Date of Hearing: July 8, 2025
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 238 (Smallwood-Cuevas) – As Amended May 1, 2025

SENATE VOTE: 27-10

PROPOSED AMENDMENTS

SUBJECT: Workplace surveillance tools

SYNOPSIS

Presumably, the right to privacy should not be a commodity that one is required to exchange for the opportunity of employment – or for people to access goods and services, for that matter. While employers surveilling their workers, both during and after work hours, is far from a new phenomenon, advances in affordable surveillance technology have made that surveillance much more intrusive. As with personal information in general, employers are able to collect vast dossiers on their employees by gathering sweeping amounts of data about every aspect of their jobs and personal lives. Many workers, while generally aware they are being monitored, are not aware of the extent of the surveillance or what is being done with the information.

Employers are using more surveillance technology than ever — digital cameras, motion scanners, Radio Frequency Identity (RFID) badges, Apple Watch badges, Bluetooth beacons, keystroke logging — to track every single movement of workers in the office and to gauge their productivity, potentially without the employee knowing that they are being surveilled or what personal information is being collected. Some workplaces are using biometric data such as eye movements, body shifts, and facial expressions, captured by webcams to evaluate whether or not employees are being sufficiently attentive in their work tasks. Even body temperature, sweat, and frequency of bathroom visits can be tracked and analyzed.

This bill requires private and public employers to provide an annual notice to the Department of Industrial Relations (DIR) of all workplace surveillance tools the employer is using in the workplace with specified information about their technological capabilities and uses.

The proposed Committee amendments, detailed in Comment #4, conform the definition of "workplace surveillance tool" to the definition contained in AB 1331 (Elhawary).

This bill is author sponsored. It is supported by Oakland Privacy, Consumer Federation of California, and the California Association of Psychiatric Technicians. Among the opponents are a coalition of eight local government associations, including the League of California Cities and the California State Association of Counties.

This bill was previously heard by the Assembly Labor and Employment Committee, where it passed on a 5-1-1 vote.

THIS BILL:

1) Defines "employer" to mean 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. "Employer" includes an employer's labor contractor.

2) States that the term "employer" further includes 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.

3) Defines "personal information" to mean any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to a worker or a consumer, regardless of how the information is collected, inferred, or obtained.

4) Defines "significant updates or changes" to mean changes that materially alter the function or scope of the surveillance tool, including new forms of data collection or 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.

5) Defines "worker" to mean 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.

6) Defines "workplace surveillance tool" to mean any system, application, instrument, or device that collects or facilitates the collection of worker personal information, 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.

7) Requires an employer to annually provide a notice to DIR of all workplace surveillance tools the employer is using in the workplace. An employer is not required to report tools that are used exclusively for basic information technology operations, such as spam filters, antivirus software, or server uptime monitors.

8) Requires an employer who began using a workplace surveillance tool before January 1, 2026, to provide the notice before February 1, 2026.

9) Requires the notice to 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 personal information 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 personal information 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 information collection.

f) A list of all entities and individuals other than the employer that will have access to the personal information collected from workers and consumers.

g) Whether the employer has disclosed the use of the workplace surveillance tool with the affected workers and consumers.

10) Requires the DIR to make the notice publicly available on its internet website within 30 days of receiving the notice from the employer.

EXISTING LAW:

1) Provides, pursuant to the California Constitution, that all people are by nature free and independent and have inalienable rights. Among these is the fundamental right to privacy. (Cal. Const. art. I, § 1.)

2) States that the "right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them." Further states these findings of the Legislature:

   a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies.

   b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.

   c) In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits. (Civ. Code § 1798.1.)

3) States that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society. (Pen. Code § 630.)

4) Prohibits a person from intentionally and without the consent of all parties to a confidential communication, using an electronic amplifying or recording device to eavesdrop upon or record the confidential communication.

    a) For purposes of this section, defines a "person" to mean an individual, business association, partnership, corporation, limited liability company, or other legal entity. (Pen. Code § 632.)

5) Enacts the California Electronic Communications Privacy Act (CalECPA), which generally prohibits a government entity from compelling the production of or access to electronic communication information from a service provider or to electronic device information from any person or entity other than the authorized possessor of the device, absent a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant to specified conditions, or pursuant to an order for a pen register or trap and trace device, as specified. (Pen. Code § 1546 et seq.)

