Thursday January 9, 2025

California Privacy Protection Agency
2101 Arena Boulevard
Sacramento, CA 95834

Dear Board Members, Executive Director Soltani, and Agency Staff,

The signed organizations and individuals write to provide recommendations in response to the California Privacy Protection Agency's request for comments on proposed regulations for the California Consumer Privacy Act (CCPA). We commend Executive Director Soltani, Agency staff, and members of the Board for their commitment and dedication to giving guidance to California businesses, consumers, and now workers on the most important and consequential data privacy policy in the U.S.

For union and non-union workers alike, the emergence of AI and other data-driven technologies represents one of the most important issues that will shape the future of work in California for decades to come, potentially affecting workers' privacy, race and gender equity, wages and working conditions, job security, health and safety, right to organize, and autonomy and dignity.

By covering worker data in the CCPA and in the promulgation of regulations, California has a historic opportunity to lead the U.S. in establishing workers as key stakeholders in decisions about how best to govern artificial intelligence and related technological innovations – and in particular, to ensure that workers have the ability to control the collection and use of their personal data.

A Brief Overview of Data-Driven Technologies in the Workplace

With the advent of big data and artificial intelligence, employers in a wide range of industries are increasingly capturing, buying, and analyzing worker data, electronically monitoring workers, and using algorithmic management to make important employment-related decisions.[1] Recent studies have documented the use of data-driven technologies in sectors as diverse as trucking and warehousing, hospitals and home care, retail and grocery, hotels and restaurants, call centers, building services, and the public sector. Key functions for which employers are using these technologies range from hiring and firing, to workforce scheduling, performance monitoring and evaluation, and augmentation and automation of job tasks.

While digital technologies can benefit both workers and employers, the current challenge is the lack of robust guardrails to ensure responsible use and transparency regarding which employers are using which technologies. Many legal scholars have documented the inadequacies of existing laws in the U.S. to

[1] For overviews, see Ifeoma Ajunwa, *The Quantified Worker*, Cambridge University Press (2023); Annette Bernhardt, Lisa Kresge, and Reem Suleiman, "Data and Algorithms at Work: The Case for Worker Technology Rights," UC Berkeley Labor Center (2021); Matt Scherer and Lydia X. Z. Brown, "Warning: Bossware May Be Hazardous to Your Health," Center for Democracy & Technology (2021); Wilneida Negrón, "'Little Tech' Is Coming for Low-Wage Workers: A Framework for Reclaiming and Building Worker Power," Coworker (2021); Aaron Rieke, et al., "Essential Work: Analyzing the Hiring Technologies of Large Hourly Employers," Upturn (2021); Aiha Nguyen, "The Constant Boss: Work Under Digital Surveillance," Data & Society (2021); Merve Hickok and Nestor Maslej, "A Policy Primer and Roadmap on AI Worker Surveillance and Productivity Scoring Tools," AI Ethics 3, 673–687 (2023); Alexander Hertel-Fernandez, "Estimating the Prevalence of Automated Management and Surveillance Technologies at Work and their Impact on Workers' Well-Being," Washington Center for Equitable Growth (October 1, 2024).

protect workers in the data-driven workplace.[2] As a result of these deficiencies, direct harms to workers are beginning to emerge, with disproportionate impacts on people of color, women, and immigrants. The following examples illustrate the range in applications, impacts, and industries being documented by researchers and reported by workers:

- In warehouses, the unfettered use of productivity management systems can push the pace of work to dangerous limits and cause repetitive stress injuries for workers.[3]
- More generally, the COVID-19 pandemic accelerated the adoption of e-commerce throughout the retail sector. Online order fulfillment uses significant worker surveillance via the required use of phones, handheld devices, and smart glasses, as well as workplace cameras that use AI-based software to monitor worker behavior. The deployment of these technologies is not limited to fulfillment centers and workers, but extends to grocery stores and the public as well.[4]
- Bias based on race, gender, disability, and other characteristics in recruitment and hiring algorithms can mean that qualified workers are screened out from applicant pools.[5]
- Health care employers are increasingly using automated patient monitoring technology and clinical decision-making algorithms that feed into employers' algorithmic management systems to monitor nurses' work.[6] But these systems can result in increased workloads, dangerous understaffing, heightened pressure to work faster than is safe for patients and workers, and circumventing clinical judgment of nurses and other direct care workers.[7]
- Many gig economy employers track workers and use those metrics to determine workers' access to job opportunities and to set the pay rate (which can fall below the minimum wage once expenses are factored in).[8]
- Homecare workers are increasingly required to use tablets or their phones to verify the services they've provided. But the technology–known as Electronic Visit Verification–has also been used to micromanage already very difficult care work, as well as incorporate excessive GPS monitoring.[9]
- Many low-wage employers use "just in time" scheduling software that often doesn't factor in workers' schedule constraints or prevent back-to-back or erratic assignments, wreaking havoc on workers, especially working mothers and workers of color.[10]

---

[2] For example, see Ifeoma Ajunwa, Kate Crawford, and Jason Schultz, "Limitless worker surveillance," California Law Review, 105(3) (2017); Brishen Rogers, *Data and Democracy at Work*, MIT Press (2023); Solon Barocas and Andrew D. Selbst, "Big Data's Disparate Impact," 104 California Law Review 671 (September 30, 2016); and Pauline Kim, "Data-Driven Discrimination at Work," William & Mary Law Review 58 (3): 857–936 (2017).

[3] Martha Ockenfels-Martinez and Sukhdip Purewal Boparai, "The Public Health Crisis Hidden in Amazon Warehouses," Human Impact Partners and Warehouse Workers Resource Center (2021).

[4] Francoise Carre, et al. "Change and Uncertainty, Not Apocalypse: Technological Change and Store-Based Retail." UC Berkeley Labor Center (2020).

[5] Miranda Bogen and Aaron Rieke, "Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias," Upturn (2018).

[6] Peter Chan et al. "Ambient intelligence-based monitoring of staff and patient activity in the intensive care unit." *Aust Crit Care* (Jan. 2023), 36(1): 92-98. https://pubmed.ncbi.nlm.nih.gov/36244918/; "National Nurses United survey finds A.I. technology degrades and undermines patient safety." National Nurses United (May 15, 2024). https://www.nationalnursesunited.org/press/national-nurses-united-survey-finds-ai-technology-undermines-patient-safety.

