

SENATE PRIVACY, DIGITAL TECHNOLOGIES, AND CONSUMER PROTECTION COMMITTEE
Senator Christopher Cabaldon, Chair
2025-2026 Regular Session

AB 1883 (Bryan)
Version: May 18, 2026
Hearing Date: June 29, 2026
Fiscal: Yes
Urgency: No
CK

SUBJECT

Workplace surveillance tools

DIGEST

This bill regulates the use of workplace surveillance tools, as broadly defined, by both public and private employers.

EXECUTIVE SUMMARY

Workplace surveillance technology has expanded dramatically in recent years, evolving from basic security cameras and badge access systems to sophisticated digital monitoring tools that track virtually every aspect of employee activity. These tools may provide benefits to employers in the form of increased productivity and security. However, they raise serious concerns about their impact on privacy and worker organizing; the psychological effects on workers; and when decisions are based on automated performance metrics, issues of algorithmic bias and unfairness.

This bill regulates employers use of “workplace surveillance tools,” specified tools that collect or facilitate the collection of worker data, activities, communications, actions, biometrics, or behaviors by means other than direct observation by a person. This includes video or audio surveillance, continuous incremental time-tracking tools, and geolocation. Employers are prohibited from using a workplace surveillance tool on workers to carry out certain actions or make certain inferences.

The bill is sponsored by the California Federation of Labor Unions. It is supported by a large coalition of labor organizations and advocacy groups, including the State Building and Construction Trades Council of California and Privacy Rights Clearinghouse. It is opposed by a coalition of governmental associations and industry groups, including the League of California Cities and the Tri County Chamber Alliance. Should the bill pass out of this Committee, it will next be heard in the Senate Labor, Public Employment, and Retirement Committee.

PROPOSED CHANGES TO THE LAW

Existing law:

- 1) Provides, pursuant to the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const., art. I, § 1.)
- 2) Establishes the California Consumer Privacy Act (CCPA), which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. (Civ. Code § 1798.100 et seq.)
- 3) Establishes the California Privacy Rights Act (CPRA), which amends the CCPA. (Civ. Code § 798.100 et seq.; Proposition 24 (2020).)
- 4) Provides consumers the right to request that a business delete any personal information about the consumer which the business has collected from the consumer. (Civ. Code § 1798.105(a).)
- 5) Requires a business that collects a consumer's personal information to, at or before the point of collection, inform consumers of the categories of personal information to be collected and the purposes for which the categories of personal information are collected or used. (Civ. Code § 1798.100(a).)
- 6) Grants a consumer the right to request that a business that collects personal information about the consumer disclose to the consumer the following:
 - a) the categories of personal information it has collected about that consumer;
 - b) the categories of sources from which the personal information is collected;
 - c) the business or commercial purpose for collecting, selling, or sharing personal information;
 - d) the categories of third parties with whom the business shares personal information; and
 - e) the specific pieces of personal information it has collected about that consumer. (Civ. Code § 1798.110.)
- 7) Provides consumers the right to request that a business that sells or shares the consumer's personal information, or that discloses it for a business purpose, disclose to the consumer specified information, including the categories of personal information collected, shared, sold, and disclosed and the categories of third parties receiving the information. (Civ. Code § 1798.115.)

This bill:

