American Arbitration Association and
Center for Labor and Employment Law
New York University School of Law

Employment Arbitration and Mediation Today

March 16, 2026

Artificial Intelligence and Employee Monitoring:

Big Brother is an Algorithm Named Julie, and She's Hiring, Watching and Rating You

Jonathan Ben-Asher
Ritz Clark & Ben-Asher LLP
One Liberty Plaza - 23rd floor
165 Broadway
New York, N.Y. 10006
(212) 321-7075
Jben-asher@RCBALaw.com
www.RCBALaw.com

Contents

Introduction

The workplace of 2026 would be unrecognizable to a visitor from 1990. Employees routinely working from home with instant, unending electronic access to each other, their employer's documents, and a gargantuan encyclopedia of information a click away -- these would all bewilder our work-life ancestors. They would be flummoxed by how we interact with applications and algorithms -- both intentionally and unknowingly -- as if they were our human colleagues down the hall. And they would probably be aghast at how we apply for jobs and have our qualifications judged by algorithms, and how employers can incessantly track and monitor their employees' every working moment and evaluate their performance using AI tools.

This paper discusses two major issues for employees arising out of our current technology: artificial intelligence and employee monitoring.

I. Artificial intelligence

Artificial intelligence refers to systems that use data and computational techniques to make decisions or assist people in making them. AI tools use large amounts of data to detect patterns, and then use those patterns to predict outcomes in new situations. Pauline T. Kim and Matthew T. Bodie, Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy, *ABA Labor and Employment Law Journal*, June 2021, at 290.

We use artificial intelligence (or artificial intelligence uses us) when we "talk" with an automated voice on a phone call (which pauses embarrassedly and says, "I'm sorry… I didn't get

that…"), "chat" with a smiling robot on a website ("Hi! I'm Kaitlin. How can I help you today?") and ask it to analyze or draft complex documents.

As employers increasingly use AI to handle tasks currently done by human beings, the impact on global employment may become apocalyptic, particularly because of the tremendous power of generative AI tools. Generative AI can scan, analyze and use vast amounts of data (i.e. the entire Internet) to produce content that can rival writing and images created by humans. A 2023 Goldman Sachs study concluded that about two-thirds of current jobs are exposed to some degree of AI automation, and generative AI could substitute for up to one-fourth of current work. Globally, AI could expose the equivalent of 300 million full-time jobs to automation. Goldman Sachs Economics Research, *The Potentially Large Effects of Artificial Intelligence on Economic Growth*, March 26, 2023. https://www.gspublishing.com/content/research/en/reports/2023/03/27/d64e052b-0f6e-45d7-967b-d7be35fabd16.html

Other observers are less apocalyptic, arguing that AI will create more other new positions, although noting that that job losses and the commodification of labor will lead to reduced wages and more insecurity for workers. *What if Labor Becomes Unnecessary*, New York Times Roundtable, February 4, 2026. https://www.nytimes.com/2026/02/04/opinion/ai-jobs-employment-industry.html?unlocked_article_code=1.JlA.h-Zs.2yxmDuFhAaX-&smid=url-share

A side effect of AI is that the work of annotating the vast amounts of data it uses is performed by underpaid workers in developing countries, who are often cheated out of their pay. As the Washington Post explained, "While AI is often thought of as human-free machine learning, the

technology actually relies on the labor-intensive efforts of a workforce spread across much of the Global South and often subject to exploitation." Washington Post, *Behind the AI boom, an army of overseas workers in 'digital sweatshops,* August 28, 2023.

Employers have leapt at the chance to use AI to recruit, screen, interview and rate job candidates and evaluate employees' performance. More than 90 percent of employers use some form of automated system to filter or rank job applicants. World Economic Forum, *Hiring Doesn't Have to be So Inhumane*, March 28, 2025, https://www.weforum.org/stories/2025/03/ai-hiring-human-touch-recruitment/.

A 2025 survey found that 6 in 10 managers rely on AI to make decisions about their direct reports, and that the overwhelming majority of them use AI to determine layoffs, promotions, and raises. Unfortunately, two thirds of the managers using AI to manage employees have not been given any formal AI training. More than half were told to determine if AI could replace their reports. Resume Builder, *Half of Managers Use AI To Determine Who Gets Promoted and Fired*, June 30, 2025 https://www.resumebuilder.com/half-of-managers-use-ai-to-determine-who-gets-promoted-and-fired/

Employers argue that in these contexts, AI saves time and reduces costs, is better than humans at predicting performance and evaluating job candidates, and, unlike humans, isn't subject to bias in decision making. Whatever the savings in time and cost, AI presents tremendous problems for job seekers and employees and can erect discriminatory barriers.

A. AI in sourcing and hiring

As a first step in recruitment, employers use AI to find candidates who may be in the job market. How important is this? 90 percent of recruiters look for candidates on LinkedIn, which contains more than 50 million companies. Two-thirds of employers research potential candidates using social media, and a survey found that more than half had disqualified a candidate because the employer disagreed with something in a candidate's social media profile. Surprising Social Media Recruiting Statistics, https://www.apollotechnical.com/social-media-recruiting-statistics/.

