SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2025-2026 Regular Session

SB 238 (Smallwood-Cuevas)
Version: March 26, 2025
Hearing Date: April 29, 2025
Fiscal: Yes
Urgency: No
CK

SUBJECT

Workplace surveillance tools

DIGEST

This bill requires employers to provide the Department of Industrial Relations (DIR) an annual notice on all workplace surveillance tools being used in the workplace along with specified details regarding them, such as who makes them, what information they collect, and who will have access to that data. DIR is required to publicly post these notices on their website.

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 does not limit the use of these tools or even place parameters on them. Rather, it ensures a level of transparency into the increasing use of these workplace surveillance tools by requiring employers to annually notify DIR of what tools they are deploying along with accompanying information such as who the tools will affect, the data that will be collected, and who will have access to the data collected.

This bill is author-sponsored. It is supported by the California Federation of Labor Unions and the California Association of Psychiatric Technicians. It is opposed by a large coalition of industry groups, including the California Retailers Association and the California Chamber of Commerce. This bill passed out of the Senate Labor, Public Employment and Retirement Committee on a vote of 4 to 1.

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 following:
    a) the categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected without providing the consumer with notice consistent with this section;
    b) if the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected without providing the consumer with notice consistent with this section; and
    c) the length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period, provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal

information was collected for longer than is reasonably necessary for that disclosed purpose. (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.)

8) Provides a consumer the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. It requires such a business to provide notice to consumers, as specified, that this information may be sold or shared and that consumers have the right to opt out of the sale or sharing of their personal information. (Civ. Code § 1798.120.)

9) Defines "personal information" as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The CCPA provides a nonexclusive series of categories of information deemed to be personal information, including biometric information, geolocation data, and "sensitive personal information." It does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. (Civ. Code § 1798.140(v).)

10) Extends additional protections to "sensitive personal information," which is defined as personal information that reveals particularly sensitive information. (Civ. Code § 1798.140(ae).)

11) Provides various exemptions from the obligations imposed by the CCPA, including where they would restrict a business' ability to comply with federal, state, or local laws. (Civ. Code § 1798.145.)

This bill:

1) Requires an employer to annually provide a notice to DIR of all workplace surveillance tools the employer is using in the workplace. If it began using a workplace surveillance tool before January 1, 2026, the employer shall provide the notice before February 1, 2026. DIR shall make the notice publicly available on its website within 30 days of receiving the notice from the employer.

2) Requires the notice shall contain all of the following information:
    a) The individuals, vendors, and entities that created the workplace surveillance tool and the individuals, vendors, and entities that will run, manage, or interpret the worker data gathered by the workplace surveillance tool.
    b) The name of the model and a description of the technological capabilities of the workplace surveillance tool.
    c) Any significant updates or changes made to the workplace surveillance tool that are already in use or any changes on how the employer is using the existing workplace surveillance tool.
    d) Whether the workplace surveillance tool will affect consumers or other individuals in addition to workers.
    e) The data that will be collected from workers or consumers by the workplace surveillance tool and whether they will have the option to opt out of personal data collection.
    f) A list of all entities and individuals other than the employer that will have access to the data collected from workers and consumers.
    g) Whether the employer has disclosed the use of the workplace surveillance tool with the affected workers and consumers.

3) Defines the relevant terms, including:
    a) "Worker" means a natural person or that person's authorized representative acting as a job applicant to, an employee of, or an independent contractor providing service to, or through, a business or a state or local governmental entity in a workplace.
    b) "Workplace surveillance tool" means any system, application, instrument, or device that collects or facilitates the collection of worker data, activities, communications, actions, biometrics, or behaviors, or those of the public, 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 use of a photo-optical system or other means.
    c) "Employer" means a person who 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. This shall include all branches of state government, or the several counties, cities and counties, and municipalities thereof, or any other political subdivision of the state, or a school district, or any special district, or any authority, commission, or board or any other agency or instrumentality thereof. This includes an employer's labor contractor.

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. 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, 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.[1]

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

[1] 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. All internet citations current as of April 19, 2025.

factors. This could magnify existing disability, racial, or gender inequalities in the workplace.[2]

2. Ensuring some transparency regarding workplace surveillance

This bill takes a measured approach to the issue by simply requiring more transparency around the use of these workplace surveillance tools, rather than banning them or otherwise limiting their use.

The bill complements existing privacy laws by requiring employers to provide notice to DIR when they are deploying workplace surveillance tools, defined as any system, application, instrument, or device that collects or facilitates the collection of worker data, activities, communications, actions, biometrics, or behaviors, or those of the public, 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 use of a photo-optical system or other means.

The notice must include details regarding the tools, such as the model name, who makes them, and what their capabilities are. Employers must further disclose any significant updates or changes to the tools or how they are used.

To further appreciate the reach and oversight of workplace surveillance, employers must include details about what data is being collected by the tools, who manages and interprets that information, and who will have access to the information on both workers and consumers, if applicable. The notice must state who will be affected outside of workers, such as consumers entering the workplace. Employers must indicate whether they disclose the use of these tools to those affected and whether workers are given the opportunity to opt out of personal information collection. These details are important given the potential encroachment on workers' privacy rights.