- 1) Prohibits an employer from using a “workplace surveillance tool” on workers to do any of the following:
 - a) Prevent compliance with or violate any federal, state, or local labor, occupational health and safety, employment, or civil rights laws or regulations.
 - b) Infer information about workers engaging in activity protected by state or federal law.
 - c) Make inferences about an individual’s emotional state.
 - d) Make inferences about an individual based on their gait.
 - e) Collect neural data.
 - f) Infer a worker’s protected status.
- 2) Defines “workplace surveillance tool” as any system, application, instrument, or device that collects or facilitates the collection of worker data, activities, communications, actions, biometrics, or behaviors by means other than direct observation by a person, including video or audio surveillance, continuous incremental time-tracking tools, geolocation, electromagnetic tracking, photoelectronic tracking, or that utilizes a photo-optical system or other means.
- 3) Prohibits an employer from using facial recognition technology to make inferences about a worker for firing, deactivation, or disciplinary purposes.
- 4) Defines additional relevant terms, including:
 - a) “Employer” means a person or governmental entity that directly or indirectly, or through an agent or any other person, employs or exercises control over the wages, benefits, other compensation, hours, working conditions, access to work or job opportunities, or other terms or conditions of employment, of any worker, including all branches of state government, and all cities, counties, cities and counties, charter cities, charter counties, special districts, including transit districts, the University of California, the California State University, community college districts, school districts, or any other state or local governmental entity. This includes an employer’s labor contractor.
 - b) “Worker” means a natural person, an employee of, or an independent contractor providing service to, or through, a business or a state or local governmental entity in a workplace.
- 5) Provides for civil enforcement by the Labor Commissioner, public prosecutors, and a worker or their representative, who has suffered a violation. Such petitioners may bring a civil action seeking appropriate temporary or preliminary injunctive relief, including punitive damages, and reasonable attorney’s fees and costs. Public enforcers may additionally seek civil penalties.

- 6) Authorizes the Labor Commissioner, in addition to the above civil action, to further enforce this part, including by investigating an alleged violation, and ordering appropriate temporary relief to mitigate a violation or maintain the status quo pending the completion of a full investigation or hearing, including issuing a citation against an employer in violation, as specified.
- 7) Clarifies that it does not apply to the use of a workplace AI tool or a workplace surveillance tool to the extent that use of the tool is required by, or reasonably necessary to comply with, a federal statute, federal regulation, or binding federal contract relating to any of the following:
 - a) The development of aircraft for use in the national airspace.
 - b) The development of products or services for national security, military, space, or defense purposes.
- 8) Provides that the above exemption applies only to the operations covered by a federal statute, federal regulation, or binding federal contract as outlined.
- 9) Clarifies that it does not prohibit an employer from using a workplace surveillance tool to ensure safety, provided that the tool does not incorporate AI that makes inferences or predictions based on a worker's emotional, gait, neural data, protected status, or about activity protected by state or federal law.

COMMENTS

1. The rising deployment of workplace surveillance tools

Workplace surveillance tools are technologies used by employers to monitor and evaluate things such as workflow and employee activities and performance. Common examples include keystroke logging software, which tracks keyboard activity to gauge productivity, and screen monitoring tools that capture screenshots or live feeds of employee screens. Email and communication monitoring systems are also widely used to scan messages for sensitive information or inappropriate content. GPS tracking is used to monitor employees' location and movement, both in the field and in factories and other workplaces. Additionally, video surveillance cameras in offices or warehouses can monitor physical behavior and security.

In recent years, some employers are even requiring workers to wear tracking tools that monitor not only location and movement, but biometric information such as eye movements, body shifts, and facial expressions, captured by computer webcams, to evaluate whether their employees are appropriately attentive in their work tasks. As an example, AI systems at call centers record and grade how workers are handling calls. This technology can be used to "coach" workers while they are talking to customers,

telling them to sound happier or be more empathetic.¹ Another example is wearable technology that, among other things, tracks a worker's movements throughout the day, gathering biometric data, measuring how many times they use the bathroom, how long they spend in break areas, and which employees are spending time together. At least one company sells biometric ID badges with microphones, sensors, and other tools to record conversations, monitor speech, body movements, and location.² Even body temperature, sweat, and frequency of bathroom visits can be tracked and analyzed by employers.

These tools aim to enhance productivity and security but often raise serious concerns about privacy and trust, especially as their incidence rapidly expands.

Research out of Cornell University identifies this trend and questions just how useful these tools are for accomplishing employers' goals:

Organizations using AI to monitor employees' behavior and productivity can expect them to complain more, be less productive and want to quit more – unless the technology can be framed as supporting their development, Cornell research finds.

Surveillance tools, which are increasingly being used to track and analyze physical activity, facial expressions, vocal tone and verbal and written communication, cause people to feel a greater loss of autonomy than oversight by humans, according to the research.

