Date of Hearing: April 16, 2026
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 1883 (Bryan) – As Amended March 12, 2026

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 can 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 employees are being appropriately attentive in their work tasks. Even body temperature, sweat, and frequency of bathroom visits can be tracked and analyzed by employers.

This bill, sponsored by the California Labor Federation, seeks to regulate a specific subset of particularly invasive and scientifically questionable practices, including inferring information about workers engaging in a protected activity; making inferences about a person's emotional state; making inferences about an individual based on their gait; or collecting neural data. The bill also states that nothing prohibits employers from using workplace surveillance tools to ensure safety, provided that the tool does not incorporate artificial intelligence that makes inferences or predictions about a worker's emotional state, gait, protected status, a protected activity, or collect neural data.

This bill is supported by over one dozen labor and privacy organizations. It is opposed by a number of business and local government organizations, including the California State Association of Counties, League of California Cities, the California Chamber of Commerce, and the California Grocers Association.

This bill was previously heard by the Labor and Employment Committee, where it passed on a 5-0 vote. If passed by this Committee, it will next be referred to the Judiciary Committee.

EXISTING LAW:

1) Provides, pursuant to the California Constitution, that all people are free and independent by nature 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.)

    a. 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 confidential communication.

    b. 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.)

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

5) 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.)

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, health and safety, employment or civil rights laws or regulations.

   b. Infer information about workers engaging in a protected activity.

   c. Make inferences about a person's emotional state.

   d. Make inferences about an individual based on their gait.

   e. Collect neural data.

2) Prohibits an employer from using facial recognition technology unless it is strictly used to open a locked device or grant access to a secure area.

3) Defines the following:

   a. "Employer" means a person or governmental entity that directly or indirectly, or through another person, employs or exercises control over a worker, as defined. "Employer" also includes an employer's labor contractor.

   b. "Facial recognition technology" means an AI tool that analyzes a person's facial features and attempts to identify, verify, or track the person in a still or video image.

   c. "Neural data" to mean information that is generated by measuring the activity of a worker's central or peripheral nervous system, and that is not inferred from nonneural information.

   d. "Worker" to mean 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.

e. "Workplace surveillance tool" to mean 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, 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.

4) States that nothing prohibits employers from using workplace surveillance tools to ensure safety, provided that the tool does not incorporate artificial intelligence that makes inferences or predictions about a worker's emotional state, gait, protected status, a protected activity, or to collect neural data.

5) Provides for enforcement by the Labor Commissioner, public prosecutor, workers, or the workers' representative.

COMMENTS:

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

2) **Surveillance tools in the workplace.** 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]

---

[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.*

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.

Over the last five years, surveillance tools have become more affordable and more intrusive. As with personal information in general, employers can collect vast dossiers on their employees, 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 at their workplace 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 their employees are 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. 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.

---

[3] *Ibid.*
[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/

> [. . .]
>
> 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 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]

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 claims 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 workstation. 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 manually 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, investigated 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," Oxfam's report states, "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.

---

[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/

[. . .]

> 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.

3) **This bill.** Prior to the recent amendments, this bill prohibited the use of certain technologies by employers on their employees. Specifically, emotion recognition technology, gait recognition technology, and technology that can collect neural data. The amendments substantially tighten the language to narrowly prohibit specific practices. Allowing employers to continue to use surveillance technology. The only technologic specific restriction is related to facial recognition technology, which can only be used for two purposes – to open a locked device or grant access to locked or secured areas. That restriction remains in the bill.

In addition to moving toward largely technology neutral language, to make it clear that surveillance technology was not banned, the amendments added language stating that the bill does not prohibit an employer from using a workplace surveillance tool for safety or security purposes as long as it is not used for the prohibited purposes.