6) Establishes the California Consumer Privacy Act (CCPA). (Civ. Code §§ 1798.100-1798.199.100.)

7) Provides a consumer, subject to exemptions and qualifications, various rights, including the following:

    a) The right to know the business or commercial purpose for collecting, selling, or sharing personal information and the categories of persons to whom the business discloses personal information. (Civ. Code § 1798.110.)

    b) The right to request that a business disclose the specific pieces of information the business has collected about the consumer, and the categories of third parties to whom the personal information was disclosed. (Civ. Code § 1798.110.)

    c) The right to request deletion of personal information that a business has collected from the consumer. (Civ. Code § 1798.105.)

    d) The right to opt out of the sale of the consumer's personal information if the consumer is over 16 years of age. (Sale of the personal information of a consumer below the age of 16 is barred unless the minor opts-in to its sale.) (Civ. Code § 1798.12.)

    e) The right to direct a business that collects sensitive personal information about the consumer to limit its use of that information to specified necessary uses. (Civ. Code § 1798.121.)

    f) The right to equal service and price, despite the consumer's exercise of any of these rights, unless the difference in price is reasonably related to the value of the customer's data. (Civ. Code § 1798.125.)

COMMENTS:

1) **Author's statement**. 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.

2) **The evolution of workplace surveillance.** Employers surveilling their workers, both during and after work hours, is far from a new phenomenon. For almost 200 years, if not longer, employers have been watching their employees' activities. The roots of employers actively surveilling their workers in the United States can be traced back to the counting of the North-Western Police Agency, later known as the Pinkerton National Detective Agency, in 1855. The agency was borne out of employers' desire for more control over their employees, both inside and outside of work. Pinkerton detectives fulfilled that need. Among the roles played by the detectives were monitoring workers who were deemed to be a threat to an employer's interests; infiltrating and busting unions; and enforcing company rules.[1]

Early efforts at surveilling workers were limited by both the cost of hiring people to watch workers and the lack of technology. Henry Ford, often remembered as the inventor of the modern assembly line, infamously used to prowl his factory floor, timing his workers' motions with a stopwatch looking for ways to improve efficiency. As with other employers, he also used private investigators to spy on his workers when they were off work to discover if they had any personal problems that could hinder their work.[2]

As the 20th century wore on, punch time clocks, which allowed employers to track their workers' work time down to the minute, gave way to closed circuit video cameras, and then starting in the 1980s, computer monitoring became increasingly common.[3] Even then, it was not humanly possible for employers to monitor their workers 24 hours a day, 7 days a week.

Over the last 40 years, advances in technology have allowed employers to surveil their workers in ways that could only have been imagined in science fiction novels. Punch cards have given way to biometric scans, key cards and workplace badges are giving way to RFID tags. A person could not be blamed for finding that technology almost quaint, given the other 21st Century advances in surveillance technology.

Regardless of the type of work employees do, whether it what has been traditionally termed "blue-collar" for the working class, or "white-collar" for the management and professional class, most employees are likely being constantly watched by their employers. For those using computers, whether desktop or laptop, in an office or working remotely, surveillance tools capture their keystrokes and remotely monitor the websites they search on their browsers. As

---

[1] Ifeoma Ajunwa, et al. "Limitless Worker Surveillance" *105 California Law Review 735* (2017) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746211
[2] *Ibid.*
[3] *Ibid.*

more workers shifted to remote work during the COVID pandemic, employers required their workers to install "bossware" on their home computers, introducing a plethora of invasive surveillance tools into their personal computers and their homes.