Businesses and other organizations using the fast-changing technologies to evaluate whether people are slacking off, treating customers well or potentially engaging in cheating or other wrongdoing should consider their unintended consequences, which may prompt resistance and hurt performance, the researchers say. They also suggest an opportunity to win buy-in, if the subjects of surveillance feel the tools are there to assist rather than judge their performance – assessments they fear will lack context and accuracy.

“When artificial intelligence and other advanced technologies are implemented for developmental purposes, people like that they can learn from it and improve their performance,” said Emily Zitek, associate professor of organizational behavior in the ILR School. “The problem occurs when they feel like an evaluation is happening automatically,

¹ Kevin Roose, *A Machine May Not Take Your Job, but One Could Become Your Boss* (June 23, 2019) *The New York Times*, <https://www.nytimes.com/2019/06/23/technology/artificial-intelligence-ai-workplace.html>. All internet citations current as of June 24, 2026.

² *This ID badge tracks your every move on the job* (May 12, 2017) CBS News, <https://www.cbsnews.com/news/humanyze-id-badge-tracks-workers-all-day/>.

straight from the data, and they're not able to contextualize it in any way."

...

Algorithmic surveillance has already induced backlash. In 2020, an investment bank swiftly dropped a pilot program testing productivity software to monitor employee activity, including alerting them if they took too many breaks.³

The federal Government Accountability Office (GAO) developed a report assessing the use of workplace surveillance tools and their effects. Some of their takeaways are:

- **Worsens mental health:** Constant surveillance can amplify workers' stress and anxiety levels, making them feel like they're under a microscope. The sheer act of surveillance can contribute to workers' feeling less confident or enthusiastic about their jobs. Workers increasingly reported feeling that they cannot voice concerns or share suggestions out of fear that their digital footprint will bite back. When the work environment makes workers feel scrutinized, it may very well foster a culture of distrust. For example, a call center worker said that surveillance tools have resulted in an unrelenting push to improve sales. They said, "The pressure to sell and the various ways that managers can monitor me creates an enormous amount of stress."
- **Discourages unionization:** Being perpetually watched can also eat away at a workers' sense of autonomy and privacy. Consequently, some workers feel it discourages workplace solidarity and unionization efforts. When workers fear their every move is being tracked, organizing for better conditions feels risky – undermining solidarity and weakening workplace morale.
- **Potential to create discrimination:** Workers' advocates and researchers worry about the potential for digital surveillance to create bias or discrimination. Some worry that AI-driven performance metrics might unfairly target certain groups. For instance, those who take longer to complete tasks due to disability or other factors. This could magnify existing disability, racial, or gender inequalities in the workplace.⁴

2. Ensuring some transparency regarding workplace surveillance

This bill regulates the use of these "workplace surveillance tools" by employers. The term is defined broadly to mean any system, application, instrument, or device that

³ James Dean, *More complaints, worse performance when AI monitors work* (July 2, 2024) Cornell Chronicle, https://news.cornell.edu/stories/2024/07/more-complaints-worse-performance-when-ai-monitors-work?utm_source=chatgpt.com.

⁴ 'Why do I feel like somebody's watching me?' Workplace Surveillance Can Impact More Than Just Productivity (October 29, 2024) GAO, <https://www.gao.gov/blog/why-do-i-feel-somebodys-watching-me-workplace-surveillance-can-impact-more-just-productivity>.

collects or facilitates the collection of worker data, activities, communications, actions, biometrics, or behaviors by means other than direct observation by a person, including, but not limited to, video or audio surveillance, continuous incremental time-tracking tools, geolocation, electromagnetic tracking, photoelectronic tracking, or that utilizes a photo-optical system or other means. The bill applies to both private and governmental employers and protects employees and independent contractors.

The bill prohibits an employer from using a workplace surveillance tool on workers to do any of the following:

- Prevent compliance with or violate any federal, state, or local labor, occupational health and safety, employment, or civil rights laws or regulations.
- Infer information about workers engaging in activity protected by state or federal law.
- Make inferences about an individual's emotional state.
- Make inferences about an individual based on their gait.
- Collect neural data.

An employer also cannot use these tools to infer a worker's protected status. The bill also provides that an employer shall not use facial recognition technology to make inferences about a worker for firing, deactivation, or disciplinary purposes.