1. AI in recruiting ads on social media

LinkedIn and Facebook enable companies advertising job openings to target specific audiences, using both the criteria the advertiser has established and the platform's algorithms, which decide who sees which ads. Outside auditors seeking to determine whether a platform's algorithm is reliable, fair or discriminatory are hampered because "they investigate the platform's algorithms as a black-box, without access to the code or inputs of the algorithm, or access to the data or behavior of platform members or advertisers." Auditing for Discrimination in Algorithms Delivering Job Ads, International World Wide Web Conference Committee, 2021, https://ant.isi.edu/datasets/addelivery/Discrimination-Job-Ad-Delivery.pdf. The authors of the study identified several ways that a platform can skew an ad with potentially discriminatory effects:

1. An advertiser can select a platform's targeting options and an audience in a way that skews the results.

2. A platform can choose options in its ad delivery optimization algorithm to increase the ad's relevance, which skews results. For example, "if an image used in an ad receives better engagement from a certain demographic, the platform's algorithm may learn this association and preferentially show the ad with that image to the subset of the targeted audience belonging to that demographic."

3. Other factors, such as the time of day or competition among advertisers, may skew results. An ad may reach more men than women, because more men than women are on the site at a particular time. Id. at 2-3.

Of course, advertisers have always worked hard to direct ads to a particular demographic. The many drug ads on CNN target a very different audience than ads for American Eagle on Instagram. But Title VII prohibits employers from categorizing job applicants using discriminatory criteria, and that includes job ads. It precludes employers from publishing ads that "indicate a preference, limitation, specification, or discrimination" based on a forbidden characteristic. 42 U.S.C. § 2000e-3(b). The ADEA has a similar prohibition of ads that indicate an age preference. 29 U.S.C. § 623(e).

In 2019, Facebook reached a settlement in a case where five civil rights groups alleged that its algorithms discriminated against women and older job seekers. Facebook agreed to no longer allow advertisers to target job seekers based on gender, age or zip code, and that it would no longer give advertisers detailed targeting options based on protected classes. https://www.aclu.org/legal-document/exhibit-describing-programmatic-relief-facebook-settlement.

In a statement announcing the settlement, Sheryl Sandberg said the company was

"grateful" for the plaintiffs' "leadership." Using the well-worn language that we're used to hearing from people who've been caught doing something wrong, Sandberg wrote, "Today's changes mark an important step in our broader effort to prevent discrimination and promote fairness and inclusion on Facebook. But our work is far from over. We're committed to doing more, and we look forward to engaging in serious consultation and work with key civil rights groups, experts and policymakers to help us find the right path forward." https://about.fb.com/news/2019/03/protecting-against-discrimination-in-ads/.

However, several studies after the settlement indicate that Facebook's algorithm still manages to discriminate. One study by Northeastern University researchers found that the modified algorithm relies on proxy characteristics that correlate with age and gender. Algorithms that "Don't See Color": Measuring Biases in Lookalike and Special Ad Audiences, https://arxiv.org/pdf/1912.07579.pdf. Although the algorithm, called "Special Ad Audiences," doesn't consider audience members' age, gender, race or zip code, the researchers found that it created audiences almost as biased by age, gender and race. Id. at 2. In one example, the algorithm delivered an ad for jobs in AI mostly to young men, while another ad for supermarket jobs went to middle-aged women.

The researchers concluded, "Taken together, our results show that simply removing demographic features from the inputs of a large-scale, real-world algorithm will not always suffice to meaningfully change its outputs" about those features. They noted that they didn't believe that Facebook had breached the settlement; "Rather, the findings in this paper are a natural result of how complex algorithmic systems work in practice." Id. at 2.

Another study showed that Facebook's ad delivery algorithm can discriminate based solely on the ad's content. Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes, https://arxiv.org/pdf/1904.02095.pdf. The researchers discovered that ads targeting the same users with identical headlines, text, and images ended up being automatically delivered to significantly different audiences based on race or gender. So, ads featuring body-building can deliver mostly to men, ads for cosmetics mostly to women, ads for country music mostly to white people and ads for hip-hop mostly to Black people. Facebook's algorithm selectively delivered ads to stereotypical audiences based solely on the ad's images, *even if the content wasn't related to the stereotypical group.* The authors concluded that it is the algorithm that classifies an ad image as relevant to a user and skews delivery to audiences -- not the users' interaction with the ad. Id. at 2.

Employers can prevent this by applying draconian standards to where they advertise and the methods and criteria for ad delivery. This means going past what a platform's public relations and marketing materials claim, interrogating platforms about their algorithms, and seeking proof that their practices are fair and not affected by bias.

2. AI in evaluating, hiring and rejecting job applicants

Employers also use AI to evaluate, accept and reject job candidates based on their social media behavior. For example, the AI recruitment tools available through SignalHire search 350 million social media profiles using terms picked by recruiters. A company video explains that its algorithms display candidates' social media postings and analyze a candidate's social behavior to determine if the candidate would be likely to move to another job. https://youtu.be/jckRoRc9k5Y

Employers can go deeper by using AI to scan candidates' social media activity for potentially troublesome signs. As one consulting firm explains, an algorithm can quickly scan social media, score a candidate on their tendencies toward certain behaviors, and analyze "the tendency for the post to promote violence, racism, sexism, and bullying, just to name a few." Icon Consultants, Social Media Screening - The Next Stage in Recruitment, https://www.iconconsultants.com/blog/social-media-screening-the-next-stage-in-recruitment/.

