussed further in Section V, this understanding may extend FCRA protections to the right to organize by implicating employers that use surveillance reports and outputs from union avoidance consultants and ADSs to target worker organizers without consent or a permissible purpose under FCRA. Similarly, CRAs that provide this information would be liable to workers under this application of the CFPB's framework.

FCRA is a critical set of privacy protections for workers, but it, too, has its weaknesses. Most notable is FCRA's consent-based approach.[118] As noted above, FCRA requires a worker's consent before CRAs can disclose a consumer report to an employer. In light of the power imbalance between workers and employers, however, this can be an easy box for employers to check.[119]

114 *Id*. § 1681g(a)(3)(A)(i).
115 CFPB, *supra* note 105.
116 The first case to apply this theory, *Kistler v. Eightfold AI*, was filed in early 2026 and is ongoing. 3:26-cv-01768 (removed to N.D. Cal. Mar. 2, 2026) For more information, see Outten & Golden, *Landmark Class Action Accuses Eightfold AI of Illegally Producing Hidden "Credit Reports" on Job Applicants* (Jan. 21, 2026).
117 CFPB, *supra* note 105, at 5–6.
118 For a brief discussion of the problems of notice and consent frameworks, *see* Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 Stan. Tech. L. Rev. 74, 95–97 (2018).
119 Matthew Bodie, *The Law of Employee Data: Privacy, Property, Governance*, 97 Ind. L.J. 707, 720 (2022) ("Because the FCRA largely focuses on procedural requirements of notice and consent, employers can generally comply with the statutory scheme if they follow the rules.").

3. State Privacy Laws

While 24 states have enacted comprehensive privacy laws so far,[120] only one state law, the California Consumer Privacy Act (CCPA), includes any protections for workers.[121] In addition, while Illinois does not have a comprehensive privacy law, its Biometric Information Privacy Act (BIPA) is often held up as an example of a strong, worker-inclusive privacy law because it provides a private right of action against any entity that collects, stores, or distributes biometric information without consent.[122] The CCPA took the important step of creating notice and data access rights for workers and establishing a data minimization standard for Californians' personal information. Specifically, the CCPA provides workers with the right to know when employers are monitoring them and for what purpose, including whether employers are buying data about them or tracking their social media activity.[123] Workers also have the right to access the data collected about them, request that it be corrected or deleted, and opt out of the sale of their data.[124]

The CCPA also implements strong data minimization requirements that limit an employer's collection, use, retention, and disclosure of personal information to what is "reasonably necessary and proportionate to achieve" a limited set of disclosed purposes.[125] Establishing an appropriate data minimization standard is significant because it substantively limits what data an employer may collect and for what purpose. Under this law, an employer's use of workers' data should not cover interfering with union campaigns; undermining workers' legal rights is

[120] These states are Alabama, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Louisiana, Maryland, Montana, Nebraska, New Hampshire, New Jersey, Oklahoma, Oregon, Rhode Island, Tennessee, Texas, Utah, Vermont, and Virginia. *See, e.g.,* Maryland Online Data Privacy Act, Md. Code Ann., Com. Law §§ 14-4701 *et seq*. In 2024, EPIC coauthored a report with the U.S. PIRG Education Fund that discussed 14 state privacy laws. Caitriona Fitzgerald, Kara Williams, & R.J. Cross, *The State of Privacy: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better* (Feb. 2024).
[121] Mishal Khan & Annette Bernhardt, *The Current Landscape of Tech and Work Policy in the U.S.: A Guide to Key Laws, Bills, and Concepts*, U.C. Berkeley Lab. Ctr. (Dec. 15, 2025).
[122] Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1 *et seq*. (2026).
[123] Kung Feng, *Overview of New Rights for Workers Under the California Consumer Privacy Act*, U.C. Berkeley Lab. Ctr. (Dec. 6, 2023).
[124] *Id*. Notably, the CCPA allows workers to designate authorized agents, such as unions and other worker organizations and advocates, to make requests for data access, correction, or deletion on their behalf. Implemented correctly, this could be a valuable tool for correcting the asymmetries between workers and employers.
[125] Cal. Civ. Code § 1798.100(c) (2026); Cal. Code Regs. tit. 11, § 7002 (2026).

not a legitimate reason for which to collect data, nor is it compatible with other acceptable purposes that the law recognizes. However, the effectiveness of the CCPA is limited by its failure to provide a private right of action.

Illinois' BIPA, despite being focused only on biometric data collection,[126] is an extremely effective law for workers.[127] BIPA provides a private right of action against any entity that collects, stores, or discloses biometric information without consent.[128] The private right of action has made BIPA a very effective tool to ensure that workers have some notice and say before any biometric data can be collected about them. However, BIPA is constrained by the inherent flaws of notice and consent frameworks[129] that fail to account for workers' realities. Employers control the means of work and can put stipulations on hiring and continued employment, including requiring workers to consent to background checks, agree to follow policies laid out in employee handbooks, and use the tools selected by employers. The unilateral control employers enjoy significantly diminishes worker agency and consent. Another limitation is that workers face surveillance using all kinds of their personal data, not just biometric information. Still, these frameworks in California and Illinois are more robust than any other state.

4. State Worker Surveillance Notice Requirement Laws

Several states have enacted laws that require employers to notify workers of workplace surveillance. For example, New York requires every private employer to provide notice of its electronic monitoring practices to all employees upon hiring, place that notice in a conspicuous place viewable by all employees, and to obtain employee acknowledgement of the notice.[130] Connecticut law requires

[126] BIPA defines "biometric information" broadly to include any information used to identify someone using their biometric identifier, including retina or iris scans, fingerprints, voiceprints, and scans of hand or face geometry. 740 Ill. Comp. Stat. Ann. 14/20. Courts have also found that photos and videos that analyze information about individuals, like inferring emotions, are biometric identifiers. *See Konow v. Brink's, Inc.,* 721 F. Supp.3d 752 (N.D. Ill., 2024); *Wilk v. Brainshark, Inc.*, 631 F. Supp. 3d 522, 529–30 (N.D. Ill. 2022).