There are a host of exemptions and a carveout for using workplace surveillance tools to ensure safety, provided that the tool does not incorporate AI that makes inferences or predictions based on a worker's emotional, gait, neural data, protected status, or about activity protected by state or federal law.

The Labor Commissioner is authorized to investigate alleged violations and grant specified relief. Civil enforcement actions can be brought by the Labor Commissioner, public prosecutors, and workers, or their representatives.

According to the author:

Workplace surveillance has evolved into highly invasive systems that track worker movements and collect massive amounts of data. Current laws fail to protect workers from these practices. AB 1883 will prohibit the use of invasive surveillance systems in the workplace, systems that pose profound risks not just to employee privacy but also to unaccountable discrimination. It also prohibits the use of surveillance tools to infer protected and personal information about workers, including immigration and health status, and the likelihood of unionizing or speaking up against workplace violations.

3. Stakeholder positions

A large coalition of labor organizations and advocacy groups, including the Teamsters California and the California Teachers Association, write in support:

Employers have used surveillance to monitor, manage, and control workers for decades. However, today's employers now have access to a plethora of AI enabled surveillance tools capable of analyzing a worker's gait, neural activity, emotional state, and face. AI enabled surveillance differs from traditional video and audio monitoring in several ways. For one, these tools strip workers of their biometric data, essentially committing a full-scale invasion of workers' physical, mental, and emotional space at all hours of the day. Rather than requiring a human to monitor live surveillance feeds, today's tools utilize active AI monitoring that are capable of monitoring workers with zero interruptions. Heart rate, perspiration, facial expressions, and eye movements are tracked and used as data points to target "unproductive" workers and to "minimize risk" in the workplace.

AI tools rely on black-box algorithms to surveil workers. Data from emotion recognition, neural sensors, and facial and gait sensors are not just observations, but analysis of the data collected. Not only is that data potentially unreliable, but it can have bias built in, further exacerbating discrimination and inequities. For example, tools that utilize emotion recognition technology may very well fail to understand cultural nuances of expression and may be trained on biased information that inaccurately tags certain forms of speech as "aggressive" or "inappropriate." Similarly, facial recognition has a long history of failing to accurately recognize people of color, thus automating discrimination on a massive scale.

In order to protect workers from unregulated forms of military grade surveillance technology, AB 1883 prohibits employers from deploying gait, emotional, and neural recognition technologies in the workplace. AB 1883 also sets guardrails on the use of facial recognition technology by prohibiting employers from using the technology to make inferences to fire, discipline, or deactivate a worker. AB 1883 also prohibits employers from using any surveillance tool to infer personal and sensitive information of a worker such as their immigration status, gender identity, or sexual orientation and if a worker is exercising their protected rights. Lastly, the bill prohibits the use of any AI tool that prevents compliance with or violates any federal, state, or local labor, occupational health and safety, employment, or civil rights laws or regulations.

A large coalition of associations representing public employers, including the California State Association of Counties, writes in opposition:

We have fundamental concerns with this and other bills that aim to restrict how public agencies can use the tools defined as “workplace surveillance tools,” which we believe are essential and, in many cases, routine tools used for security.

- We oppose any legislation that will compromise health, safety, and security for our employees, the public we serve, and our officials.
- We oppose any legislation that compromises our ability to conduct investigations into fraud, waste, or abuse.
- We do not believe it is appropriate to regulate tools used for security and basic operations in response to private sector labor concerns. State law has protected the right of public employees to bargain and most public employees have a property interest in their position that is protected by due process.

AB 1883 would impose several rules on how public agencies may use surveillance tools – a term that is vast in its application, including video cameras, ID badge or key fob access, digital workplace messaging collaboration platforms (e.g. Microsoft Teams or Slack), and a wide array of tools used to keep workplaces safe, conduct essential government services, and protect against abuse, fraud, and waste of public resources.

We understand the reasonable concerns one could have about the rapid integration of surveillance tools into every aspect of daily life, particularly as new technologies emerge. However, we are concerned that this bill and others aimed at limiting workplace technology are too broad, too expensive, and too dangerous for public agencies and those we serve.