One AI developer, Humantic, says its AI tool creates a candidate's personality profile without requiring them to take a test. The tool ranks a candidate on "five big personality traits: Openness, Neuroticism, Agreeableness, Extroversion and Conscientiousness," as well as dominance, influence, and steadiness, and potential work behaviors like teamwork. It also gives personalized advice about how to deal with a particular type of candidate, such as "Be respectful but crisp. Come to the point quickly," but "avoid being a story teller. Don't talk too much about process and rules." https://humantic.ai/

Of course, a critical question for employers and applicants is whether these tools measure what they claim to. Are candidates' social media postings an accurate indicator of a long list of highly specific personality traits? And are those traits even relevant to the requirements of a particular job? And even if an employer's use of an algorithm isn't intentionally discriminatory, it may be liable in a disparate impact case, in which an apparently neutral criterion has a discriminatory impact on members of a protected class. 42 U.S.C. § 2000e-2(k) (setting out burden of proof in disparate impact cases under Title VII).

In evaluating candidates, an AI tool can create bias when the data it uses reflects gender or

race disparities. For example, Amazon developed a hiring tool that rated the resumes of applicants for tech jobs on a scale that was skewed to favor men. This was because the criteria for the ratings were based on the resumes submitted by applicants in the previous ten years, and most of those applicants were male. The tool gave lower ratings to resumes containing the word "women's" (so "women's chess club" hurt the applicant's chances) or containing the names of women's colleges. Amazon announced that it scrapped the project in 2017 and never used the tool to evaluate candidates. Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G.

Companies that sell AI evaluation tools say that their algorithms can fairly and reliably evaluate applicants. For example, Cappfinity says that its tools test eight strengths that "align with success in a job role," "assess business-critical soft skills," "measure the personality traits that deliver performance at work," and "discover meaningful work experience beyond a resume." https://www.cappfinity.com/tempo/. Pymetrics, part of Harver, uses "a patented set of 12 engaging games to fairly and accurately measure cognitive and emotional attributes in only 25 minutes. Each game captures thousands of behavioral data points, then builds a profile of what makes a person and job unique." https://harver.com/why-harver/predictive-assessment-matching/. Other assessments of how an applicant will "behave at work" can take only seven minutes for hourly workers, and twelve minutes for professional talent. https://harver.com/behavioral-assessments/

Job seekers who make it past an AI screening may find that their job interview will be

conducted by an algorithm. Applicants respond to questions that appear as text on the screen or are posed by a digital voice. Beyond the impersonality and discomfort of having a one-sided interaction with an algorithm that can't have an authentic conversation, there are grave questions about whether some AI interviews tell an employer anything accurate about a candidate.

In one study, the MIT Technology Review tested AI interview platforms from two companies, MyInterview and Curious Thing, and found gross inaccuracies in the responses they reported to employers, their predictions and job matching.

In two interviews on Curious Thing, an applicant (playing the role for the study) answered identical automated questions. In the first, she answered in English, and the algorithm rated her English competency as 8.5 points out of 9. In the second, she answered the questions by reading a Wikipedia entry – in German. The tool also thought her English was fine, giving her a 6 -- and scored her identically again on another try, where she again answered with the same German Wikipedia reading.

When the candidate repeated the experiment on MyInterview, again answering questions in German, the algorithm rated her as a 73 percent match for the job and assessed her on a broad range of personality traits. MyInterview gives employers an interview transcript; the transcript interpreted the applicant's German as if it were English, so it was entirely gibberish:

> So humidity is desk a beat-up. Sociology, does it iron? Mined material nematode adapt. Secure location, mesons the first half gamma their Fortunes in for IMD and fact long on for pass along to Eurasia and Z this particular location mesons.

https://www.technologyreview.com/2021/07/07/1027916/we-tested-ai-interview-tools/#:~:text=AI%2Dpowered%20interview%20software%20claims,about%20their%20accuracy%20and%20reliability.

Another company that markets an AI tool to conduct and evaluate millions of interviews is HireVue. It uses its database to create a list of competencies for a particular position and automated questions for the interview; employers can add their own. The questions come in the form of text on a screen. For example, a question testing for adaptability reads:

> Please give an example of when you had to change direction on a project or work assignment midway through implementation. What happened as a result of the change? Please describe the situation, your actions, and the outcome.

HireVue's algorithm then evaluates how the applicant did in the interview and scores them on the job competencies. It also rates candidates on "soft" competencies like communication skills, conscientiousness, problem-solving skills, team orientation, and initiative. https://www.hirevue.com/blog/candidates/how-to-prepare-for-your-hirevue-assessment.

The algorithm tells an employer how an applicant scores on a particular job competency using this scale:

> Is unlikely to be successful in situations that require this competency.
>
> Is likely to demonstrate the competency or ability in simple or a limited number of situations.
>
> Consistently demonstrates competency or ability, but may require assistance in more difficult situations.
>
> Is likely to be effective in moderate to complex situations that require this competency or ability.
>
> Is likely to be very effective and excel in complex situations that require this competency or ability.