[7] Lisa Bannon. "When AI Overrules the Nurses Caring for You." *Wall Street Journal* (Jun. 15, 2025). https://www.wsj.com/articles/ai-medical-diagnosis-nurses-f881b0fe; Bruce Giles. "'I don't ever trust Epic to be correct': Nurses raise more AI concerns." *Becker's Hospital Review* (Jun. 14, 2024). https://www.beckershospitalreview.com/ehrs/i-dont-ever-trust-epic-to-be-correct-nurses-raise-more-ai-concerns.html.

[8] Michael Reich, "Pay, Passengers, and Profits: Effects of Employee Status for California TNC Drivers," UC Berkeley Institute for Research on Labor and Employment, Working Paper No. 107-20 (2020).

[9] Alexandra Mateescu, "Electronic Visit Verification: The Weight of Surveillance and the Fracturing of Care," Data & Society (2021).

[10] Daniel Schneider and Kristen Harknett. "It's About Time: How Work Schedule Instability Matters for Workers, Families, and Racial Inequality," The Shift Project, Harvard University (2019); Ethan Bernstein, Saravanan Kesavan, and Bradley R. Staats, "How to Manage Scheduling Software Fairly," Harvard Business Review (December 2014).

But these types of negative impacts are not inevitable. We believe that employers can use data-driven technologies in the workplace in ways that benefit both workers and their businesses; the goal is not to block innovation. In fact, our organizations can offer many examples where technology has helped make jobs safer, opened up new skills and careers, and improved the quality of products and services. But it will take robust guardrails, of the kind that the CCPA begins to establish, to ensure that workers are not harmed by a rapidly evolving set of often unproven and untested technologies, many of which employers and even engineers themselves do not fully understand.

In what follows, we offer recommendations on the Agency's proposed regulations for Risk Assessments (Article 10) and Automated Decisionmaking Technology (Article 11), building upon the policy principles that many of us shared with the Board and Agency staff in our February 26, 2024 letter. We use the term "workers" to include employees, independent contractors, and job applicants, following the CCPA's scope in defining workplace-related personal information. Suggested deletions are in red; suggested additions are in green.

Automated Decisionmaking Technology (ADMT)

Recommendation 1: Expand the definition of Automated Decisionmaking Technology.

The data-driven transformation of the U.S. workplace is unprecedented in its speed and scope, and requires broad worker protections that respond to the range of technologies, uses, and harms. In particular, the definition of Automated Decisionmaking Technology (ADMT) will be critical to ensuring the scope of data privacy protections that the 21st Century workplace requires and that the law itself intends.

The December 2023 draft regulations defined the term ADMT to include systems that were a "whole or part of a system to make or execute a decision or facilitate human decisionmaking."[11] But the final proposed regulations revise this definition to only cover systems that "execute a decision, replace human decisionmaking, or *substantially facilitate* human decisionmaking."[12] (Italics added).

This change from "facilitates" to "substantially facilitates" creates a large opening for companies to side-step the accountability that the CPPA was charged to develop through its regulations. Essentially, an employer could self-certify itself out of coverage by the CCPA, by simply deciding that a given automated system does not "substantially facilitate" decisions by its personnel. Meanwhile, the employer could be drawing on the system to make highly consequential decisions regarding the terms and conditions of employment for its workers. But because under the proposed regulations, no one needs to be alerted that the employer is using the tool at all, neither workers nor the Agency would be able to challenge the company's unilateral determination that the automated system's role in a given decision-making process was not "substantial." In our assessment, the current narrow definition of ADMT effectively creates a self-regulation regime for employers hoping to escape regulatory oversight.

[11] December 2023 Draft Risk Assessment Regulations, Section 7001.

[12] Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies, Section 7001 (November 22, 2024).

Moreover, in practice there is significant variation in how and to what extent employers rely on automated decision-making tools.[13] Employers may use these tools to assist them, to different degrees and in combination with many other inputs, in making critical employment-related decisions. Or, they may rely on these tools to fully automate such decisions. Harms such as discrimination, invasions of privacy, overwork injuries, and suppression of the right to organize can equally result from assistive and automated management technologies. And as several recent studies document, attempting to create fine-grained distinctions between different levels of employers' reliance on these technologies is very difficult in practice, especially given that this reliance will inevitably vary from case to case.[14] In short, the full range of these use scenarios should be covered in the ADMT rights and protections being detailed in the proposed CCPA regulations.[15]

We therefore recommend that the Agency align with other areas of state policy and adopt the State Administrative Manual's (SAM) definition of Automated Decision System, in place of the current ADMT definition:[16]

> Automated Decision System: A computational process derived from machine learning, statistical modeling, data analytics, or artificial intelligence that issues simplified output, including a score, classification, or recommendation, that is used to assist or replace human discretionary decisionmaking and materially impacts natural persons. An "automated decision system" does not include a spam email filter, firewall, antivirus software, identity and access management tools, calculator, database, dataset, or other compilation of data.

As an example, this SAM definition is currently being used in deliverables stemming from Governor Newsom's Executive Order on AI, such as the state's March 2024 public sector procurement guidelines.[17] This definition is also increasingly being used in proposed legislation and by other regulatory agencies.

If the Agency does decide to adopt the SAM definition in its regulations, we recommend clarifying that "material impact" for the purposes of these regulations has the same meaning as the definitions of "significant decision" and "profiling."

Finally, we support other key definitions and coverage concepts in the proposed regulations regarding ADMTs. This includes the explication of "significant decisions" and "extensive profiling" in the employment context. These should not be narrowed in any future revisions to the proposed regulations.

---

[13] See the studies cited in Rashida Richardson, Defining and Demystifying Automated Decision Systems, *Maryland Law Review,* 81(3):785-840 (2022) and in Maria De-Arteage, et al., "A Case for Humans-in-the-Loop: Decisions in the Presence of Erroneous Algorithmic Scores," ACM CHI '20: Proceedings of the 2020 Chicago Conference on Human Factors in Computing Systems (Apr. 21, 2020).