4. Amendments

In response to concerns raised about the breadth of the bill, the author has agreed to a series of amendments that dramatically narrow the bill. As agreed to be amended, the bill prohibits an employer from using a workplace surveillance tool that uses AI on workers that is capable of recognizing or making inferences or predictions about an individual’s emotional state or of collecting neural data.

SUPPORT

California Federation of Labor Unions, AFL-CIO (sponsor)
Alameda Labor Council
American Federation of Musicians, Local 7

American Federation of State, County and Municipal Employees (AFSCME) California
California Alliance for Retired Americans (CARA)
California Conference Board of the Amalgamated Transit Union
California Conference of Machinists
California Employment Lawyers Association
California Faculty Association
California Federation of Teachers AFL-CIO
California Nurses Association
California Professional Firefighters
California School Employees Association
California State Legislative Board of the Smart - Transportation Division
California State University Employees Union, SEIU Local 2579
California Teachers Association
Center on Policy Initiatives
Central Coast Labor Council
Central Labor Council, Fresno-Madera-Tulare-kings Counties, AFL-CIO
Communications Workers of America, District 9
Engineers and Scientists of California, IFPTE Local 20, AFL-CIO
Inland Empire Labor Council, AFL-CIO
Kapor Center Advocacy
North Bay Labor Council
North Valley Labor Federation
Orange County Labor Federation, AFL-CIO
Privacy Rights Clearinghouse
San Mateo County Central Labor Council
Service Employees International Union California
State Building and Construction Trades Council of California, AFL-CIO
Teamsters California
TechEquity Collaborative
Unite Here, AFL-CIO
Utility Workers Union of America, AFL-CIO
What We Will

OPPOSITION

Association of California Healthcare Districts (ACHD)
Association of California School Administrators
California Airports Council
California Association of Joint Powers Authorities (CAJPA)
California Association of Recreation & Park Districts
California Association of School Business Officials (CASBO)
California Manufacturers and Technology Association
California Special Districts Association
California State Association of Counties (CSAC)

California Transit Association
County Health Executives Association of California (CHEAC)
County of Kern
County of Riverside
Insights Association
League of California Cities
Public Risk Innovation, Solutions, and Management (PRISM)
Rural County Representatives of California (RCRC)
Southwest California Legislative Council
The Greater Coachella Valley Chamber of Commerce
Tri County Chamber Alliance
Urban Counties of California (UCC)

RELATED LEGISLATION

SB 947 (McNerney, 2026) establishes a comprehensive set of requirements governing the use of automated decision systems (ADS) in the workplace by requiring human oversight and independent corroboration when employers use ADS for decisions that impact workers' livelihoods. Certain types of ADS, such as those that infer sensitive information about workers or attempt to predict their behavior, are prohibited. The bill prohibits employers from relying solely on the ADS to make decisions involving discipline, termination, or deactivation. SB 947 is currently on the Assembly floor.

SB 238 (Smallwood-Cuevas, 2025) requires employers to provide the Department of Industrial Relations (DIR) with an annual notice on all workplace surveillance tools being used in the workplace along with specified details regarding them, such as what information they collect, what purposes they are being used for, and who will have access to that data. DIR is required to report to the Legislature regarding these notices. SB 238 is currently in the Assembly Privacy and Consumer Protection Committee.

AB 1221 (Bryan, 2025) would have regulated workplace surveillance technology by, in part, requiring employers to provide advanced notice before deploying these tools and information about them, restricts certain uses, and prohibits employers from selling or disclosing worker data, as provided. AB 1221 was held in the Assembly Appropriations Committee.

AB 1331 (Elhawary, 2025) regulates and limits the use of workplace surveillance tools, by both public and private employers, as specified. AB 1331 is currently on the Senate Inactive File.

PRIOR VOTES:

Assembly Floor (Ayes 52, Noes 12)

Assembly Appropriations Committee (Ayes 10, Noes 1)

AB 1883 (Bryan)

Page 12 of 12

Assembly Privacy and Consumer Protection Committee (Ayes 11, Noes 2)

Assembly Labor and Employment Committee (Ayes 5, Noes 0)