4) **Opposition concerns.** A coalition of local government employers, including the League of California Cities and the California State Association of Counties, have raised several concerns about limiting the use of surveillance technology in the workplace:

> It is unclear how a court could interpret the meaning of this bill. While we understand and sympathize with the concerns this bill intends to address, our concern is that a reasonable interpretation could blanketly prohibit routine tools used for security, operations, or public health.
>
> Routine security tools like security cameras, key fobs, ID badges, digital workplace collaboration platforms (e.g. Teams or Slack), or GPS trackers passively collect worker data, including when they are actively working at a computer or cell phone or where they are at a given point in a day. Section 1581(a)(1)(B) prohibits any tool that identifies or infers information about workers engaging in activity protected by state or federal law.
>
> We believe it is critical to protect the civil and labor rights of the public workforce. Our concern is that an overbroad interpretation of what it means to "identify," or "infer," worker information could endanger essential tools that, while not designed or used to intentionally undermine the rights of employees, may passively collect information that happens to meet the law's threshold for an outright ban on their use.
>
> While some technologies identified in the bill conjure images from science fiction, we are concerned that their breadth could sweep in routine or innocuous technologies and have other unforeseen operational or safety consequences for public agencies.

The recent amendments appear to address many of the concerns related to prohibiting the use of surveillance tools. Surveillance technology used in the workplace would still be permitted. Employers simply cannot use them for narrow, overly invasive purposes.

It is important to note that the opposition's suggestion that the bill "conjures images from science fiction" is inaccurate, however. Surveillance technology companies are currently marketing and deploying surveillance tools that claim to collect neural data, make determinations about a person based upon their gait, and determine a person's emotional and psychological state.

Emotion recognition. As an example, Affectiva, Inc., a spin-off from the MIT Media Lab, has developed emotion AI, specializing in analyzing facial expressions and vocal tones to assess emotional responses.[14] According to their website, Affectiva is a facial expression module that uses facial analysis and "a suite of other biometric sensors" allowing the tool to "simultaneously capture and analyze facial expressions alongside physiological arousal indicators, brain activity, eye tracking, voice analysis, heart rate, and more. This synergy of data sources allows for a complete and nuanced understanding of human behavior, actions, and thoughts."[15]

Gait recognition. Gait recognition is the identification of individuals based on their walking patterns. Researchers point to its potential to accurately identify individuals from a distance. "Gait recognition systems involve a complex integration of technical, operational and definitional choices and have been applied in a variety of contexts such as security, medical examinations, identity management, and access control."[16] Recfaces, a biometric identification company, provides tools intended to identify a person based on their walk and movements. On their website they state:

> A person's gait is as unique as their voice timbre. Leveraging this knowledge, gait recognition technology has been developed using Machine Learning (ML) algorithms. ML-based systems can identify a person from an image even if their face is out of view, turned away from the camera, or concealed behind a mask. The system analyzes the silhouette, height, speed, and walking characteristics to identify individuals from a database. This technique is more convenient than retinal scanners or fingerprints in public places as it is unobtrusive. Moreover, gait recognition is unlikely to be fooled – every person's gait has no duplicates.[17]

Neural data collection. The term neurotech device is a catchall term for gadgets that, with the help of dry electrodes, connect human brains to computers and algorithms that analyze the brain-wave data. Neurotechnology, while initially used in medical research, is becoming more common in the workplace as a means to monitor workers. Examples of this technology include SmartCaps, developed and marketed by Wenco, a company that focuses on mine safety equipment. According to the company, "The Wenco SmartCap fatigue monitoring solution is built around the LifeBand, a battery-powered wearable device that produces highly accurate measures of alertness and fatigue impairment by measuring EEG (electroencephalogram), more

---

[14] *Top 10 Companies in Global Emotion AI Market in 2025*, Emergen Research (Nov. 14, 2025). https://www.emergenresearch.com/blog/top-10-companies-in-global-emotion-ai-market.
[15] Product: Human Behavioral Research with iMotions. https://www.affectiva.com/product/imotions-behavioral-research/.
[16] Rani, V., Kumar, M. Human gait recognition: A systematic review. Multimed Tools Appl 82, 37003–37037 (2023). https://doi.org/10.1007/s11042-023-15079-5.
[17] *Gait recognition system: deep dive into this future tech,* https://recfaces.com/articles/what-is-gait-recognition.

commonly known as 'brainwaves'."[18] While marketed as a safety tool designed to alert the wearer if they are becoming fatigued or distracted, the company notes, "The real-time data produced by SmartCap is owned by the customer and hosted on the cloud. Our LifeHub management application allows custom configuration, reporting and monitoring to enable real-time actionable insights."[19]

While many may wish that these technologies were simply science fiction or something imagined for a far-off future, these tools are real. Whether the tools are accurate and work as advertised however remains an open question. Regardless, the tools are increasingly common in the workplace.