[14] Lukas Wright, et al., "Null Compliance: NYC Local Law 144 and the Challenges of Algorithm Accountability," FAccT '24: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency, https://dl.acm.org/doi/10.1145/3630106.3658998 (June 2024). See also Data & Society, Comment on Proposed Rules for Implementation and Enforcement of Local Law 144 (January 23, 2023), https://datasociety.net/wp-content/uploads/2023/01/Data-Society-AEDT-Public-comment-1.pdf, as well as Lara Groves, et al., "Auditing Work: Exploring the New York City Algorithmic Bias Audit Regime," FAccT '24 (June 2024), https://facctconference.org/static/papers24/facct24-74.pdf.

[15] See Grace Gedye and Matt Scherer, "Are These States About to Make a Big Mistake on AI?," Politico (April 30, 2024).

[16] California Department of General Services, State Administrative Manual, Definitions - 4819.2 (last revised March 2024). Accessed at https://www.dgs.ca.gov/Resources/SAM/TOC/4800/4819-2.

[17] California Department of Technology, "State of California GenAI Guidelines for Public Sector Procurement, Uses and Training" (March 2024). Accessed at https://www.govops.ca.gov/wp-content/uploads/sites/11/2024/03/3.a-GenAI-Guidelines.pdf.

Recommendation 2: Strengthen notice and access rights for workers when an employer has used an ADMT to make a decision about them.

One of the hallmarks of the CCPA is that it recognizes the importance of transparency and disclosure in order for consumers and workers to make informed decisions about their data privacy. But currently, the biggest obstacle to ensuring responsible use of data-driven technologies in the workplace is that they are largely hidden from both policymakers and workers. Without transparency and disclosure, job applicants won't know why a hiring algorithm rejected their resume; truck drivers won't know when and where they are being tracked by GPS; and workers won't realize their health plan data is being sold. In an especially pernicious example, some employers are using surveillance to identify workers who are trying to organize a union, as well as predictive algorithms that data-mine social media to identify workers who might be *likely* to try to organize one.[18]

Given the "black box" nature of much of digital workplace technology, notice and access rights will be critical for California's workers, who need to know what types of ADMTs are being used to make critical decisions about them, including which traits or attributes the ADMTs analyze and the methods by which they measure those traits or attributes. This information is particularly important for ADMTs that require the worker to input information or otherwise interact with the ADMT, since such information is needed to ensure that workers entitled to accommodation under applicable law, such as workers with disabilities, know whether they need to request accommodation.

Equally important, once such a system has been used to make an employment-related decision, workers should have the right to know what model was used, what the inputs were, and crucially, what the outputs were and how the employer used them. Such disclosures are the first step in workers' ability to identify and challenge errors and unfair treatment. To illustrate, consumer-facing industries are increasingly incorporating customer ratings in their worker assessment systems. But we know that customer ratings are highly unreliable and carry significant risk of bias and discrimination on the basis of race, gender, accent, and other characteristics.[19] Without disclosure that these ratings have been used to evaluate them, and how, workers are left in the dark about the actual determinants of their performance evaluations.

Importantly, we do not believe that these notice requirements will be onerous on employers. For pre-use notice, the required information consists of information that companies will already have in their possession. For hiring algorithms, the notice can be given at the time of application; for incumbent workers, the notices can be automated and given to workers as part of the onboarding process and annually thereafter to remind workers of the systems in use. Similarly, notice of actual use of such systems, and workers' right to access more information about that use, can be routinized and automated, and is in line with general notice requirements already established by the CCPA.

We support the overall structure and substance of the notice and access rights; these should not be weakened in any future revisions of the regulations. That said, we recommend the following three changes to ensure that these provisions are sufficiently strong to protect workers in the use of ADMTs.

---

[18] Susan Berfield, "How Walmart Keeps an Eye on Its Massive Workforce: The Retail Giant Is Always Watching," Bloomberg BusinessWeek (November 24, 2015). For more on the importance of transparency, see also the recent guidance by the Consumer Finance Protection Bureau, "Background Dossiers and Algorithmic Scores for Hiring, Promotion, and Other Employment Decisions," Consumer Financial Protection Circular 2024-06 (October 24, 2024).

[19] Alex Rosenblat, Solon Barocas, Karen Levy, and Tim Hwang, "Discriminating Tastes: Customer Ratings as Vehicles for Bias," Data & Society (2016).

Recommendation 2.1: Expand the definition of an "adverse significant decision" triggering additional access notice requirements. The proposed regulations rightly identify key adverse decisions in the employment context, such as termination and loss of compensation. Two other types of adverse decisions should be included in this list, since they have significant impacts on workers: disciplinary actions (such as being put on probation, not being promoted, and being transferred involuntarily) and changes to working hours and shifts (which are common and can wreak havoc on the lives of low-wage women workers in particular). We recommend the following changes:

> Section 7222(k)(1)(A): Resulted in a consumer who was acting in their capacity as a student, employee, or independent contractor being denied an educational credential; having their compensation decreased~~, or~~; being suspended, demoted, terminated, disciplined, or expelled; having changes to work hours and shift assignments; or

Recommendation 2.2: Reinstate the requirement that allows a worker to access aggregate outputs relevant to the use of an ADMT with respect to the worker. A key component of transparency and disclosure of ADMT use in the workplace setting is providing aggregate comparison data so that workers can understand the context in which their own data was analyzed. We therefore recommend the following changes to Section 7222(b)(4):

> (4) How the automated decisionmaking technology worked with respect to the consumer. At a minimum, this explanation must include subsections (A)~~, and~~ (B) and (C):
>
> (A) How the logic, including its assumptions and limitations, was applied to the consumer; ~~and~~
> (B) The key parameters that affected the output of the automated decisionmaking technology with respect to the consumer, and how those parameters applied to the consumer.
> (C) ~~A business also may provide the range of possible outputs or aggregate output statistics to help a consumer understand how they compare to other consumers. For example, a business may provide the five most common outputs of the automated decisionmaking technology, and the percentage of consumers that received each of those outputs during the preceding calendar year.~~ A simple and easy-to-use method by which the consumer can obtain the range of possible outputs, which may include aggregate output statistics (for example, the five most common outputs of the automated decisionmaking technology, on average, across all consumers during the preceding calendar year, and the percentage of consumers that received each output during the preceding calendar year).