Over the last five years, surveillance tools have become more affordable and more intrusive. As with personal information in general, employers are able to collect vast dossiers on their employees, by gathering sweeping amounts of data about every aspect of their jobs and personal lives. Often that is done "without employees' full informed or free consent. Many workers, while generally aware they are being monitored, don't know the extent of the surveillance or what is being done with the information."[4]

Employers are using more surveillance technology than ever — digital cameras, motion scanners, RFID badges, Apple Watch badges, Bluetooth beacons, keystroke logging — to track every single movement of workers in the office and to gauge their productivity. Some workplaces are using biometric data such as eye movements, body shifts, and facial expressions, captured by computer webcams, to evaluate whether or not their employees are being appropriately attentive in their work tasks. As an example, artificial intelligence (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.[5] 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. According to the author, at least one company sells biometric ID badges with microphones, sensors, and other tools to record conversations, monitor speech, body movements, and location.[6] Even body temperature, sweat, and frequency of bathroom visits can be tracked and analyzed by employers.

A recent article in *MIT Technology Review* describes one company's surveillance tool this way:

> Companies that use electronic employee monitoring report that they are most often looking to the technologies not only to increase productivity but also to manage risk. And software like Teramind[7] offers tools and analysis to help with both priorities. While Teramind, a globally distributed company, keeps its list of over 10,000 client companies private, it provides resources for the financial, health-care, and customer service industries, among others—some of which have strict compliance requirements that can be tricky to keep on top of. The platform allows clients to set data-driven standards for productivity, establish thresholds for alerts about toxic communication tone or language, create tracking systems for sensitive file sharing, and more.
>
> [. . .]
>
> Selecting and tuning the appropriate combination of data is up to Teramind's clients and depends on the size, goals, and capabilities of the particular company. The companies are

---

[4] *Ibid.*
[5] Kevin Roose, "A Machine May Not Take Your Job, but One Could Become Your Boss," *New York Times* (Jun. 23, 2019) https://www.nytimes.com/2019/06/23/technology/artificial-intelligence-ai-workplace.html
[6] Humanyze: The Future of Workforce & Market Intelligence https://humanyze.com/
[7] https://www.teramind.co/solutions/compliance-management/

> also the ones to decide, based on their legal and compliance requirements, what measures to take if thresholds for negative behavior or low performance are hit.[8]

3) **Case study: Amazon.** Perhaps the most extreme example of the intrusive surveillance tools used by employers can be found at Amazon. According to documents filed by Amazon workers with the National Labor Relations Board, Amazon tracks every minute that their workers spend off of their tasks. To do this, they use handheld scanners that are also used to track packages. The worker claim they "can receive a written warning for accumulating 30 minutes of time off task in a day one time in a rolling one-year period. They can be fired if they accumulate 120 minutes of time off task in a single day or if they have accumulated 30 minutes of time off task on three separate days in a one-year period."[9] Counted among the activities considered "time off task" are going to the bathroom, talking to another worker, or going to the wrong work station. Workers reported that they were afraid to go to the bathroom or get a drink of water for fear of being disciplined.[10] At the end of each shift, supervisors are required to interrogate the worker with the highest time off task.

Along with the handheld devices, Amazon uses an AI camera system trained on each workstation analyzing workers' movements. The cameras automatically register the location of products and catalog every mistake workers make.[11] Monitoring the workers' non-stop manual also helps improve the AI computer system, which learns from the responses of Amazon's video reviewers and becomes more accurate over time.[12]

Oxfam, an international organization focused on fighting global poverty, conducted an investigation into the workplace surveillance practices at both Amazon and Walmart warehouses in the United States. Employers, like Amazon, often claim that their surveillance systems are designed to make workers safer. "However, in recent years worker groups have decried the high injury rates and horrific working conditions that workers encounter as Amazon employees."[13] The report describes the surveillance technology as follows:

> The scanners play a key role in the surveillance machine because what the scanner records can lead to "Associate Development and Performance Trackers," or "ADAPTs," which are automated write-ups that penalize workers for not meeting production goals. In addition, hundreds of security cameras are constantly monitoring the warehouse floor, ready to notify a manager when a worker is away from their station for too long. Badges are another form of worker surveillance, allowing managers to track when workers start or end their shifts, when they take their breaks, and their location across the warehouse. Being monitored this minutely takes a physical and mental toll as workers need to make decisions about taking

---

[8] Rebecca Akermann, "Your Boss is Watching," *MIT Technology Review* (Feb. 24, 2025