ARGUMENTS IN SUPPORT: California Federation of Labor Unions, sponsors of the bill, write in support:

> Employers have used surveillance to monitor, manage, and control workers for decades. From auto assembly lines to Amazon warehouses, surveillance has enabled companies to ensure maximum productivity and control. Artificial intelligence has supercharged workplace surveillance and taken it to a new level. Today's employers now have access to surprisingly affordable high-tech surveillance equipment. These AI surveillance tools not only watch workers but extract, compile, and analyze troves of data instantly to recognize emotions, analyze neural data, and detect faces and gait for the sake of maximizing productivity.
>
> Gait recognition technology has become widespread in recent years. Capable of identifying an individual by analyzing their walking pattern and body shape, gait technology is an extremely powerful form of biometric surveillance. Companies such as KZero market gait recognition services across a multitude of industries. KZero touts that these tools can aid in "identifying health risks in individuals…information that may be included as a factor when determining insurance premiums for health and life insurance policies." Evidently, employers can use gait to not only identify workers but make decisions impacting their employment based on a machine analyzing their physical movements.
>
> Emotion recognition technology has also seen a boom in the workplace in recent years. Emotion recognition uses biometric data such as a person's facial expression, heart rate, skin conductance, or tone of voice to infer a person's emotional state. Verint, formerly known as Cogito, has developed emotion recognition technology that has been used on call center workers for MetLife and Humana. In both instances, call center workers were monitored by the emotion recognition tool to ensure the caller provided a happy and receptive tone when speaking to customers. The system would additionally provide a report to supervisors with details of which call center workers received the highest number of suggestions.
>
> Neural recognition technology is a new addition to the workplace surveillance landscape. It is purported to capture the brain activity of a person's central and peripheral nervous system to supposedly identify when a worker is concentrating, tired, or stressed. Emotiv, a developer of neural recognition hardware and software, offers their tools to employers under the premise that "understanding a worker's true mental and cognitive state is the key to…an

---

[18] *The SmartCap Solution,* Wenco. https://www.wencomine.com/our-solutions/safety.
[19] *Ibid.*

improvement in ROI." Employers' use of neural data can ostensibly allow them to extrapolate the private opinions and feelings of workers that they have not chosen to share.

Facial recognition technology, arguably the most normalized form of surveillance, has existed in the workplace for years. Tools, such as Amazon's Rekognition, have become easily accessible for businesses and individual consumers. Employers can use facial recognition for tracking attendance and tardiness, productivity, and location, even without traditional video cameras.

These AI enabled surveillance tools differ from traditional video and audio monitoring in several ways. For one, AI tools combine real time surveillance data with massive stores of data extracted and scraped from a worker's work activity, social media, website browsing, credit scores, and any other data from the workplace or web. Heart rate, perspiration, facial expressions, and eye movements are all tracked and used as data points to target "unproductive" workers and to "minimize risk" in the workplace.

AI tools also notoriously rely on black-box algorithms to analyze workers. Data from emotion recognition, neural sensors, and facial and gait sensors are not just observations, but an 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, such as Verint, may very well fail to understand cultural nuances of expression and may be trained on biased data 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. The biases of these tools can lead to detrimental decisions affecting the livelihood of workers as seen in the recent lawsuit between UberEats and a driver who was deactivated due to faulty facial recognition technology failing to identify the driver for verification purposes.