See the company's White Paper at Science-Backed Hiring: Enhance Quality & Fairness with Structured Interviews: https://www.hirevue.com/resources/whitepaper/guide-science-backed-

hiring-enhance-quality-and-fairness-with-structured-interviews.

In 2019, the Electronic Privacy Information Center filed a complaint at the Federal Trade Commission, alleging that HireVue's processes constitute an unfair or deceptive trade practice. The complaint said that HireVue uses facial recognition technology to evaluate candidates concerning social intelligence, personality traits, communications skills and job aptitude, and that the technology does not properly evaluate interviews based on race, improperly interpreting the expressions of Black faces.

https://epic.org/wpcontent/uploads/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf.

One 2021 study concluded that AI tools could not properly read people's facial expressions in photographs, because the meaning of those expressions tremendously varies based on an individual's background and culture. https://www.nature.com/articles/s41467-021-25352-6#Sec2.

HireVue claims that an independent audit affirmed the reliability and validity of the interview process. Industrial Organizational Psychology Audit Report: https://webapi.hirevue.com/wp-content/uploads/2021/04/hirevue-industry-organizational-psychology-audit-report-2021.pdf?_ga=2.158371386.1827309848.1693334614-850478031.1693334614. In January 2021, it announced it would no longer use facial analysis to evaluate job candidates. https://epic.org/hirevue-facing-ftc-complaint-from-epic-halts-use-of-facial-recognition/

B. Legislative and regulatory responses to the use of AI in employment decisions

Other than what AI vendors tell the public about the validity of their tools, what legislative and regulatory protections can an employee or job applicant rely on to ensure that an AI tool measures what it's supposed to measure?

1. State and local legislation

In 2025, legislatures in all fifty states, the District of Columbia and Puerto Rico introduced bills to regulate the use of AI. Most of these proposals were either pending, not enacted, or focused on areas other than employment. National Conference of State Legislatures, Artificial Intelligence 2025 Legislation: https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation.

However, over the last few years, some jurisdictions have enacted protections for employees, with various degrees of significance.

California

In October, Governor Newsom signed the Transparency in Frontier Artificial Intelligence Act (SB 53), the first law in the country regulating "frontier developers." https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260SB53

Frontier developers are trainers of "frontier models" -- AI models trained using a defined high level of computer power. However, many of the requirements only govern "large" frontier developers - those with annual gross revenues greater than $500 million in the previous calendar year (including revenue from affiliates).

Frontier developers must include transparency reports on their websites and report

safety violations to the California Office of Emergency Services. Large frontier developers have to publish a frontier AI safety and security framework, which sets out how the developer analyzes and lessens the catastrophic risks of its models. Violators can be fined civil penalties of up to $1 million for each violation.

Employees responsible for assessing, managing, or addressing critical AI safety incidents have whistleblower protections for reporting either violations of the law or substantial violations of public safety, either internally or to the state Attorney General, and are given a private right of action to contest retaliatory acts.

The law is effective August 2, 2026 (delayed from January 1).

In 2020, California enacted the California Privacy Rights Act. Cal. Civil Code § 1798.100. https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020/. It established the California Privacy Protection Agency, and directed it to issue regulations "governing access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling." Those regulations require "businesses' responses to access requests to include meaningful information about the logic involved in those decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer." Cal. Civ. Code § 1798.185(a)(16). The law includes detailed requirements for handling employees' data.

New York City

A New York City law regulating AI in hiring processes went into effect in January 2023. It requires that employers notify applicants *and employees* who "reside in" New York City that an "Automated Employment Decision Tool" (AEDT) will be used in the employer's decision and

what job qualifications and characteristics the tool will use to assess the employee or candidate. The employee or candidate can request an alternative means of doing the evaluation. The law provides that "in the city" it is unlawful for an employer or employment agency to use an AEDT to screen a candidate or employee for an employment decision (hiring or promotion) *unless* "1. Such tool has been the subject of a bias audit conducted no more than one year prior to the use of such tool…" The results of the audit have to be publicly available on the employer's website. While the law doesn't include a private right of action, it provides for civil penalties for each day an employer violates it. Local Law 144, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9. [1]

The law doesn't require employers to post the audits in a central government repository and doesn't penalize employers for not using AEDTs that either don't measure what they say they measure or have a discriminatory impact. It simply requires that employers use AEDTs that have complied with the audit requirements.

Before the bill passed, a large number of advocacy groups, including the National Employment Law Project, the New York Civil Liberties Union and the NAACP Legal Defense and Educational Fund, wrote the City Council criticizing it as vague and ineffective. https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/5faeb73303633f0646ae5533/1605285684675/Intro.+1894+Sign-On+Letter+%281%29.pdf.

The City Department of Consumer Affairs issued final rules to implement Local Law

[1] Former Mayor Bill de Blasio neither signed nor vetoed the bill, so it became law.

144. The rules have detailed definitions of terms, explain what employers must do to conduct a bias audit, and describe the notice employers have to provide employees and job candidates. Rules of the City of New York, Title 6, Chapter 7, Subchapter T, https://rules.cityofnewyork.us/wp-content/uploads/2023/04/DCWP-NOA-for-Use-of-Automated-Employment-Decisionmaking-Tools-2.pdf.