[127] BIPA does exclude certain categories of employees, including most railroad and airline employees, *Miller v. Sw. Airlines Co.*, 926 F. 3d 898, 903 (7th Cir. 2019), and unionized workers subject to arbitration agreements. *Fernandez v. Kerry, Inc.*, 14 F. 4th 644, 646 (7th Cir. 2021); *Williams v. Jackson Park SLF, LLC*, No. 19-CV-8198, 2020 WL 5702294, at *4 (N.D. Ill. Sept. 24, 2020).

[128] 740 Ill. Comp. Stat. Ann. 14/20.

[129] *Waldman*, *supra* note 118 at 95–97. See also *Cohen*, *supra* note 54.

[130] *N.Y. Civ. Rights Law* § 52-C-2 (2025).

both public and private employers to provide prior written notice to employees about the types of electronic monitoring which may occur, but does not require affirmative acknowledgement by the employee.[131] Delaware law also requires both private and state employers to provide prior written notice regarding monitoring of phone transmissions and email and internet access or usage.[132]

Most recently, Maine passed a law that requires an employer to disclose its use of workplace surveillance before it begins using it and places several additional limits on employers.[133] The law covers any private or public employer and ensures broad coverage of workers by widely defining employee as "an individual who provides services or labor for an employer for wages or other remuneration."[134] The law also prohibits an employer from using audiovisual monitoring in an employee's residence, personal vehicle, or on the employee's property as a means of surveillance unless the monitoring is required by the employer for the duties of the job.[135] Lastly, an employee may decline an employer's request to install data-collection or transmission applications on the employee's personal electronic devices.[136] The law creates several carveouts from its notice requirement, however: safety and security cameras, GPS and safety devices on employer-owned vehicles, and personal care services, such as when a home-care worker provides services in a patient's residence.

Requiring employers to provide notice of workplace surveillance to workers is an important first step in breaking down the information asymmetry in the workplace. However, only one of these laws empowers individual workers to vindicate their rights. The persistent lack of private rights of action in these laws make them less potent. Further, the laws do not directly address the uses of workplace surveillance data for interference with worker organizing.

5. State Laws Governing Automated Decisionmaking Systems

Several states have also sought to regulate ADSs, and these efforts often prioritize regulating automated decisions regarding employment. California's CCPA, which extends to employment-related decisions, provides workers with

[131] Conn. Gen. Stat. § 31-48d.
[132] Del. Code Ann. tit. 19, § 705.
[133] *An Act to Regulate Employer Surveillance to Protect Workers*, L.D. 61, 132d Leg., 2d Reg. Sess. (Me. 2026) (codified at Me. Rev. Stat. tit. 26, § 620-A).
[134] *Id*.
[135] *Id*. § 620-A(3).
[136] *Id*. § 620-A(4).

some rights and protections when ADS are used to make decisions about their employment. However, its implementing regulations contain multiple carveouts, fail to cover a broad range of algorithmic management systems, and lack strong guardrails.[137] Similarly, Colorado has a law going into effect in 2027 that will require an employer using ADSs to materially influence a consequential employment decision to provide clear and conspicuous notice that an ADS was used, specific information about the ADS and the personal information that was used in the decision, and rights to correct incorrect personal information and request human review and reconsideration if they are adversely affected by an ADS-influenced decision.[138] Connecticut has a law specific to the employment context that similarly requires employers to provide notice about their use of an ADS to affected employees and applicants.[139] Some states, such as Illinois, have amended their laws to clarify that using ADS in employment-related decisions in ways that use protected characteristics (and their proxies) and effectively discriminate against workers is illegal.[140] With the potential exception of the CCPA, none of these laws substantially require employers to use the least privacy-invasive methods or prevent employers from using an ADS to interfere with worker organizing. Further, these laws tend to rely heavily on the flawed notice-and-consent framework.

[137] *See* EPIC, *supra* note 13. For example, § 7221(b)(2)–(3) exempts ADS used for assessing workers for hiring decisions, allocation or assignment of work, and compensation from requiring employers to provide an opt-out mechanism.
[138] Automated Decision-Making Technology, S.B. 26-189, 2026 Reg. Sess. (Colo. 2026) (codified at Colo. Rev. Stat. §§ 6-1-1701 et seq.).
[139] An Act Concerning Online Safety, S.B. 5, 2026 Sess., Pub. Act 26-15 (Conn. 2026).
[140] H.B. 3773, 103d Gen. Assembly, Pub. Act 103-0804 (effective January 1, 2026) (amending the Illinois Human Rights Act (IHRA)).

V. How to Shut Down Algorithmic Unionbusting

As invasive surveillance continues to quickly scale up in both ease and access, workers need solutions now. State and federal legislators alike can tackle employers repurposing data-driven surveillance for algorithmic unionbusting by implementing new privacy protections and ramping up enforcement of existing laws. Solutions must align with organizing principles by providing collective and individual protections, resetting the power balance between workers and companies, and removing existing incentives to continuously collect and misuse worker data. While federal labor law has been significantly weakened by decades of industry influence, effective change on these issues is still possible at the federal level.

A. Center These Principles to Shut Down Algorithmic Unionbusting.

We urge policymakers to center the following principles in any legislation created to address algorithmic unionbusting.