Recommendation 2.3: Clarify that a worker has the right to use an authorized representative to access information relevant to the use of an ADMT with respect to the worker. The ability of workers to exercise their rights under the CCPA will depend crucially on their ability to designate representatives to act on their behalf, including unions and other worker organizations, since research has shown that accessing data rights can be challenging to navigate, especially for individuals who may lack the resources or expertise.[20] We therefore recommend the following provision be added to Section 7222.

[20] Jef Ausloos and Pierre Dewitte, "Shattering One-Way Mirrors – Data Subject Access Rights in Practice." International Data Privacy Law 8, no. 1 (February 1, 2018).

A consumer may use an authorized agent to submit a request to access information about a business's use of an automated decisionmaking technology on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf.

Recommendation 3: Restore a meaningful right for workers and consumers to opt-out of consequential ADMT systems.

A key hallmark of the CCPA is that it establishes a baseline level of agency for consumers and workers, such as the right to correct their data or to opt-out of the sale or sharing of their data. The proposed CCPA regulations detail several additional touchpoints for personal agency that will be especially important to workers. In particular, workers should have the right to opt-out of harmful, consequential, or especially intrusive automated decision-making systems, just as consumers do. There are important policy precedents for this approach.

For example, a range of public policies and collective bargaining agreements in the U.S. and other countries recognize the importance of allowing workers to refuse to work in conditions that are harmful to their physical or mental health.[21] In leading privacy policy models, highly consequential decisions require human review and can not be automated; an example in the workplace context is that workers should be able to opt-out of or challenge the use of automated hiring and firing systems, given their significant economic impact.[22] Similarly, workers should have the right to preserve their privacy against highly intrusive monitoring systems by opting out of them. For example, the ubiquity of electronic monitoring and data collection systems have increased the ability of employers to monitor workers off-duty, including social media eavesdropping.[23] And in the retail industry, vendors have developed software that mines data from workers' social media accounts to predict whether a job candidate will become a whistleblower.[24]

Unfortunately, the proposed regulations effectively eliminate the ability for workers to protect themselves by opting-out of consequential ADMT systems. The December 2023 draft regulations provided consumers with opt-out rights for uses of ADMTs to make decisions that produce "legal or similarly significant effects."[25] The revised draft adds a complex series of exceptions to those opt-out rights specifically for workers, and more generally for consumers, and the impact will be to undermine their agency over how they are tracked, profiled, evaluated, and potentially harmed by algorithmic tools.

---

[21] For examples of policies and collective bargaining provisions establishing workers' right to refuse unsafe work, see "Collective Bargaining Language - Health and Safety Rights," Labor Occupational Health Program, University of California, Berkeley (2024). For an overview of the negative mental health impacts of electronic monitoring, see Lisa Kresge and MT Snyder, "35 Years Under Electronic Monitoring and Still Waiting for Worker Rights," UC Berkeley Labor Center (2023).

[22] Many AI principles frameworks, including the White House's Blueprint for an AI Bill of Rights, include some version of the right to opt-out of automatic decision-making systems that pose significant risks or harms, especially in sensitive domains including employment. For example, Article 22 of the GDPR establishes an individual's right not to be subject to a consequential decision based solely on automated data processing.

[23] Richard Bales and Katherine Stone, "The Invisible Web at Work: Artificial Intelligence and Electronic Surveillance in the Workplace," Berkeley Journal of Employment & Labor Law 41 (1) (2020).

[24] See for example, https://fama.io/retail-hospitality/.

[25] See December 2023 Draft Risk Assessment Regulations, Section 7030.

Ultimately, legislation will be needed to fully protect the rights of workers and consumers in California in the use of ADMTs. In the meantime, our recommendations in this section are intended to restore a meaningful right for workers and consumers to opt-out of consequential ADMT systems, consistent with the language and purpose of the CCPA.

Recommendation 3.1: Add guardrails on the "security, fraud prevention, and safety exception" to prevent businesses from misusing it. Businesses can readily misclassify or misuse the results of ADMTs as evidence of "fraud" or "dishonesty," harming California consumers and workers.[26] First, we recommend the business must show that its use of ADMT under this exception is both "strictly necessary" and "proportionate." Both are well-established principles under the GDPR.[27] Second, consumers must have a right to a written explanation for why the ADMT is strictly necessary and proportionate so they can act as whistleblowers in case of a business's misuse of this exception. Third, in the case of allegations for fraud or dishonesty, businesses should be required to make their allegations with specificity—a long-standing legal principle to deter non-meritorious fraud allegations and to ensure that the party charged with fraud can intelligently respond to the allegations.[28] This is particularly important in the ADMT context, in which workers are likely to be at a heightened informational disadvantage in comparison to the business that made the ADMT decision.[29] Specifically, we recommend that Section 7221 (b)(1) be revised as follows:

(1) If all of the following are true: ("security, fraud prevention, and safety exception")
  (A) The business's use of that automated decisionmaking technology is proportionate and strictly necessary to achieve, and is used solely for, the security, fraud prevention, or safety purposes listed below:
    (i) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information;
    (ii) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions; or
    (iii) To ensure the physical safety of natural persons.
  (B) The consumer has a right to request to obtain, pursuant to the procedures in Section 7222, a sufficiently precise and adequately substantiated explanation of why the business's use of automated decisionmaking technology is strictly necessary and proportionate to accomplish the allowable purpose as specified in Section 7221(b)(1)(A).
  (C) For any decision concerning a consumer as set forth in Section 7221(b)(1) that involves allegations of fraud or dishonesty by the consumer, the business must provide, in writing, specific details on any allegations of fraud or dishonesty and provide the consumer with an opportunity to appeal such allegations.

---

[26] For example, in the context of online labor platforms, a business's failure to correctly recognize a worker using facial recognition software can be characterized by the business as fraudulent use of the platform, which can lead to the worker's suspension or termination. See, e.g., "Uber's Anti-Fraud Systems and the Failure of Human Review," Worker Info Exchange, May 14, 2021; "Road to Nowhere," Chicago Gig Alliance and the People's Lobby, 2023, p. 5.

[27] See, e.g., GDPR, Recital 47 and European Data Protection Supervisor.

[28] See, e.g., *Committee on Children's Television v. General Foods Corp.* (1983) 35 Cal.3d 197, 216–217 ("*Committee on Children's Television*").