[9] Lauren Kaori Gurley, "Internal Documents Show Amazon's Dystopian System for Tracking Workers Every Minute of Their Shifts" *Vice* (Jun. 2, 2022) https://www.vice.com/en/article/internal-documents-show-amazons-dystopian-system-for-tracking-workers-every-minute-of-their-shifts/

[10] *Ibid.*

[11] Niamh McIntyre and Rosie Bradbury, *The eyes of Amazon: a hidden workforce driving a vast surveillance system*, The Bureau of Investigative Journalism (Nov. 21, 2022) https://www.thebureauinvestigates.com/stories/2022-11-21/the-eyes-of-amazon-a-hidden-workforce-driving-a-vast-surveillance-system/

[12] *Ibid.*

[13] *At Work and Under Watch: Surveillance and suffering at Amazon and Walmart warehouse*, Oxfam (Apr. 10, 2024) https://www.oxfamamerica.org/explore/research-publications/at-work-and-under-watch/

> breaks, eating, going to the bathroom, or even drinking water with their pace or performance metrics in mind.
>
> [. . .]
>
> Another example of the detailed metrics that Amazon monitors is a worker's units per hour (UPH) score, which records how many actions a worker is able to accomplish in an hour. . . . [W]orker metrics are prominently displayed on a monitor, which keeps workers psychologically primed to constantly worry about "making rate" and about how they are doing compared with their co-workers. . . . Importantly, workers are not told what the data that electronic devices are constantly collecting is being used for, nor are they properly notified of their privacy rights.

4) **Amendments.** AB 1331 (Elhawary), similar to this measure, also focuses on technology that surveils workers. AB 1331 and this bill, however, have somewhat different definitions of "workplace surveillance tool." The author has agreed to an amendment that make the definitions in this bill compatible with the definition in AB 1331. The amendment is as follows:

> 1550. (f) "Workplace surveillance tool" means a~~ny~~ system, application, instrument, or device that collects or facilitates the collection of ***information about the*** worker***s'*** ~~**personal information,**~~ activities, communications, actions, biometrics, or behaviors, or ~~**those of**~~ ***about*** the public***, that are capable of passively surveilling workers***, 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.**~~ ***electronic workplace tracking, geolocation, electromagnetic tracking, photoelectronic tracking, or utilization of a photo-optical system or other means. "Workplace surveillance tool" does not include smoke or carbon monoxide detectors or weapon detection systems that automatically screen a person's body.***

ARGUMENTS IN SUPPORT: Oakland Privacy writes in support:

> As a privacy group, we want to focus this letter on the intersection between the proposal in Senate bill 238 and already existing privacy protections. When the California Consumer Privacy Act (CCPA) was enacted, it contained an exemption or carve-out for workers who were employed by covered employers. That exemption sunsetted and was not renewed and qualified California employers became subject to the CCPA and the succeeding ballot initiative, the California Privacy Rights Act, CPRA. Because SB 238 enacts its protections into the labor code, rather than into the Civil Code under CPRA, it is important that both its provisions and its remedies be consistent with the privacy protections in the civil code. We believe that to be the case and it is an essential factor in our support for the bill.
>
> As one might expect from a law titled the California Consumer Privacy Act, the CCPA and its later amendment are focused on the public as consumers. We recognize that employer/employee is a different kind of relationship than business/customer and that the power dynamics in place are substantially different.
>
> That is why we see enhanced protections for workers on top of the basement protections provided by the comprehensive statewide data privacy law to be appropriate, including the enforcement agent being the Labor and Workforce Agency.

Another element that SB 238 adds to privacy protections available to California workers is to extend the protections in this bill to workers who work for public employers in the state, as well as to companies too small to be covered entities under CPRA. For these employees this bill, or one like it, would be the only workplace privacy protections they would be eligible for. For that reason alone, workplace privacy protections in addition to CPRA are neither duplicative nor excessive.

The protections provided by Senate Bill 238, while they do go beyond the right to know, right to correct, and right to opt-out structure provided by CPRA, are fairly basic. They include prompt and informed notice requirements that are delivered within 30 days that include meaningful information about the technological tools being used, who runs and operates them, what data will be collected, who will have access to it and whether it is possible to opt out of the collection if one wishes. These parameters are similar to what a best practice "privacy policy" on a consumer website is supposed to provide and essentially maintains the right to know and the right to opt out (when possible) in a proactive rather than reactive fashion. It makes perfect sense to place the burden of a reporting mechanism on employers rather than placing the burden of inquiry on employees who may be scared or intimidated to launch such inquiries - and thus this bill protects their right to know.