- **Empower all workers, not some.** All workers deserve protection from workplace surveillance and algorithmic exploitation. Existing labor and employment law protects many, but not all, workers. For example, as more jobs become platform and gig-based, employers are able to improperly classify more workers as "independent contractors" despite exercising great control over them in ways that more closely resemble traditional employees. Further, existing law does not grant supervisors the right to organize or join unions despite many supervisors now being similarly subject to algorithmic management themselves. To shut down algorithmic unionbusting, legislation must expand coverage to include these workers.
- **Protect workers against abuses by anyone in the algorithmic unionbusting ecosystem.** As discussed throughout this paper, algorithmic unionbusting is a networked system made up not only of employers and consultants but also entities that make and sell data and tools for algorithmic unionbusting. To adequately address the scale of networked harms, and the power behind it, solutions must hold all members of the algorithmic unionbusting ecosystem accountable and place the burden of proof on these actors.

- **Provide collective solutions for collective harms.** Algorithmic unionbusting produces harm at scale. To dismantle this practice, we must meet collective harms with collective solutions. Thinking collectively means removing roadblocks to challenging harm, including permissive consent-based standards; providing workers with rights they may assert as a collective; and guaranteeing collective and individual privacy rights that recognize the dangers of aggregated, inferential data and the concerted effect of algorithmic unionbusting.

B. States Can Protect Worker Privacy Now.

While protecting labor rights has traditionally fallen to federal agencies, state legislators are far from powerless. Privacy law presents a viable path for states to protect the right to organize for every worker. Comprehensive privacy laws that protect workers' interests are a strong choice given the diminishing boundaries between a person's personal and professional life. Whether a strong privacy law is comprehensive or specific to workers, however, it should contain similar features, including substantial data minimization, outright bans and significant limitations on dangerous automated tools, and a private right of action. Policymakers should strive to center collective privacy—not only individual privacy—in any legislation. In addition, policymakers should prohibit the use of overly invasive and illegitimate electronic monitoring tools, particularly those that continuously extract and produce information.[141]

1. Impose a Data Minimization Framework That Raises the Bar for Data Collection

Data minimization is a key requirement for providing workers with necessary protections for their privacy and autonomy. This framework prevents many of the worst abuses of worker data and surveillance.[142] To start, a workplace data minimization framework should prohibit employers' collection and use of worker data unless it is strictly necessary for a defined, legitimate, employment-related purpose, and noting specific illegitimate purposes for which data collection and

[141] With this recommendation, we echo the call from our colleagues in their paper about the "privacy" trap. See Longiaru et al., *supra* note 55.

[142] For discussion of data minimization in consumer settings, see Suzanne Bernstein, *Data Minimization: Centering Reasonable Consumer Expectation in the FTC's Commercial Surveillance Rulemaking*, EPIC (Apr. 20, 2023).

use is always prohibited, such as opposing union campaigns or selling worker data, which serves no legitimate employment-related purpose.[143]

The "strictly necessary" standard would also require employers to ensure that the method they use to monitor workers is the method least likely to violate worker privacy and civil rights while still achieving the legitimate goal at hand. Some uses, such as emotion recognition systems, would never meet this threshold because those systems rely on pseudoscience, have an unacceptable risk of discrimination and bias, and serve the inherently illegitimate purpose of interpreting a worker's mental state.[144] An effective data minimization standard could also create context-based standards, as workplaces and their legitimate needs differ significantly between industries and roles. For example, in most workplaces, it would not be strictly necessary to collect data outside of working hours or work sites, collect data from personal devices, or collect highly sensitive data when other non-sensitive data suffices.

Finally, policymakers should take care to construct a data minimization framework that forbids an employer from skirting around the prohibited purposes by obtaining consent—the employer simply cannot collect and use worker data for impermissible purposes, including hindering worker organizing. This tackles the power asymmetry that exists today, where employers enjoy discretion to decide how to collect and use data about workers with few limitations and often based on functionally coerced consent from workers. A strong data minimization framework would also ensure that employers cannot pressure individual workers through notice and consent mechanisms.

2. Enact Automated Decisionmaking Systems Laws that Ban or Limit Harmful Systems

Given the proliferation of ADS in the workplace and the ease of weaponizing such systems against worker organizing, states should enact strong guardrails.[145] ADS laws should broadly cover systems that make or influence decisions in the workplace, including for hiring, scheduling, pay, benefits, task assignments, demotion, promotions, and performance assessments.

Employers should be prohibited from relying primarily on ADS for significant decisions and should be required to have a competent human in the loop who

[143] Nguyen et al., *supra* note 7.
[144] Ajunwa, *supra* note 11, at 138–52.
[145] EPIC, *supra* note 13, at 24–43.

is trained on the strengths and weaknesses of these systems and empowered to ignore or override automated decisions based on their expertise.[146] Workers must be able to understand, and employers must be able to explain, the decisions after they are made, including the data sources and reasoning of the decisions. Further, workers must be empowered to correct and challenge decisions in a timely manner and with little burden. In addition, systems must be required to undergo pre-deployment assessments to ensure that the system works as intended for the stated purpose, and that it does not lead to discriminatory, erroneous, or unfair outcomes. Potential impacts that should be tested for include 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.[147] After deployment, independent audits should be required to continuously monitor the systems with oversight by a competent government authority.

3. Include a Private Right of Action

While enforcement by the government is essential,[148] its resources are limited and its timeframes often ineffective against the breakneck speed of a union election and the real demands of workers' daily lives. Including a private right of action in new privacy laws empowers worker voices, preserves and focuses government resources, and imposes enforceable legal obligations on companies that use data to violate the right to organize.

A private right of action is the most important tool policymakers can give to workers looking to protect their privacy and dignity. Dignity and expression are bound up in both privacy and worker organizing—the right to have a voice in your workplace and conditions extends to the right to have a voice in how your

[146] National Institute for Workers' Rights, *AI Is Not the Boss of Me* (forthcoming 2026); Khan & Bernhardt, *supra* note 121. It's important to also ensure that the employer does not impose undue pressure or incentive on the worker that is the human in the loop to rubber-stamp the ADS's outputs. EPIC, *supra* note 13, at 47–49.