Before the rules were finalized, the Department of Consumer Affairs issued an FAQ, which clarifies that the law's provision applies to employers and employment agencies that use an AEDT "in the city." This means that either the job location is an office in NYC, at least part time, or the job is fully remote but the location associated with it is an office in NYC. For employment agencies, it means that the location of the employment agency using the AEDT is in NYC or, if the location of the employment agency is outside NYC, one of the two previous criteria is met. https://www.nyc.gov/assets/dca/downloads/pdf/about/DCWP-AEDT-FAQ.pdf. The FAQ notes that the law doesn't apply just to hiring or promotion decisions, but also when employers or employment agencies use an AEDT to substantially help them assess or screen candidates at any point in the hiring or promotion process. However, it doesn't apply when employers scan a resume bank, conduct outreach to potential candidates, or invite applications.

How effective is Local Law 144 as a practical matter? A February 2024 Cornell University study surveyed 391 companies and found that only five percent of them had filed bias audits on their websites, and only four percent had filed notices about the use of AEDTs.

Summary: https://citizensandtech.org/research/2024-algorithm-transparency-law/

Full study: https://dl.acm.org/doi/pdf/10.1145/3630106.3658998

New York State

Over the last three years, several bills regulating employers' use of AI tools were introduced in the New York State legislature. None of them have been enacted, including proposals to prevent discrimination by AI tools against a wide range of protected classes, prohibiting developers from selling "high risk" AI systems unless they have been independently audited, requiring notice to employees and applicants that a high risk AI tool will be used in making an employment decision, providing for whistleblower protections for employees and applicants who disclose violations of the law, and prohibiting uses of "social scoring systems" which test for personality characteristics or social behavior to treat people differently in a way that is unjustified or disproportionate.

Texas

In June 2025, Governor Abbot signed the Texas Responsible AI Governance Act ("TRAIGA" HB 149). It broadly regulates AI developers and deployers, applying to anyone who promotes, advertises or conducts business in Texas, produces a product or service used by Texas residents, or develops or deploys an artificial intelligence system in Texas.

Its definition of an AI system is expansive: "any machine-based system that, for any explicit or implicit objective, infers from the inputs the system receives how to generate outputs, including content, decisions, predictions or recommendations, that can influence physical or virtual environments."

Among many other provisions, the statute makes it unlawful for any person to "develop or deploy an artificial intelligence system with the intent to unlawfully

discriminate against a protected class in violation of state or federal law." However, it notes that "For purposes of this section, a disparate impact is not sufficient by itself to demonstrate an intent to discriminate."

Although TRAIGA doesn't provide for a private right of action, it has a mechanism for enforcement by the state attorney general, with significant fines.

https://capitol.texas.gov/tlodocs/89R/billtext/pdf/HB00149F.pdf

Illinois

Illinois' law governing the use of AI in employment decisions went into effect on January 1, although it was enacted in 2024. It amends the state Human Rights Act, which makes it unlawful for employers to use an AI tool to make employment decisions that have the effect of discriminating against a protected class, or to use zip codes as a proxy for a protected class. The law requires employers to give employees notice that the employer is using an AI tool. IL HB 3773. https://ilga.gov/legislation/publicacts/103/PDF/103-0804.pdf

In 2019, Illinois enacted the Artificial Intelligence Video Interview Act. It applies to employers that ask applicants for Illinois-based jobs to submit to a recorded video interview, which will use an AI analysis for the interview. The employer must inform the applicant that AI may be used to analyze the interview and evaluate the applicant, tell the applicant how the AI tool works and what general types of characteristics it uses to evaluate applicants, and obtain the applicant's consent in advance. If the applicant requests that the video be deleted, the employer has to do so within thirty days. https://www.ilga.gov/legislation/publicacts/101/PDF/101-0260.pdf.

The Act was amended in 2020 to require that employers who use only an AI interview to determine if a candidate will be interviewed in person must collect and disclose to the State Department of Commerce and Economic Opportunity data on the race and ethnicity of candidates who are and aren't given a second interview, as well as those ultimately hired.

https://custom.statenet.com/public/resources.cgi?id=ID:bill:IL2021000H53&ciq=ncsl&client_md=cf812e17e7ae023eba694938c9628eea&mode=current_text

Colorado

In 2024, Colorado enacted a law restricting the use of "high risk" AI systems by both "deployers" (any business in Colorado that uses an AI tool) and developers; it goes into effect on June 30 (delayed from February 1). Colorado AI Act (SB 24-205).

https://leg.colorado.gov/bill_files/47770/download

A high risk AI system is one that "makes, or is a substantial factor in making, a consequential decision." A "consequential decision" is one that "has a material legal or similarly significant effect on the provision or denial to any consumer [any Colorado resident] of, or the cost or terms of" an employment or employment opportunity, educational enrollment or opportunity, a financial or lending service, essential government service, health care, housing, insurance or legal service.

Developers and deployers have to use reasonable care to ensure they avoid "algorithmic discrimination" against a variety of protected classes. Deployers must complete annual impact assessments of the risk of algorithmic discrimination and maintain them for three years. They must disclose the AI systems and the impact assessments to consumers and give them the chance

to opt out of their use. If a deployer deploys a high risk AI system as a substantial factor in making a decision about a consumer, the deployer has to disclose that to the consumer, along with information about the AI system. If the decision is unfavorable to the consumer, the deployer must disclose to them the reasons for the decision, the chance to correct incorrect personal data that the AI system processed, and the opportunity to appeal the decision.