From a fiscal point of view, California's economic vitality is tied to the energy, morale and initiative of its workforce, and the dystopian workplace of science fiction is likely incompatible with a dynamic economy. Protective measures like SB 238 to keep human workers in California motivated and empowered are an important way to maintain the world's 4th largest economy and California's reputation for imagination and innovation.

To address the elephant in the room, a more aggressive bill on employee surveillance, Issac Bryan's AB 1221, did not survive the appropriations process. The opposition to that bill has now turned their attention to SB 238, which is a much more measured bill. We find this misguided. Many of the concerns directed at the Assembly bill are addressed in Senate Bill 238 and the approach here is very balanced.

ARGUMENTS IN OPPOSITION: In opposition to the bill, a coalition of local government organizations argues:

SB 238 Would Widely Apply to Many Technologies
We understand the reasonable concerns about the slow creep of surveillance tools into every aspect of daily life. However, the scope of this bill is vast and would deem banal tools used for everyday work, including badge access, collaboration tools like Teams or Slack, or GPS tools used to track fleets, to be "surveillance tools" whose use could be covered by this bill. Under SB 238, any device that collects or facilitates collection of data of an employee's activities, actions, communications, behaviors, personal information, or biometrics, or those of the public, is deemed a surveillance tool. Given the bill's broad scope, the burdens from compliance with its notification requirements are significant.

SB 238 Would Jeopardize Local Government and Schools Security Efforts
SB 238 would require reporting to the Department of Industrial Relations (DIR), and for the DIR to thereafter publicize, sensitive data on which tools public employers use, their capabilities, and the names of individuals and vendors that run the systems or receive data. Disclosure of this information could provide a material advantage to bad actors seeking to exploit vulnerabilities or gaps in coverage.

Due to the unique aspects of public sector service delivery, public employers may use a variety of surveillance tools to protect employees, students, or the public at large, including emergency alarms for teachers, body cameras for law enforcement, or tools used for public vehicle fleets, including dash cameras, speed monitors, or GPS tracking. Local governments are responsible for securing and operating critical infrastructure, jails, hospitals, police and fire departments, and protecting students in schools.

Further, we have seen rising hostility and threats against government entities and their workforces. That includes violence and threats of violence against government employees whose job requires them to serve the public like library staff, teachers, firefighters, benefits officers, among myriad other examples.

Reporting and publication of the detailed information required by SB 238 could set back public employers' efforts to protect employees and the public.

SB 238 is an Unfunded Mandate on Local Budgets
The initial and ongoing reporting obligations required by this bill will burden local human resources and information technology departments, increasing costs and diverting them from their core responsibilities. This constitutes an unfunded mandate on public employers without a clear need. For schools, this is a drain of Proposition 98 funding.

REGISTERED SUPPORT / OPPOSITION:

Support

California Association of Psychiatric Technicians
California Federation of Labor Unions, Afl-cio
Consumer Federation of California
Oakland Privacy

Oppose

Acclamation Insurance Management Services
Allied Managed Care
American Petroleum and Convenience Store Association
Associated General Contractors
Association of California Healthcare Districts (ACHD)
Association of California School Administrators
California Alliance of Family Owned Businesses
California Apartment Association
California Association of Joint Powers Authorities (CAJPA)
California Association of Sheet Metal & 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 Landscape Contractors Association
California League of Food Producers
California Retailers Association
California Special Districts Association
California State Association of Counties (CSAC)
Coalition of Small and Disabled Veteran Businesses
Flasher Barricade Association
Housing Contractors of California
League of California Cities
Los Angeles Area Chamber of Commerce
Pacific Association of Building Service Contractors
Rural County Representatives of California (RCRC)
Security Industry Association
Urban Counties of California (UCC)
Western Car Wash Association
Wine Institute

Oppose Unless Amended

California Airports Council

Analysis Prepared by: Julie Salley / P. & C.P. / (916) 319-2200