[147] Longiaru et al., *supra* note 55, at 12.

[148] Hybrid enforcement models, where private and public enforcement move simultaneously to one another, are common, including in employment and labor law. See, e.g., Lauren Henry Scholz, *Private Rights of Action in Privacy Law,* 63 Wm. & Mary L. Rev. 1639, 1655–63 (2022). This is for good reason; hybrid enforcement promotes broader and faster enforcement, avoids issues of political will and capture, and helps conserve and focus limited government resources. See J. Maria Glover, *The Structural Role of Private Enforcement Mechanisms in Public Law*, 53 Wm. & Mary L. Rev. 1137, 1153–60 (2012). For recommendations on shaping effective public enforcement, see Cohen, *supra* note 54.

employer shapes its information practices and adopts workplace technology. Workers are in the best position to identify algorithmic unionbusting and bring actions to vindicate their rights. Where regulators move slowly and are susceptible to political pressure,[149] a private right of action puts workers back in control and lets them respond quickly when their rights are violated. Any bill that centers worker voice and dignity must include a private right of action.[150]

A private right of action is also key to disincentivizing employers from collecting and abusing workers' information. Ensuring individuals have the right to hold companies accountable in court is the best way to ensure companies take compliance with the law seriously. As privacy expert and professor Woodrow Hartzog has noted, "only private causes of action seem capable of meaningfully deterring companies from engaging in practices…based on business models that inevitably lead to unacceptable abuses."[151] The potency of private rights of action are further evidenced by industry's scramble to oppose any proposal that includes them.[152]

Finally, a well-structured private right of action reduces the burdens on workers seeking justice. In order to ensure that the private right of action is functional, workers must be able to easily exercise it and the burden of proof must shift to employers to demonstrate that they did not misuse worker data or workplace technologies in ways that act as algorithmic unionbusting.[153] By implementing fee-shifting frameworks, explicit protections for the right to file suit as a class, remedies like disgorgement of profits and data, or other elements that promote the use of this remedy, legislators avoid their private right of action becoming a functionally unavailable bauble.

[149] Woodrow Hartzog, *BIPA: The Most Important Biometric Privacy Law in the US?*, in Regulating Biometrics: Global Approaches and Urgent Questions 101–103 (Amba Kak ed., Sep. 2020). Scholz, *supra* note 148, at 1646.
[150] Scholz, *supra* note 148, at 1645.
[151] Hartzog, *supra* note 149, at 101–103.
[152] Scholz, *supra* note 148, at 1642–44.
[153] AI Now Institute, *Algorithmic Management: Restraining Workplace Surveillance* (Apr. 11, 2023).

C. There's Work to Be Done at the Federal Level.

1. Congress Should Act Now

By following the same guidelines we've recommended to states, Congress could enact a strong nation-wide privacy law that protects workers from algorithmic unionbusting. But why wait? Congress can protect workers now by passing the No Robot Bosses Act,[154] the Stop Spying Bosses Act,[155] and the Richard L. Trumka Protecting the Right to Organize (PRO) Act.[156]

a. Pass the No Robot Bosses Act & the Stop Spying Bosses Act

In 2026, several senators, led by Senator Ed Markey, introduced the No Robot Bosses Act and the Stop Spying Bosses Act, two bills that are key to protecting workers from employers abusing worker data to violate their rights.

The No Robot Bosses Act prohibits employers from predominantly relying on ADSs to make workplace decisions, mandates pre-deployment assessments and transparency about the use of ADS, gives workers the right to opt out of algorithmic management in favor of human review, and creates several other privacy protections for job applicants and workers.

The Stop Spying Bosses Act curtails employers' ability to surveil workers, including by limiting collection and use of worker data to what is strictly necessary for a legitimate employment-related purpose and prohibiting the use of worker data to surveil workers' union activity, political or religious views, immigration status, or off-duty conduct. It also mandates transparency. Workers are entitled to know what data is collected, how it is used, and who has access to it. At the same time, workers can demand access to their data and that it be corrected if it is inaccurate.

Both of these bills would be significant steps in protecting the right to organize by imposing a strong data minimization framework, limiting ADSs that could be abused to punish organizers, and taking steps to correct the data and power imbalances that data consolidation and obfuscation create. The Stop Spying Bosses Act, in particular, reins in what an employer may know about its workers at all, removing access to information that employers and their consultants frequently use to target workers.

[154] No Robot Bosses Act, S. 4833, 119th Cong. (2026); H.R. 6371, 119th Cong. (2025).
[155] Stop Spying Bosses Act, S. 4831, 119th Cong. (2026). H.R. 9402, 119th Cong. (2026).
[156] Richard L. Trumka Protecting the Right to Organize Act of 2025, S. 852, 119th Cong. (2025); H.R. 20, 119th Cong. (2025).

b. Pass the PRO Act

The PRO Act would be a tremendous win for workers fighting algorithmic unionbusting. Most recently introduced in 2025, the PRO Act would amend federal labor laws like the NLRA and LMRDA to expand protections for workers' rights to organize and collectively bargain in their workplaces.

In particular, the PRO Act ensures that employers cannot fire and replace striking workers, change working conditions during negotiations, or suspend or withhold work from employees to stop them from striking—all tactics made significantly easier for employers to impose through algorithmic unionbusting. If an employer violates these rights, workers can use the PRO Act's private right of action to hold employers personally liable.

The PRO Act would also level the playing field when companies hire union avoidance consultants. Not only would it close the advice loophole in the LMRDA by requiring reporting of any indirect activities carried out by union avoidance consultants, but the PRO Act also narrows the information gap by requiring the Department of Labor to make this information easily accessible and searchable.