[29] Sara Baiocco, Enrique Fernández-Macías, Uma Rani and Annarosa Pesole, "The Algorithmic Management of Work and its Implications in Different Contexts," JRC Working Papers Series on Labour, Education and Technology 2022/02, p. 22 (noting the information asymmetries and power imbalances that arise between management and workers in the context of algorithmic management).

Recommendation 3.2: Eliminate the overly broad "hiring," "allocation/assignment of work and compensation," and "work profiling" exceptions under Sections 7221(b)(3), (b)(4), and (b)(5). These exceptions only require a company to assert that the ADMT in question is "necessary" to achieve some purpose, and to evaluate in some undefined way the ADMT for accuracy and non-discrimination (the latter is no added protection at all, since these anti-discrimination protections are already provided for under Sections 7152(a)(5) and 7152(a)(6) in the proposed regulations.[30] Such vague and broad categorical exceptions threaten to deprive workers of agency over algorithmic tools that can have significant impacts on their work and livelihoods, as well as their right to protect their personal data.

Recommendation 3.3: Strengthen the human review and appeal requirements under the "human appeal exception." We recommend significant strengthening of the human appeal exception, on three fronts. First, by only requiring that the human reviewer be "qualified" and "have the authority to overturn the decision," the proposed regulations insufficiently mitigate the risks of partiality and of human reviewers excessively deferring to algorithmic decisionmaking, given that the same business will be both making and evaluating the appeal of the ADMT decision. We therefore recommend two requirements derived from the European Union Platform Directive: (1) mandating that the business allocate sufficient human resources to ensure effective appeals for the decision, and (2) expressly protecting human reviewers from retaliation for overturning ADMT decisions.[31] We also recommend training, impartiality, anti-bias, and conflict of interest-related protections. These protections are derived from Title IX, which can serve as a comparable regulatory framework that significantly relies on internal dispute resolution systems.[32]

Second, the proposed regulations make it unnecessarily onerous for consumers to pursue an appeal. Given that many consumers will face significant barriers in the ADMT appeal process—language, disability, literacy, etc.—the proposed regulations should expressly authorize that a business must permit the consumer to be represented by an authorized agent or advisor of their choice.[33] We also identify several additional procedural protections to deter arbitrary decisonmaking by the business.[34]

Third, in the event that a human reviewer finds that a covered ADMT decision has infringed upon the rights of a consumer, we recommend that the business be required to undertake certain actions to deter and prevent such erroneous decisions in the future. This recommendation is modeled on the European Platform Directive.[35]

Specifically, we recommend that Section 7221(b)(2) be revised as follows:

(2) For any significant decision concerning a consumer as set forth in Section 7200, subsection (a)(1), if the business provides the consumer with a method to appeal the decision to a qualified human reviewer who is required to objectively evaluate all relevant evidence and has the authority to overturn the decision ("human appeal exception"). To qualify for the human appeal exception, the business must do the following:

(A) The business must designate a human reviewer who:

[30] Specifically, Section 7152(a)(5)(B) requires the business, as part of its mandated risk assessment, to identify "[d]iscrimination upon the basis of protected classes that would violate federal or state antidiscrimination law." Section 7152(a)(6) requires the business to identify the safeguards that it plans to implement to address discrimination and other potential negative impacts.
[31] E.U. Platform Directive, Article 10.2.
[32] See, e.g, 34 C.F.R. § 106.45(d)(3)(iii)-(iv); 34 C.F.R. § 106.8(d)(2).
[33] See, e.g., 34 C.F.R. § 106.46(c)(1)(ii).
[34] 34 C.F.R. § 106.45(h)(2); see also E.U. Platform Directive, Art. 11.1, 11.2.
[35] E.U. Platform Directive, Article 11.3.

(i) Is trained and qualified to understand the significant decision being appealed, ~~and~~ the consequences of the decision for the consumer, how to evaluate the decision, and how to serve impartially, including by avoiding prejudgment of the facts at issue, conflict of interest, and bias;

(ii) Does not have a conflict of interest or bias for or against the business or the consumer generally, or against the business or consumer specifically;

(iii) Was not involved in the initial decision being appealed;

(iv) Must enjoy protection from dismissal or its equivalent, disciplinary measures, or other adverse treatment for exercising their functions under this section; and

(v) Must be allocated sufficient human resources by the business to conduct an effective appeal of the decision.

(B) This human reviewer must consider the relevant information provided by the consumer in their appeal and may consider any other sources of information about the significant decision.

(C) The business must clearly describe to the worker how to submit an appeal and enable the worker to submit corrections or otherwise provide information, evidence, and a written statement in support of or challenging the outcome, for the human reviewer to consider as part of the appeal.

(i) The method of the appeal must also be easy for the workers to execute, require minimal steps, and comply with sections 7004 and 7020.[36]

(ii) The business must permit the worker to be represented by an authorized agent or advisor of their choice, who may be, but is not required to be an attorney.

(iii) In responding to the appeal, the business must provide the consumer with a sufficiently precise and adequately substantiated reply in the form of a written document, describing the result and explaining the reasons for its decision, which may be in electronic format.

(iv) In the event that the significant decision in paragraph (b)(2) of this section is found by the human reviewer to have infringed on the rights of the consumer, the business shall rectify that decision without delay and in any case within fourteen calendar days of the finding by the human reviewer. The business shall also take the necessary steps in order to avoid such decisions in the future, including, if appropriate, a modification of the ADMT or a discontinuance of its use.

Recommendation 3.4: Require ex-ante human review and expedited appeals for "highly-consequential decisions" when claiming the human appeal exception. A majority of Americans consistently report that they are uncomfortable with the use of artificial intelligence in high-stakes decisions about their lives.[37] Especially when it comes to consequential decisions like the loss of one's job, workers should have a right to human review *before* an ADMT-assisted decision takes place – not afterwards, when a harm may already have occurred. Research indicates that when using an automated system, people are biased towards accepting the outcomes the system produces even when other factors indicate that the results

[36] Consistent with this reference to Section 7020, we also recommend that Section 7020 be revised so that the same methods which currently apply to the submission of requests to know, delete and correct also apply to the submission of requests to appeal ADMT.