The bill requires the notice to identify "any significant updates or changes made to the workplace surveillance tool." This term is undefined and to address concerns this may lead to overly burdensome disclosure requirements for employers, the author has agreed to an amendment that provides the following definition: "'Significant updates or changes' means changes that materially alter the function or scope of the surveillance tool, including new forms of data collection, analysis capabilities, or new third-party access. Routine maintenance or changes that do not affect the tool's functionality or data use are not considered significant." To this same end, the author has agreed to

[2] '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.

amendments that carve out certain tools, such as spam filters, antivirus software, and server uptime monitors.

To ensure full disclosure, DIR is required to make these notices publicly available.

According to the author:

> SB 238 ensures transparency and accountability in using workplace surveillance tools and artificial intelligence by requiring employers to disclose what technologies they use, what data is collected, and who has access to that data. As AI increasingly shapes employment decisions without workers' knowledge, this bill provides a critical baseline for public oversight and worker empowerment. By making this information publicly accessible, SB 238 promotes fairness, privacy, and informed consent in the workplace, particularly for communities disproportionately impacted by surveillance and algorithmic bias.

There is some concern about requiring the employers to identify *individuals* who created the tools used. This could be interpreted to mean employees of the company developing the product. This seems somewhat unnecessary and perhaps its own invasion of a worker's privacy. The author may wish to consider more narrowly tailoring this provision.

In addition, the definition of "data" in the bill closely mirrors the definition of "personal information" in the CCPA and other statutes. The author has agreed to amendments that replace "data" with the term "personal information" to avoid confusion.

3. Stakeholder positions

The California Federation of Labor Unions writes in support:

> Workplace surveillance is not a new phenomenon, however, the tools currently available to employers are far more powerful and invasive than a simple camera or microphone. Employers now have access to seemingly military grade surveillance technology that can track heat signatures, biometrics, and walking patterns. A recent study published by coworker.org reported over 500 surveillance and management tools currently being sold to employers to track worker activities, interactions, and body movements. These tools are widely available and surprisingly affordable. Workers live in a constant state of surveillance and are often unaware they are even being watched.
>
> SB 238 seeks to increase transparency in the workplace by requiring employers to disclose their use of workplace surveillance tools to the

> Department of Industrial Relations. Transparency is essential to foster public trust and a safe working environment.

A coalition of industry groups, including the California Chamber of Commerce, writes in opposition:

> The breadth of information that SB 238 requires to be reported to DIR and made publicly available online is concerning to many of our members. The definition of workplace surveillance tools in the bill is very broad and encompasses many tools that are standard and basic components of a security program on an employer's premises or cybersecurity software. Video surveillance, communications/equipment tracking, and cybersecurity software are especially necessary for workplace safety as well as the prevention and investigation of fraud and theft. For example, financial institutions must have highly sophisticated security systems, otherwise there is risk of theft or exposure of sensitive consumer information. They would be required to disclose exactly which tools they use, the names of individuals and vendors that run or receive any of that data, and what changes have been made to those systems. This is essentially requiring those institutions to provide a roadmap for bad actors to gain a better understanding of the tools they are using for fraud prevention and security measures and how to exploit them. The bill could put many entities, and more importantly their employees and consumers, in a vulnerable position by exposing exactly what tools are being used and how they are being used, who has access to sensitive worker and consumer data, and the extent of data that is being collected. This is especially true for employers with sensitive consumer data or government data where companies have state or federal contracts.

SUPPORT

California Association of Psychiatric Technicians
California Federation of Labor Unions, AFL-CIO

OPPOSITION

Acclamation Insurance Management Services
Allied Managed Care
American Petroleum and Convenience Store Association
Associated General Contractors of California
California Alliance of Family Owned Businesses
California Apartment Association
California Association of Sheet Metal and Air Conditioning Contractors National Association

California Association of Winegrape Growers
California Attractions and Parks Association
California Beer and Beverage Distributors
California Chamber of Commerce
California Credit Union League
California Farm Bureau
California Grocers Association
California Hospital Association
California League of Food Producers
California Retailers Association
Coalition of Small and Disabled Veteran Businesses
Flasher Barricade Association
Housing Contractors of California
Los Angeles Area Chamber of Commerce
Security Industry Association
Wine Institute

RELATED LEGISLATION

Pending Legislation: SB 7 (McNerney, 2025) regulates the use of automated decision systems (ADS) in the employment context by requiring employers and their vendors to provide pre- and post-use notices that inform workers, including applicants, that they are subject to ADS and of the ADS details. It establishes a series of prohibited uses. Workers have the right to access information used by the ADS, to correct that information, and to appeal any decision made by ADS. SB 7 is being heard by this Committee the same day as this bill.

Prior Legislation: AB 302 (Ward, Ch. 800, Stats. 2023) required CDT, on or before September 1, 2024, to conduct a comprehensive inventory of all high-risk ADS that have been proposed for use, development, or procurement by, or are being used, developed, or procured by, any state agency.

PRIOR VOTES:

Senate Labor, Public Employment and Retirement Committee (Ayes 4, Noes 1)

****