Opponents of the PRO Act accuse it of forcing companies to violate employee privacy by delivering eligible voter lists to unions. This accusation reflects a weak understanding of privacy. What is privacy for? First, privacy provides the essential boundaries—space from prying eyes—that individuals need in order to determine their own critically rooted thoughts, beliefs, and opinions and to build relational ties.[157] Workers in particular require this space. Employers have outsized control over the workplace and outsized influence over their workforce.[158] Privacy is meant to diminish the effect of those power asymmetries and provide workers a haven from employer control and influence so that they may determine their thoughts and actions for themselves.[159] Second, privacy strengthens the collective interests of communities and democratic institutions by interrupting harmful information flows to powerful actors and creating the room to build trust and collective identity among community members.[160] The PRO Act's strong protections for the right to

157 Julie E. Cohen, *What is Privacy For?*, 126 Harv. L. Rev. 1904, 1905–11 (2013).
158 Rogers, *supra* note 6, at 81–103.
159 *See id*. at 88–89 (arguing that workers need spaces safe from employers to deliberate and plan, which existing NLRA doctrine does not provide).
160 Cohen, *supra* note 157, at 1906, 1912–18. See also Rogers, *supra* note 6, at 81–103.

organize deliver this space. In this way, the PRO Act is, contrary to employer outcry, a strong protector of worker privacy.[161]

2. The National Labor Relations Board Should Bring the NLRA into the Modern Era of Worker Surveillance.

The drafters of the NLRA designed it for a different era, one where employer surveillance meant a foreman with a clipboard or a company detective stationed outside a union hall. The emergence of algorithmic management fundamentally changed workplace dynamics, enabling employers to monitor worker behavior at a scale, scope, and granularity that labor doctrine never contemplated. Existing Board frameworks cannot properly address systems that track keystrokes, enforce productivity quotas in real time, and correlate protected activity with adverse employment decisions through machine learning. This results in a legal regime that, without significant revisions, will be inadequate to maintain conditions under which workers can meaningfully exercise their Section 7 rights. Three reforms, each grounded in existing Board authority, would assist in closing that gap.

a. Adopt a Presumption-Based Framework for Intrusive Surveillance

The most doctrinally accessible reform available to the Board is adopting a tiered presumption system for algorithmic monitoring modeled on an existing framework.[162] As proposed by scholar Charlotte Garden and former NLRB General Counsel Jennifer Abruzzo, the Board should create a sliding scale under which the most intrusive forms of electronic monitoring (such as continuous audio recording in break rooms, real-time behavior scoring, and biometric tracking) are presumptively unlawful unless the employer can demonstrate that special circumstances make them necessary.[163] Less intrusive forms of surveillance would be presumptively lawful, but only where: 1) the employer demonstrates a legitimate business purpose, and 2) workers

[161] This is not to mention the careful protections that the PRO Act brings in. Employers are only required to deliver voter lists to unions after an election has been approved by the NLRB, strengthening the ability of every worker to make an informed decision. Further, the Act does not purport to replace any other privacy protection guaranteed under the law, including regarding the sale or disclosure of personal information.

[162] *Republic Aviation Corp. v. National Labor Relations Board*, 324 U.S. 793 (1945) (establishing the balancing test for how employers can restrict employee solicitation and distribution of union materials on company premises).

[163] Garden, *supra* note 68, at 68; Memorandum GC 23-02 from Jennifer A. Abruzzo, General Counsel, *supra* note 76.

are unable to show that the monitoring was adopted or deployed to deter protected concerted activity.[164]

Labor law's current indifference to employer baseline choices in non-union workplaces, where the chilling effects of surveillance are the most acute yet the least visible, would be directly addressed by this presumption framework. Abruzzo's now-rescinded GC Memo 23-02 articulated a balancing approach that would require employer surveillance practices be "narrowly tailored" to a legitimate business need before any interference with Section 7 rights could be justified, and she connected this proposed approach to existing authority.[165] Thus, the Board has both precedent and institutional tools to implement this kind of framework without waiting for legislative action.

b. Find Algorithmic Management a Per Se Unfair Labor Practice Under Section 8(a)(1)

A more aggressive, but legally defensive, move forward would be for the Board to find that algorithmic management (where it operates so pervasively as to prevent workers from meaningfully engaging in protected concerted activity) constitutes a per se Section 8(a)(1) violation. When algorithmic systems are enmeshed into the operations of a workplace to such a degree that organizing is practically impossible, the "laboratory conditions" necessary for a fair election were already destroyed before any campaign even begins.[166] Such a dynamic goes beyond traditional union busting and impacts the structural social reality of workers. AI-driven productivity and surveillance systems can set a pace of work so relentless that workers have no realistic opportunity to engage in the informal, repeated conversations among coworkers that form the foundation of collective action, let alone a successful union campaign.