[37] Consumer Reports, Survey, Jul. 25, 2024.

are wrong, undermining the protections of a human appeal process.[38] In light of these risks, we recommend a stronger set of requirements for businesses who wish to claim the human appeal exception when using ADMTs to make highly-consequential decisions about their workers. In these cases, human review should be required before the decision is made.

Specifically, we recommend that the following new Section 7221(b)(2)(D) be added for "highly-consequential decisions":

(D) For uses of ADMTs in making hiring, firing, disciplinary, or compensation-related decisions as set forth in Section 7200(a)(1)(B)(i)-(iv) ("highly consequential decisions"), the business must in addition do the following in order to claim the "human appeal exception":
  (i) The business must conduct its own evaluation of the consumer before making the highly consequential decision, independent of the output used from the ADMT.
  (ii) This includes establishing meaningful human oversight by a designated internal reviewer to corroborate the ADMT output by other means. Meaningful human oversight requires that the designated internal reviewer meet the following conditions:
    1. The designated internal reviewer is granted sufficient authority, discretion, resources, and time to corroborate the ADMT output;
    2. The designated internal reviewer has sufficient expertise in the operation of similar systems, and a sufficient understanding of the ADMT in question to interpret its outputs as well as results of relevant risk assessments; and
    3. The designated internal reviewer has education, training or experience sufficient to allow the reviewer to make a well-informed decision.
  (iii) Where a business cannot corroborate the ADMT output produced by the ADMT, the business is prohibited from relying on the ADMT to make the highly-consequential decision.
  (iv) When a business can corroborate the ADMT output and makes the highly-consequential decision, the business must notify the consumer of the consumer's right to appeal, as described in proposed Section 7221(b)(2)(C) above. All information and judgments involved in the business's corroboration of the ADMT output must be communicated to the consumer as part of this appeal notification, and the business must follow the appeal response timelines for highly consequential decisions set forth in Section 7021(b).

Recommendation 3.5: Shorten the appeal timelines for the "highly consequential ADMT decisions" (as defined in Recommendation 3.4). The proposed regulations currently allow a business between 45 and 90 days to process an appeal of an ADMT decision. Considering that more than half of Americans live paycheck to paycheck, this timeline could result in significant economic harm in the context of a highly consequential ADMT decision like a firing, suspension, or demotion.[39] We recommend a two-week deadline for a business to respond to a consumer's appeal of a highly consequential ADMT decision. This

[38] This bias can make human oversight ineffective at curbing the worst harms of ADMT, as the human meant to act as a final judge will often take the system's output as preferable to their analyses, even disregarding evidence to the contrary.Mary L. Cummings, *Automation and Accountability in Decision Support System Interface Design*, 32 J. Tech. Stud. 23, 25 (2006). See also Saar Alon-Barkat and Madalina Busuioc, *Human–AI Interactions in Public Sector Decision Making: "Automation Bias" and "Selective Adherence" to Algorithmic Advice*, 33 J. Pub. Admin. Rsch. and Theory 153, 155 (2022) ("Automation bias refers to undue deference to automated systems by human actors that disregard contradictory information from other sources"), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3794660.

[39] United States Interagency Council on Homelessness. "Data and Trends." https://www.usich.gov/guidance-reports-data/data-trends.

is modeled on the European Union's Platform Directive.[40] Specifically, we recommend that Section 7021(b) be revised as follows:

> (b) Businesses shall respond to a request to appeal a highly consequential ADMT under Section 7221(B)(2)(D) no later than 14 calendar days after receipt of the request. For all other requests, b~~B~~usinesses shall respond to a request to delete, request to correct, and request to know, request to access ADMT, and request to appeal ADMT no later than 45 calendar days after receipt of the request . . . . [same]

Recommendation 3.6: Expressly prohibit businesses from retaliating against consumers who have exercised their access and appeal rights. Retaliation by businesses on such opt-out grounds is clearly prohibited under Civil Code Section 1798.125, subdivisions (a)-(b).[41] This recommendation is consistent with the rationale provided in the October 2024 Draft Initial Statement of Reasons, which states that the addition of subdivision (l) is to "facilitate[] compliance with the [CCPA's] statutory prohibition against retaliation …. [by] consolidat[ing] the relevant requirements for the right to opt-out of ADMT in one place."[42] Specifically, we recommend that Section 7221(l) be revised as follows:

> (l) A business must not retaliate against a consumer because the consumer exercised their opt-out right, including, but not limited to, their right to opt-out of the use of an ADMT, their right to access details about an ADMT-assisted decision, or their right to appeal an ADMT-assisted decision, as set forth in Civil Code Section 1798.125 and Article 7 of these regulations.

Risk Assessments

The proposed regulations detail an important set of procedures for providing notice of risk assessments of data collection and automated decision-making systems. Such assessments are widely considered a critical tool for identifying and mitigating harmful impacts of digital technologies.[43] In the workplace context, conducting risk assessments prior to use will be absolutely critical; it is not fair to workers to wait until invasions of privacy and other harms have already occurred to begin regulatory oversight. Moreover, conducting risk assessments prior to use also helps to identify potential design flaws and harms early on, when they are easier and less costly for developers and employers to address.[44] Here too we do not believe these requirements to be onerous for employers, because the proposed regulations include an exemption for routine administrative data processing.

Recommendation 4: Strengthen the required elements of risk assessments.

The proposed regulations deliver a critical framework for ensuring that businesses consider the risks posed to consumers and workers by the use of automated decisionmaking technology. The regulations

---

[40] E.U. Platform Directive, 11.1, 11.2.

[41] These subdivisions broadly prohibit businesses from discriminating or retaliating against a consumer "because the consumer exercised any of the consumer's rights under this title." Cal. Civ. Code § 1798.125, subd. (a)(1).

[42] "Draft Initial Statement of Reasons," California Privacy Protection Agency, Oct. 4, 2024, p. 91.

[43] Emanuel Moss, et al., "Assembling Accountability: Algorithmic Impact Assessment for the Public Interest," Data & Society (2021); Daniel J. Solove, "Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data," Northwestern University Law Review 118 (2024).