The law creates a rebuttable presumption that the deployer used reasonable care to protect consumers from algorithmic discrimination if they meet certain criteria. It doesn't include a private right of action to enforce it.

Maryland

In 2020, Maryland enacted a law requiring consent by a job applicant to the use of facial recognition technology. It prohibits the use of a "facial recognition service" (a technology that analyzes facial features) for the purpose of creating a "facial template" (a "machine-interpretable pattern of facial features extracted by facial recognition") in an employment interview, unless the applicant gives written consent.

https://mgaleg.maryland.gov/2020RS/Chapters_noln/CH_446_hb1202t.pdf.

2. Federal administrative actions

The Biden administration had sought to regulate the use of AI to protect employees and consumers, but the Trump White House has blocked and eliminated most of those steps.

The Biden actions included:

> An EEOC initiative to ensure that AI tools used in employment decisions comply with federal civil rights laws, and technical guidances on AI in employment decision-making concerning both Title VII and the ADA
>
> An expansive Blueprint for an AI Bill of Rights
>
> An Executive Order on Safe, Secure and Trustworthy Artificial Intelligence, directing numerous federal agencies to promulgate rules and standards to address the risks and benefits of using AI tools. Based on it, the Department of Labor issued Principles for Developers and Employers when using AI in the workplace.

These mandates have all been rescinded by the Trump administration.

On Trump's first day in office, he issued Executive Order 14148, Initial Recissions of Harmful Executive Orders and Actions, revoking Biden's Executive Order on Safe, Secure and Trustworthy Artificial Intelligence, as well as many other Biden administration actions.

Three days later, he issued Executive Order 14179, Removing Barriers to American Leadership in Artificial Intelligence. It states that U.S. policy concerning AI is to "sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security," and that its purpose is to "revoke certain existing AI policies and directives that act as barriers to American AI innovation, clearing a path for the United States to act decisively to retain global leadership in artificial intelligence." It requires a review of all Biden administration AI policies which conflict with the new U.S. policy, and directs federal agencies to rescind, suspend or revise them. It similarly requires federal agencies to develop AI "Action Plans" to implement the

government's new AI policy. https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/

Based on these Executive Orders, in January 2025, the EEOC removed from its website its guidances on AI.

In the Administration's latest actions, in December 2025, Trump issued another executive order, Ensuring a National Policy Framework for Artificial Intelligence. It is based on the notion that although "United States AI companies must be free to innovate without cumbersome regulation…excessive State regulation thwarts this imperative" in three ways: "by creating a patchwork of 50 different regulatory regimes that makes compliance more challenging, particularly for start-ups," by "requiring entities to embed ideological bias within models," and by "impinging on interstate commerce."

> The Executive Order targets state regulation of AI through several avenues:
>
> It establishes an AI Litigation Task Force in the Justice Department, charged with challenging state AI laws that "unconstitutionally regulate interstate commerce, are preempted by existing Federal regulations, or are otherwise unlawful in the Attorney General's judgment."
>
> It requires the Commerce Secretary to publish an evaluation of existing state AI laws, identifying "onerous" laws that conflict with the Administration's AI policy or require disclosures that may violate the First Amendment.
>
> It tells federal agencies to evaluate whether they can withdraw discretionary federal funding from states that have laws conflicting with the Administration's AI policies.
>
> It requires the Federal Trade Commission to issue a Policy Statement explaining the circumstances under which state laws requiring alterations to the "truthful outputs" of AI models are preempted by the FTC's prohibition on deceptive acts or practices affecting commerce -- in other words, targeting state laws that prohibit discrimination by AI tools.

It directs relevant advisors to recommend legislation establishing a uniform Federal policy framework for AI that preempts State AI laws that conflict with the Executive Order's AI policy.

https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/

C. Employment litigation

Plaintiffs have brought cases in several jurisdictions claiming that employers' use of AI is discriminatory or otherwise violates state laws.

Based on some court decisions, vendors that sell AI tools to employers may be liable under anti-discrimination statutes. In a class action claiming that an AI tool unlawfully screens out Black job applicants, the California Supreme Court ruled that the vendor that developed the tool could be liable as the company's agent under the California Fair Employment and Housing Act. *Raines v. U.S. Healthworks Medical Group*, 15 Cal. 5th 268 (August 21, 2023); see also 2023 U.S. App. LEXIS 27666 (9th Cir. October 18, 2023). In 2025, the trial court provisionally approved a settlement with a class of more than 172,000 job applicants. *Raines v U.S. Healthworks Med. Group*, 2025 US Dist LEXIS 134811 (S.D. Ca. 2025).

In another California class action against an AI provider, the plaintiff claimed that the vendor functions as an employment agency and as an agent of its employer customers, and uses AI tools that incorporate human bias to screen out applicants by age, race and disability. He alleged that the vendor, Workday, provides discriminatory AI tools to thousands of employers, including numerous Fortune 500 companies. *Mobley v. Workday Inc.,* 23-cv-00770 (N.D. Ca. 2023).