As the Supreme Court recognized in *Eastex*, the workplace is a "particularly appropriate place" for protected concerted activity precisely because it is where workers see one another and conditions are front of mind,[167] but algorithmic management can effectively eliminate that important space

[164] Garden, *supra* note 68, at 68; Memorandum GC 23-02 from Jennifer A. Abruzzo, General Counsel, *supra* note 76.
[165] Memorandum GC 23-02 from Jennifer A. Abruzzo, General Counsel, *supra* note 76, at 8.
[166] *Melanie Mignucci, Extraordinary Times, Extraordinary Measures: Protecting the Right to Organize in the Age of Algorithmic Management*, 58 Colum. J.L. & Soc. Probs. 385, 416 (2025).
[167] *Eastex, Inc. v. NLRB*, 437 U.S. 556, 574 (1978).

without issuing a single explicit no-solicitation rule. Ideally, where the Board finds that such conditions exist, the appropriate remedy is a narrow, non-majority bargaining order. The Supreme Court in *Gissel* acknowledged in dicta that in cases of outrageous and pervasive unfair labor practices, a bargaining order could issue without proof of majority support.[168] The Third Circuit once endorsed exactly that approach.[169] Resurrecting that creative remedy in the context of algorithmic management would restore a powerful Board tool to meet employers' most recent powerful weapon against collective action and would fulfill what the Board itself has described as its responsibility to adapt the Act to the "changing patterns of industrial life."[170]

c. Require Mandatory Disclosure as a Condition of Lawful Surveillance

Both of the prior recommendations depend, in practice, on workers or their advocates actually figuring out what surveillance is taking place. Under current law, that knowledge cannot be assumed. The covert nature of modern employer monitoring coupled with the lack of regulations requiring disclosure to workers that they are being surveilled creates compounding legal disadvantages for workers. Workers likely do not know they have been surveilled, nor when the surveillance began, and thus may be unable to establish a temporal proximity between their protected activity and an adverse employment action, which is essential to demonstrating retaliation. As a result, an employer with a surveillance infrastructure can observe protected activity, hold onto that data, and then deploy it months later in conjunction with other data as pretext for discipline. In that situation, the worker may never realize that retaliation occurred at all. The GC Memo 23-02 addressed this knowledge disparity directly by proposing that where an employer's surveillance interest is found to outweigh workers' Section 7 rights, the employer must nevertheless disclose the technologies in use, the reason for their deployment, and how collected data will be used.[171] Covert surveillance, absent a specific showing of necessity, should be categorically prohibited.

---

168 Mignucci, *supra* note 166, at 418 (citing *NLRB v. Gissel Packing Co.*, 395 U.S. 575, 613 (1969)).
169 Mignucci, *supra* note 166, at 418–19 (citing *United Dairy Farmers Coop. Ass'n v. NLRB*, 633 F.2d 1054, 1068 (3rd Cir. 1980)) (noting that the failure to recognize this authority would undermine the Act's goal of furthering the majority preference of all employees and likely incentivize even worse employer misconduct.).
170 *NLRB v. J. Weingarten, Inc.*, 420 U.S. 251, 266 (1975).
171 Memorandum GC 23-02 from Jennifer A. Abruzzo, General Counsel, *supra* note 76.

This requirement would both give workers the information they need to protect the confidentiality of their protected activity (if desired) and would deter the retaliatory use of surveillance by removing the cover that secrecy provides. It is worth noting that a disclosure requirement of this kind would connect naturally to broader legislative proposals for a federal privacy statute.

Taken together, these three reforms constitute a response grounded in Board precedent to challenge the impact algorithmic management and surveillance poses to collective labor rights. The presumption framework adapts a pre-existing doctrine to the surveillance context. The per se rule and bargaining order remedy extend *Gissel's* logic to a new category of pervasive employer conduct. The disclosure requirement prioritizes the confidentiality protections the Board has long said it seeks to protect. The political environment for ambitious Board action is constrained under the Trump Board, and any progress achieved at the Board under one administration remains vulnerable to reversal under the next. But the doctrinal foundation for all three reforms already exists.

3. Workers and Advocates Should Consider Using FCRA to Inject Transparency.

As discussed throughout this white paper, employers frequently contract with third-party union avoidance consultants and use third-party software to identify individuals that are likely to organize or be sympathetic to organizing. Workers who believe that their employer used their personal information to identify and retaliate against them for their organizing (or potential to organize) may be able to bring a claim under FCRA against their employer or the third party supplying that information.

It is worthwhile to quickly recap how FCRA applies to workers. Recall that FCRA includes workers in the definition of "consumer" and imposes protections for a worker's personal information when that information is included in a consumer report and used to make decisions about that worker's employment. FCRA defines consumer reports broadly[172] to include any information with bearing on a worker's character, reputation, characteristics, or lifestyle if that information will be used, even in part, to establish the worker's eligibility for employment

[172] 15 U.S.C. § 1681a(d)(1).

or make adverse employment decisions.[173] FCRA imposes obligations on the consumer reporting agencies (CRAs) that produce consumer reports and the employers that purchase these reports, including requiring them to obtain a worker's consent prior to purchasing or selling the report.

Both a report from a union avoidance consultant and an output from an algorithm sold by companies like Perceptyx that identify the organizing risk posed by an individual worker qualify as consumer reports if a company considers that information when making decisions about hiring, firing, demotion, or relocation. As discussed previously, employers frequently retaliate against workers that organize in these ways, and reports and outputs that identify organizing risk factor into many such actions. Further, these reports often include covered kinds of information gathered from employer or public records and data brokers, including an individual's previous organizing experiences, financial situations, employment histories, and personal characteristics. Perceptyx, for example, has stated that it has "hundreds of data points" on any given worker.[174]

Of course, these entities must be CRAs to be selling consumer reports within the meaning of FCRA. Union avoidance consultants qualify as CRAs if they regularly assemble or evaluate these union risk reports on individual workers for their employer clients. Companies like Perceptyx similarly act as CRAs covered by FCRA. These entities collect information regarding workers, including job performance and collective bargaining activity, and use that information to train algorithms sold to employers for the purpose of assessing workers and informing employment decisions.

This all means that an employer that engages the union avoidance industry—and the union avoidance industry itself—is governed by FCRA when it obtains reports on individual workers.[175] Employers that fail to obtain consent from a worker to obtain these reports are liable to that worker under FCRA. The same is true for employers that take adverse action against a worker without providing them a copy of the report.