[44] Henriette Cramer, et al., "Assessing and Addressing Algorithmic Bias in Practice," Interactions 25, no. 6 (October 25, 2018); Andrew Selbst, "An Institutional View of Algorithmic Impact Assessments," Harvard Journal of Law & Technology 35, no. 1 (2021).

contain key elements to making risk assessments a meaningful part of protecting the privacy and rights of working people. In order to ensure that the proposed regulations clearly communicate safeguards put in place by businesses, the reported purposes of ADMTs, and the categories of harms that could still impact people in the workplace, there are several sections that could be enhanced. To ensure greater transparency and accountability to workers, we recommend reinstating several elements of the December 2023 draft of the regulations outlined below.

Recommendation 4.1: Explicate the worker harms that risk assessments must test for. It is important to understand that while automated hiring systems have captured the most attention in public debate, they are only the tip of the iceberg. Employers' use of data-driven technologies happens throughout the entire employment lifecycle – and negative effects on privacy, race and gender equity, and other important aspects of employment can result throughout. Important employment-related decisions include hiring and recruitment; setting of wages, benefits, hours, and work schedules; performance evaluation, promotion, discipline, and termination; job assignments, productivity requirements, and workplace health and safety; decisions that result in job augmentation, automation, and access to upskilling opportunities; and other terms or conditions of employment. In order to ensure that the proposed regulations clearly communicate how the existing categories of harms might manifest in the workplace, we recommend the following edits to Section 7152(a)(5):

> (D) Coercing or compelling consumers into allowing the processing of their personal information, such as by conditioning consumers' acquisition or use of an online service upon their disclosure of personal information that is unnecessary to the expected functionality of the service, or requiring consumers to consent to processing when such consent cannot be freely given, for example as a condition of employment.
>
> (F) Economic harms, including but not limited to limiting or depriving consumers of economic opportunities via firing, discipline, or denial of promotion, reducing compensation, task or job automation, or reclassification of workers' employment status; charging consumers higher prices; compensating consumers at lower rates; or imposing additional costs upon consumers, including costs associated with the unauthorized access to consumers' personal information.
>
> (G) Physical harms, to consumers or to property, including processing that creates the opportunity for physical or sexual violence, or physical harms stemming from productivity management systems that speed up the rate of work to the point of injury.
>
> (I) Psychological harms, including emotional distress, stress, anxiety, embarrassment, fear, frustration, shame, and feelings of violation. Psychological harm includes, for example, emotional distress resulting from disclosure of non consensual intimate imagery; stress and anxiety from regularly targeting a consumer who visits websites for substance abuse resources with advertisements for alcohol; stress resulting from pervasive surveillance at work or automated productivity quotas; or emotional distress from disclosing a consumer's purchase of pregnancy tests or emergency contraception for non-medical purposes.

We also recommend reinstating the following provision from the December 2023 draft regulations:

> Constitutional harms, such as chilling or deterring consumers' free speech or expression, political participation, religious activity, free association, freedom of belief, freedom to explore ideas, or reproductive freedom; and harms to consumers' ability to engage in collective action or that impede the right to unionize.

Recommendation 4.2: Strengthen the safeguards against harmful ADMTs that businesses are required to disclose. As the proposed regulations already identify in Section 7152(a)(5), the potential negative impacts associated with the processing of personal information include discrimination, but also a range of other potential harms. Section 7152 (a)(6)(B) in the proposed regulations should therefore pertain to all of the harms identified in risk assessments, rather than only discrimination based on protected classes. We recommend these additions to Section 7152 (a)(6)(B):

> (B) For uses of automated decisionmaking technology set forth in section 7150, subsection (b)(3), the business must identify the following:
>
> > (i) Whether it evaluated the automated decisionmaking technology to ensure it works as intended for the business's proposed use and does not discriminate based upon protected classes or contribute to other negative impacts to consumers' privacy set forth in Section 7152(a)(5) ("evaluation of the automated decisionmaking technology"); and
> >
> > (ii) The policies, procedures, and training the business has implemented or plans to implement to ensure that the automated decisionmaking technology works as intended for the business's proposed use and does not discriminate based upon protected classes or contribute to other negative impacts to consumers' privacy set forth in Section 7152(a)(5) ("accuracy and nondiscrimination safeguards").

We also recommend the following addition to Section 7152(a)(6), to ensure that workers and consumers have a better understanding of the risks that may impact them:

> The business must specifically identify how these safeguards address the negative impacts identified in subsection (a)(5). The business must specifically identify how these safeguards address the negative impacts identified in subsection (a)(5), including to what extent they eliminate or reduce the negative impacts; whether there are any residual risks remaining to consumers' privacy after these safeguards are implemented and what these residual risks are; and identify any safeguards the business will implement to maintain knowledge of emergent risks and countermeasures.

Recommendation 4.3: Require businesses to be more clear about the purpose of ADMTs. Section 7152(a)(1) in the proposed regulations states: "The business must specifically identify its purpose for processing consumers' personal information." We recommend strengthening this disclosure by reinstating several clarifications present in the December 2023 draft regulations, as follows:

> The business must specifically identify its purpose for processing consumers' personal information, how the processing achieves that purpose, and the purpose's compatibility with the context in which the personal information was collected. The purpose must not be identified or described in generic terms, such as "to improve our services" or for "security purposes."

Recommendation 4.4: Strengthen the required disclosure of risk assessments by increasing transparency around the lack of external party consultation. Reinstating provision Section 7151(b)(1) from the December 2023 draft of the regulations would ensure that businesses explain why they chose not to engage external stakeholders. We recommend reinstating this provision:

> For the uses of automated decisionmaking technology or artificial intelligence set forth in Section 7150, subsections (b)(3) and (b)(4), if the business has not consulted external parties in

its preparation or review of the risk assessment, the risk assessment shall include a plain language explanation addressing why the business did not do so and which safeguards it has implemented to address risks to consumers' privacy that may arise from the lack of external party consultation.

Recommendation 5: Clarify the role of workers and unions in risk assessments.