The district court initially held that the complaint didn't state sufficient facts to show that Workday was significantly involved in procuring employees to support plaintiff's claim that Workday is an "employment agency" under Title VII, the ADEA or ADA, or was an "agent" of its employer customers. *Mobley v. Workday, Inc*., 2024 U.S. Dist. LEXIS 11573 (N.D. Ca. January 19, 2024). After Mobley amended his complaint, the court partially denied and partially granted Workday's motion to dismiss. 740 F. Supp. 3d 796 (N.D. Ca. 2024).

The court ruled that Workday could be liable as an agent of an employer, writing that Title VII, the ADA and the ADEA "all prohibit discrimination not just by employers themselves but also by agents of those employers," and therefore employers "cannot escape liability for discrimination by delegating their traditional functions, like hiring, to a third party." Mobley, the court found, had plausibly alleged that Workday's customers "delegate traditional hiring functions, including rejecting applicants, to the algorithmic decision-making tools provided by Workday." Rejecting Workday's argument that its role as a vendor of an AI tool precluded it from be considered its customers' agent, the court noted:

> Workday's role in the hiring process is no less significant because it allegedly happens through artificial intelligence rather than a live human being who is sitting in an office going through resumes manually to decide which to reject. Nothing in the language of the federal anti-discrimination statutes or the case law interpreting those statutes distinguishes between delegating functions to an automated agent versus a live human one.[2]

The court certified a class, 2025 U.S. Dist. LEXIS 94475 (N.D. Ca. May 16, 2025), and since then, the parties have litigated various related disputes.

[2] The court dismissed Mobley's claim that Workday could be liable as an "employment agency" under the federal statutes.

In Illinois, a class action against a vendor of AI tools alleges that the company uses a facial recognition tool in job interviews without getting informed consent as required by the Illinois Biometric Privacy Protection Act. *Deyerler v. HireVue Inc*., 2024 U.S. Dist. LEXIS 32211 (N.D. Ill. 2024). The court denied HireVue's motion to dismiss, finding that its scans of plaintiffs' faces qualified as "biometric identifiers" under the BBPA; that plaintiffs' BPPA claims weren't precluded by Illinois' Artificial Intelligence Interview Act; and that HireVue wasn't a "financial institution" exempt from the BPPA. The court rejected HireVue's other arguments that the plaintiffs hadn't alleged sufficient facts to state a cause of action under the statute. Last November, HireVue again moved to dismiss, on almost identical grounds, and the court denied the motion. 2025 U.S. Dist. LEXIS 230943 (N.D. Ill 2025).

A class action in Massachusetts alleges that CVS uses AI interview tools that violate the Massachusetts law prohibiting employers from conditioning employment or continued employment on taking a lie detector test. See the Massachusetts Lie Detector Statute, Mass. Gen. Laws ch. 149, § 19B(2).

Plaintiffs allege that CVS uses video interview technology from HireVue, which includes questions such as "What does integrity mean to you?", "What would you do if you saw someone cheating on a test?", and "Tell me about a time that you acted with integrity." HireVue uploads the recordings of the responses to a third-party platform called Affectiva, which analyzes candidates' facial expressions, eye contact, voice intonation, and inflection using artificial intelligence. HireVue sends its findings to CVS.

Defendants moved to dismiss, arguing that the Lie Detector Statute doesn't allow for a

private right of action. The court denied the motion, holding that the plain language of the law clearly authorizes private suits.[3] *Baker v. CVS Health Corporation,* 2024 U.S. Dist. LEXIS 27206. (D. Ma. 2024**).**

In 2023, the EEOC settled a case it had brought against a tutoring company, iTutor, which alleged that the firm's AI tool for job applicants automatically rejected older qualified candidates because of their age. See the consent decree at https://www.workforcebulletin.com/assets/htmldocuments/blog/8/2023/08/2023.08.09-EEOC-v.-iTutorGroup-Joint-Notice-of-Settlement-22-cv-02565-PKC-PK.pdf

II. Employee monitoring

A. What employers are watching

Artificial intelligence has given employers extraordinary power to track employees' work, performance, speed, movements and keystrokes. Employers certainly have a legitimate interest in making sure that employees' electronic communications at work are job-related, that employees don't improperly use or disclose confidential, proprietary or trade secret information, and that employees' business communications are lawful, proper and appropriate. But much of the surveillance is demeaning to employees. It can leave them feeling that they're under constant suspicion, and that they're racing as fast as they can to keep up with their new demanding manager: an algorithm.

One company selling keystroke monitoring software is Teramind. Teramind captures

[3] While not a basis of the court's decision, the court noted that HireVue stated that its tool can detect whether an applicant "[h]as an innate sense of integrity and honor," can help with "lie detection" and "screen[ing] out embellishers," and can organize applicant competencies including "reliability, honesty, [and] integrity."

every keystroke an employee enters, whether in documents, emails, browsers, instant messages, applications and programs. Employers can track all apps used and websites visited and classify them as either productive or unproductive. https://www.teramind.co/features/keystroke-recorder-logger.

Teramind claims that "Keylogging is an invaluable way for employers to gain insight in to their employees' daily activity, attitude, professionalism and productivity." Id. It can track individual employees' time worked, idle time, and the costs and time for each activity, and then rank employees by productivity. It can note which activities (including website visits and social media interactions) are productive or unproductive and monitor for potential rule violations. https://democompany.teramind.co/#/tma/behavior_alerts.