---

[173] *Id*. Further, the CFPB had issued proposed rules that would bring data brokers into the fold when they sell data typically used to make employment eligibility determinations, as well. *See* CFPB, *Fact Sheet: The CFPB's Proposed Rule to Rein in Sprawling Data Broker Industry* (2024).
[174] Kessler, *supra* note 37.
[175] In its 2024, the CFPB seems to contemplate this result, as well, when it acknowledges the use of consumer reports to "predict worker behavior, including union organizing activity . . . ." CFPB, *supra* note 105, at 3.

Like all FCRA claims available to workers, this theory of liability has its limits. For example, the reports would not be covered by FCRA if they solely contained information gleaned from interactions between the report-maker and the worker who is the subject of the report. However, this is unlikely to be the case. The scant reports available about the union avoidance industry show that it gathers information from sources other than the workers, including public sources, managers, social media, and possibly data brokers.[176]

This theory of liability may be further limited by a worker's previous consent and the information and power asymmetry that pervades the workplace. Absent a union, workers have little choice in the conditions and modes of their employment. As such, a worker may have consented to their employers' purchase of consumer reports when they signed their employee handbook as a condition of employment. Further, as noted earlier, it would be difficult for workers to know whether employers purchased these reports and used them for retaliation.

Finally, it can be onerous for an individual worker to take on a civil case against their employer because of the time, cost of litigation, and threat of further retaliation. However, a lone worker is unlikely to be the only one investigated by their employer, which points to the possibility of a group or class of workers filing a FCRA suit together. While these limitations exist, this theory of employer and consultant liability under FCRA may prove useful leverage for bringing transparency and accountability back to the collective bargaining process.

[176] *See* Sections I and II, *infra*.

Conclusion

Continuously surveilled and forcibly datafied, workers are demanding a voice in their workplace to fight back against pervasive workplace technologies that diminish their autonomy. As worker organizing continues to gain momentum, employers and their consultants have responded by outfitting old techniques with new technologies. Algorithmic unionbusting violates privacy, chills worker's rights, and suppresses the benefits that workers and their communities stand to gain through labor organizing. Our legal framework is not keeping pace with these harms. Shutting down algorithmic unionbusting is possible. To do it, we must act at all levels to bring labor law into the modern day, guarantee worker privacy, and empower all workers.

Appendix: Instances of Algorithmic Unionbusting

Employer/ Consultant	Unionbusting Activity	Brief Description of Unionbusting Activity	Industry	Source	Year
Rockstar Games	Employee Surveillance –– Communications	Workers fired by Rockstar Games accuse the developer of infiltrating their private Discord groups to monitor their unionization efforts.	Media	Rockstar Trial Continues With Accusations of “Covert Monitoring”	2026
Starbucks	Employee Surveillance–– Tracking Union Activity; Digital Anti-Union Campaigning	Monitoring and tracking employees’ engagement with union-related social media posts. Sending mass texts to employees that included anti-union messaging.	Food and Beverage	Surveillance, Spacing, Screaming and Scabbing: How Digital Technology Facilitates Union Busting	2026
New York Times	Employee Surveillance–– Performance	Accused of violating union contract by secretly using AI to surveil employees and monitor job performance.	Media	Union files unfair labor practice charge, contract grievances against The Times for using AI programs to surveil and monitor union members	2026
UnityPoint	Employee Surveillance –– Communications	Attending hospital unit meeting group calls to give talks about upcoming union elections while forcing the cameras to stay on.	Healthcare	Nurses in Iowa are Fighting an Unprecedented Anti-Union Campaign	2025
Walmart	Employee Surveillance–– Tracking Union Activity	Workers attest that the company’s expansive use of surveillance technology has a chilling effect on union organizing.	Retail & Grocery	AI Surveillance Won’t Stop Theft, but It Might Stop Unions	2025

Employer/ Consultant	Unionbusting Activity	Brief Description of Unionbusting Activity	Industry	Source	Year
Walmart	Employee Surveillance –– Communications	Using AI tool to gauge employee sentiment by monitoring communications, with the capacity ––through the eDiscovery tool–– to identify otherwise anonymized employees.	Retail & Grocery	How Walmart, Delta, Chevron and Starbucks are using AI to monitor employee messages	2024
Delta Air Lines	Employee Surveillance –– Communications	Using AI tool to gauge employee sentiment by monitoring communications, with the capacity––through the eDiscovery tool–– to identify otherwise anonymized employees.	Airlines and Aviation	How Walmart, Delta, Chevron and Starbucks are using AI to monitor employee messages	2024
T-Mobile	Employee Surveillance –– Communications	Using AI tool to gauge employee sentiment by monitoring communications, with the capacity––through the eDiscovery tool–– to identify otherwise anonymized employees.	Telecomms	How Walmart, Delta, Chevron and Starbucks are using AI to monitor employee messages	2024
Chevron	Employee Surveillance –– Communications	Using AI tool to gauge employee sentiment by monitoring communications, with the capacity––through the eDiscovery tool–– to identify otherwise anonymized employees.	Energy	How Walmart, Delta, Chevron and Starbucks are using AI to monitor employee messages	2024

Employer/ Consultant	Unionbusting Activity	Brief Description of Unionbusting Activity	Industry	Source	Year
Starbucks	Employee Surveillance –– Communications	Using AI tool to gauge employee sentiment by monitoring communications, with the capacity––through the eDiscovery tool––to identify otherwise anonymized employees.	Food and Beverage	How Walmart, Delta, Chevron and Starbucks are using AI to monitor employee messages	2024
Astra-Zeneca	Employee Surveillance –– Communications	Using AI tool to gauge employee sentiment by monitoring communications, with the capacity––through the eDiscovery tool––to identify otherwise anonymized employees.	Pharma	How Walmart, Delta, Chevron and Starbucks are using AI to monitor employee messages	2024
Nestle	Employee Surveillance –– Communications	Using AI tool to gauge employee sentiment by monitoring communications, with the capacity––through the eDiscovery tool––to identify otherwise anonymized employees.	Food and Beverage	How Walmart, Delta, Chevron and Starbucks are using AI to monitor employee messages	2024
St. Peter's Health	Databasing Personal Information about Employees	Hired third-party union consultant, who collected sensitive personal information about employees, including disciplinary records, financial information, and details on family members.	Healthcare	Leak Targets Nurses Involved in Union Organizing at St. Peter's Health	2023