There is growing consensus among technology researchers that workers are important stakeholders that should be involved when their employers conduct risk assessments, whether of data collection systems or of automated decision-making systems.[45] That is both a matter of principle, but also a matter of good practice. Workers have a significant amount of firm-specific knowledge and experience to bring to the table; their input can be vital for assessing and implementing new technologies.[46]

A good example of the importance of worker involvement comes from new technologies in the hotel industry that automate housekeeper tasks and can result in inefficient orderings of rooms that do not take into account cart proximity or input from workers. As a result, workers may have to push heavy cleaning carts across significantly greater distances and may be penalized for not meeting their room quota.[47] But an innovative collaboration between engineers at Carnegie Mellon University and hotel workers and their union resulted in a system redesign that would increase worker discretion, foster collaboration and communication, and reduce workloads.[48]

The proposed regulations do not explicitly give workers and unions a role in risk assessments. While the proposed regulations could be read to imply that workers and unions should be consulted, we recommend the addition of the following text to Section 7151(a), to acknowledge the unique position and interests of workers and their unions.

In addition, when performing risk assessments of the processing of worker personal information or automated decisionmaking technologies impacting workers, a business should meaningfully consult with employees, independent contractors, and, if applicable, their exclusive bargaining representatives, including through participatory design, involvement in the identification of potential harms, and soliciting and incorporating feedback. These risk assessments should then be shared with employees, independent contractors, and, if applicable, their exclusive bargaining representatives.

[45] See Amanda Ballantyne, Jodi Forlizzi, and Crystal Weise, "A Vision for Centering Workers in Technology Development," Issues in Science and Technology (Fall 2024), and Thomas Kochan, et al. "Bringing Worker Voice Into Generative AI," Institute for Work and Employment Research, MIT Sloan School of Management (December 21, 2023).
[46] Adam Seth Litwin, "Technological Change at Work: The Impact of Employee Involvement on the Effectiveness of Health Information Technology," ILR Review 64, no. 5 (October 2011).
[47] Juliana Feliciano Reyes, "Hotel Housekeeping on Demand: Marriott Cleaners Say this App Makes their Job Harder," The Philadelphia Inquirer (July 2, 2018).
[48] Franchesca Spektor, et al., "Designing for Wellbeing: Worker-Generated Ideas on Adapting Algorithmic Management in the Hospitality Industry," Proceedings of the 2023 ACM Designing Interactive Systems Conference, 623–37 (2023).

Recommendation 6: Strengthen the power of the CPPA to act on risk assessments.

The risk assessment framework of the proposed regulations does not currently provide a clear regulatory mechanism for the Agency to disagree with a company's certification that the benefits of some processing activity outweigh the costs. This lack of authority risks hobbling the Agency's ability to prevent the most egregious privacy violations revealed by a business's risk assessment.

Risk assessments are required by the CCPA for a simple reason: when the costs associated with processing consumers' personal information outweigh the benefits, the processing should be restricted or prohibited outright. As the statute makes explicit, risk assessments weigh the risks "with the goal of restricting or prohibiting such processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public."

Regulations that only require risk assessments to be prepared by businesses and maintained internally are insufficient to protect the autonomy and dignity of the public from processing activities that do not meet the legal standard. Imagine a processing activity that risks significant harm to vulnerable consumers—like people searching for housing or employment—but which is marginally profitable for a business. When a business self-certifies that the processing's benefits outweigh the costs, it is the Agency's role under the statute to review the certification and the supporting analysis and determine whether it properly performs the cost-benefit analysis. If it does not, then the processing, under the CCPA, must be restricted or prohibited (see Civil Code § 1798.185(a)(15)(B)).

We propose the following language, based on the statutory damages provisions in § 1798.155(a), creating an explicit mechanism for the Agency to question and take action against deficient risk assessments:

> Upon review of a business's Risk Assessment, if the Agency has a cause to conclude that the benefits of the processing do not outweigh the costs as required by statute, the Agency may require additional documentation or evidence from the business. If the Agency determines, after reviewing any further materials as necessary, that there is probable cause for believing that the benefits of the processing do not outweigh the costs in violation of the statute, the Agency may hold a hearing pursuant to Section 1798.199.55(a) to determine if a violation has occurred. If the Agency so determines that a violation has occurred, it may issue an order requiring the violator to restrict the processing to address such costs or prohibiting the business from such processing.

***

The U.S. workplace is rapidly becoming a major site for the deployment of AI and other digital technologies, a trend that will only escalate going forward. Full coverage and protection by the CCPA is a critical first step to ensure that California workers have the tools necessary to advocate for their rights in the 21st century data-driven workplace.

Thank you for the opportunity to provide feedback during this important rulemaking process,

Sincerely,
The signed organizations and individuals

Organizations:

Alphabet Workers Union - CWA Local 9009
American Civil Liberties Union California Action
American Federation of Musicians Local 7
Athena Coalition
California Coalition for Worker Power
California Conference Board of the Amalgamated Transit Union
California Conference of Machinists
California Employment Lawyers Association
California Federation of Labor Unions
California Immigrant Policy Center
California Nurses Association/National Nurses United
California School Employees Association
California Teamsters Public Affairs Council
CFT, A Union of Educators and Classified Professionals
Communications Workers of America (CWA)
Coworker
Data & Society
Distributed AI Research Institute
Economic Security California Action
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Equal Rights Advocates
Gig Workers Rising
Human Impact Partners
IBEW 569
Labor Occupational Health Program, UC Berkeley
Los Angeles Alliance for a New Economy (LAANE)
National Domestic Workers Alliance
National Employment Law Project
PowerSwitch Action
SAG-AFTRA
SEIU California
Strippers United
Surveillance Technology Oversight Project
TechEquity
TechTonic Justice
The Sidewalk Project
UC Berkeley Labor Center
UC San Diego Labor Center
UDW/AFSCME Local 3930
United Food and Commercial Workers (UFCW) Western States Council
United for Respect Education Fund
Upturn
Worksafe
Writers Guild of America West

Individuals (organizations listed for identification purposes only):

Zarreen Amin (SEIU-UHW)
Sameer Ashar (UC Irvine Workers, Law, and Organizing Clinic)
Christina Chung (Center for Law and Work, Berkeley Law School)
NatsHoney Clark (Strippers United)
Andrea Dehlendorf
Veena Dubal (University of California, Irvine School of Law)
Sarah Fox (Carnegie Mellon University)
Ifeoma Ozoma (Earthseed)
Seema Patel (UC College of the Law, San Francisco [formerly UC Hastings])
Kevin Riley (UCLA Labor Occupational Safety and Health Program)