Another company, Hubstaff, uses AI to capture screenshots of an employee's work, Internet use, "activity rates," "idle time" and location. (It doesn't track individual keystrokes.) It calculates an employee's activity rate this way:

> Hubstaff detects input from your keyboard and mouse to measure your activity over ten-minute periods (600 seconds). For example, if you typed on your keyboard and moved your mouse for 300 total seconds while the timer was running, that would equal an activity rate of 50%.

Under Hubstaff's system, an employee who doesn't type or use their mouse because they are reading job-related material, thinking, or having a work discussion would have a lower activity rate. However, Hubstaff's FAQs caution employers not to rush to conclude that an employee who isn't touching their keyboard or mouse is a shirker. It notes that the situation of

> a writer working on an extensive article. A low activity rate doesn't immediately imply that they're inefficient. Heavy research and web browsing typically precede writing, so be sure to review the websites they visited before making a conclusion.

https://hubstaff.com/how-tracking-works.

Perhaps no company has perfected surveillance to monitor every aspect of its employees' work days more than Amazon, which uses handheld scanners, workstations, cameras and software at its fulfillment centers to track every second of an employee's activities and measure their productivity. Amazon's algorithm monitors how many orders a worker packs, measures "time off task" (even to go to the bathroom), and compares the worker's productivity with Amazon's quotas.

Workers report tremendous pressure to keep up. The stress also comes from the robots that scurry through the warehouse, delivering products to workers for packing. Creating more pressure, Amazon uses video games to push individual workers, teams or floors to compete with each other to handle the most products in the shortest time.

Amazon workers' breathless race to meet productivity requirements correlates with an unusually high rate of serious employee injuries. The Washington Department of Labor found that Amazon's surveillance tools were directly linked to an increase in those injuries. https://www.washingtonpost.com/technology/2021/12/02/amazon-workplace-monitoring-unions/; https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations. A Washington Post analysis of OSHA statistics in 2022 concluded that Amazon warehouse workers suffered serious injuries at almost twice the rate of warehouse workers in other companies. https://www.washingtonpost.com/technology/2021/06/01/amazon-osha-injury-

rate/?itid=lk_inline_manual_62.[4]

B. Legislation limiting how employers can monitor

The federal Electronic Communications Privacy Act of 1986, enacted years before most of this technology was available, has some mild protections for employees and gives a lot of latitude to employers. Although it bars employers from intercepting employees' oral, electronic and wire communications, it contains a broad exception for monitoring done for legitimate business reasons and for monitoring done with consent. A detailed explanation of the ECPA the other federal statutes it affects is in Eric Bosset and Hannah Lepow's Key Issues in Electronic Communications Privacy Act (ECPA) Litigation, Practical Law (2020). https://www.cov.com/-/media/files/corporate/publications/2020/06/key-issues-in-electronic-communications-privacy-act-ecpa-litigation.pdf.

In November 2021, New York State enacted new protections for employees whose employers want to monitor their electronic activity. The statute -- which covers every private sector employer with a place of business in New York -- requires prior written notice to employees when they're hired. But since it also requires employers to prominently post the notice in the workplace so all employees subject to monitoring can view it, as a practical matter it also protects current employees. New York Civil Rights Law 52-c. https://www.nysenate.gov/legislation/laws/CVR/52-C*2. (There is an entirely unrelated duplicate Sec. 52-c in the Civil Rights Law). Enforcement is by the Attorney General with violators subject to civil penalties.

[4] In Alec MacGillis' 2021 book Fulfillment - Winning and Losing in One-Click America, he details what it's like for Amazon employees to labor under these conditions. https://us.macmillan.com/books/9780374 159276/fulfillment.

Over the last several years, members of the New York legislature have introduced additional legislation to restrict employers' use of electronic surveillance of employees, as part of the proposed legislation to limit the use of AI in employment decisions, but the bills haven't been enacted.

Connecticut requires employee consent for monitoring. Conn. Gen. Stat. 31-48-d https://law.justia.com/codes/connecticut/2012/title-31/chapter-557/section-31-48d/.

Delaware also requires consent in a similar statute. Del. Lab. Code 19-7-705 https://codes.findlaw.com/de/title-19-labor/de-code-sect-19-705.html.

Hawaii generally prohibits employers from requiring employees to download location tracking apps on their personal devices, unless the employee consents, and prohibits retaliation for related protected activity. https://www.capitol.hawaii.gov/session2021/bills/HB1253_CD1_.pdf.

Where do we go from here?

AI and employee surveillance give employers an even greater hold on the balance of power in the workplace than they've always had. As these tools proliferate, legislatures and courts need to decide some critical questions: While employers need to recruit, hire and evaluate employees, how quickly and efficiently do they truly need to do that? Do AI-led interviews and applicant ratings eliminate human bias or substitute the bias in an AI tool? If AI cannot truly measure personality traits and job performance, shouldn't employers stop using it? Do employers need to micro-monitor every step, keystroke and minute of their employees' work day? Are efficiency, confidentiality and profits worth the tension, resentment, emotional stress

and workplace injuries that employees get from constant surveillance and a rush to meet AI-created performance goals? What kinds of workplace cultures do we want to encourage?