Employer/ Consultant	Unionbusting Activity	Brief Description of Unionbusting Activity	Industry	Source	Year
National Eating Disorders Association	AI Scabbing	Replaced their entire helpline workforce with an AI chabot after employees unionized.	Non-profit	Eating Disorder Helpline Fires Staff, Transitions to Chatbot After Unionization	2023
JBS	Employee Surveillance––Performance	Invested in a smartwatch app that tracks employees' mobility data, providing supervisors with metrics that could be assessed for productivity.	Food and Beverage	Big Meat Companies Want to Use Smartwatches to Track Workers' Every Move	2022
Tyson Foods	Employee Surveillance––Performance	Invested in a smartwatch app that tracks employees' mobility data, providing supervisors with metrics that could be assessed for productivity.	Food and Beverage	Big Meat Companies Want to Use Smartwatches to Track Workers' Every Move	2022
IRI Consultants (Now People Results)	Databasing Personal Information about Employees	Collecting detailed personal information on employees in order to assess their union sympathies; Working with independent contractors to obscure activities'; Monitoring employee activities during meetings to gather information about them.	Human Resources	Lazy,' 'Money-Oriented,' 'Single Mother': How Union-Busting Firms Compile Dossiers on Employees	2021

Employer/ Consultant	Unionbusting Activity	Brief Description of Unionbusting Activity	Industry	Source	Year
Holliday's Helping Hands	Employee Surveillance –– Communications	Company managers entered a Zoom call organized by union representatives and employees without being invited to do so. People familiar with the matter suspect that management spied on them to gather information about the call.	Non-profit	Inside the Secret World of Union Busting: How Employers Use Technology to Defeat Unions	2021
HelloFresh	Employee Speech Suppression–– Communications; Customer Speech Suppression–– Communications; Employee Surveillance–– Tracking Union Activity	Internal Slack messages show HelloFresh managers monitoring employees who posted on social media about unionization efforts. These conversations also indicate that HelloFresh tracked and attempted to delete online comments about the company's working conditions and attitude toward its employees' union drive.	Technology / Food and Beverage	Internal Slacks Show HelloFresh is Controlling Talk of Unionization	2021

Employer/ Consultant	Unionbusting Activity	Brief Description of Unionbusting Activity	Industry	Source	Year
McDonald's	Employee Surveillance–– Tracking Union Activity	The company's internal intelligence program uses a social media monitoring tool to collect and scrape data online and to monitorsocial media accounts, including those of its employees and prominent labor movement leaders. Former intelligence analysts have also claimed to have attempted to use the tool to piece together networks of workers involved in union efforts.	Food and Beverage	McDonald's Secretive Intel Team Spies on 'Fight for $15' Workers, Internal Documents Show	2021
Amazon	Employee Surveillance –– Communications	Hired Pinkerton spies to investigate workers at one of its warehouses in Poland; Posted a job listing stating that it was looking for analysts that would track information on labor organizing efforts in and against the company.	Technology	Amazon reportedly hired Pinkerton spies to monitor unionization efforts	2020
Amazon	Employee Surveillance –– Communications	Used fake accounts and social media monitoring tools to infiltrate private messaging channels and spy on employees and labor activists, gathering sensitive information about them and tracking their organizing efforts.	Technology	Secret Amazon Reports Expose the Company's Surveillance of Labor and Environmental Groups	2020

Employer/ Consultant	Unionbusting Activity	Brief Description of Unionbusting Activity	Industry	Source	Year
Whole Foods (Amazon)	Employee Surveillance—– Tracking Union Activity	Use of heat maps based on personal information and demographic data to track Whole Foods locations' propensity to unionize.	Retail & Grocery	Amazon-owned Whole Foods is quietly tracking its employees with a heat map tool that ranks which stores are most at risk of unionizing	2020
H&M	Databasing Personal Information about Employees	Collected sensitive personal information about employees at its service center to be used by managers in making performance evaluations and employment decisions.	Retail & Grocery	H&M fined for breaking GDPR over employee surveillance	2020
Google	Employee Surveillance—– Tracking Union Activity	Alleged to have built a surveillance tool to flag large employee events as potential union organizing efforts.	Technology	Google accused of spying with new tool that flags large employee meetings	2019
Facebook	Employee Surveillance —– Communications	Suspected of using internal communication platform to surveil employees; Signs overtly restrictive contracts with contractors that allow the firm to monitor and track communications and social media use; Hires Pinkerton to eavesdrop on employee conversations.	Technology	'They'll squash you like a bug': how Silicon Valley keeps a lid on leakers	2018

Employer/ Consultant	Unionbusting Activity	Brief Description of Unionbusting Activity	Industry	Source	Year
Google	Employee Surveillance –– Communications	Suspected of using internal communication platform to surveil employees; Hired Pinkerton to eavesdrop on employee conversations.	Technology	‘They’ll squash you like a bug’: how Silicon Valley keeps a lid on leakers	2018
Microsoft	Employee Surveillance –– Communications	Searched a private Hotmail account in 2012 to identifyan internal leaker.	Technology	‘They’ll squash you like a bug’: how Silicon Valley keeps a lid on leakers	2018

epic.org
ELECTRONIC PRIVACY INFORMATION CENTER

institute