Increasingly, employers are using sophisticated tools to monitor worker sentiment to prevent workers from unionizing or advocating for their rights. Perceptyx, a company that collects and analyzes employee surveys, digital focus groups, and other information, claims they could create a "union vulnerability index" so employers can see which group of workers is at highest risk of unionizing. The power, scope, and scale of current surveillance tools surpass anything employers have had in the past. Yet, our laws have not caught up with the advances of technology and give workers scant protection from the most invasive, discriminatory, or harmful surveillance tools on the market.

Also writing in support, Oakland Privacy argues:

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 sun-setted and was not renewed and qualified California employers became subject to the CCPA and the succeeding ballot initiative, the California Privacy Rights Act, CPRA.

As one might expect from a law titled the California Consumer Privacy Act, the CCPA and its later amendment (CPRA) 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.

An element that Assembly Bill 1883 adds to the 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 CCPA/CPRA. For that reason alone, workplace privacy protections that are supplementary to CCPA/CPRA are neither duplicative nor excessive.

The protections provided by Assembly Bill 1883 go beyond the right to know, right to correct, and right to opt-out structure provided by CPRA. The bill bans the use of four kinds of biometric surveillance in California workplaces: facial recognition, gait analysis, neural data processing and emotion identification. We agree with the author that these technologies are maximally invasive and impose on an employee's bodily autonomy. Workers are not owned by their employers, they are in an agreement with them to render services.

We should be able to agree that not every technology that can be invented should be unleashed on California's workers, and in many cases, California's most poorly paid and vulnerable workers. Whether we walk more quickly or slowly, what we are thinking silently to ourselves, and how we feel on a given day are literally what privacy is made of.

Business interests like the Chamber of Commerce will likely provide some convincing sounding edge case applications for biometric technologies in the workplace to try to convince you not to ban them. But all of these can be just as effectively performed by other methods, equipment or technologies. These arguments are to evade the central point. California employers want access to the thoughts, feelings and anatomy of their workers in order to exercise more complete control over them during the work day. But if the only way employers can hire, manage and supervise their employees is to have access to their personal thoughts and feelings, then they need to hire robots, not human beings. And if you remember your high school reading of Mary Shelley, the robots won't like it either.

The ability of employees to tolerate their workplaces and to work with positive morale and energy are tied to safe and empowering workplace conditions. We don't think it's debatable that employee energy is crucial to the vitality of California's economy going forward. By making a California a place where workers don't have to fear that their private thoughts and feelings are going to become the property of their employer, the Legislature can ensure that California will remain a desirable place to live and work.

ARGUMENTS IN OPPOSITION: In opposition to the bill, a coalition of business organizations, including TechNet and the California Grocers Association, argue:

AB 1883 Contains Certain Provisions that are Unworkable

While we appreciate changes that were made to AB 1883 as compared to its predecessor, AB 1221 (2025) (Bryan), the bill still contains certain provisions that are not workable. For example, Section 1581(a)(1)(B) provides that employers cannot use a workplace surveillance tool that identifies workers engaging in protected activities. A security camera is going to capture whatever footage it captures, which could qualify as "identifying" someone under this language. For example, a camera cannot turn itself off during a strike or if an employee chooses to have a meeting with another employee in an open area. If employees are choosing

to use their company emails or messaging functions to discuss protected activity, those communications are under cybersecurity programs or likely being stored on a server for purposes of record retention. While we appreciate the intent of not wanting to deter employees from exercising their rights, this is just not practical as written.

Proposed Section 1581(a)(2) provides that a workplace surveillance tool cannot be used to infer a person's protected status under FEHA. However, given the breadth of "workplace surveillance tools", this could include information that employees voluntarily share. For example, employees often voluntarily participate in workforce development surveys to evaluate and enhance business culture. The information that employees voluntarily share often includes demographic information like veteran status, religious beliefs, or health status. The responses to the survey are likely collected through databases or even simple email storage systems that may constitute workplace surveillance tools as defined. Further, many larger employers have affinity groups such as for people of certain religions or mentorship programs for neurodivergent employees, so those meetings will occur over computer platforms or potentially in areas where there are security cameras or require badging in and out. While we appreciate the intent of this provision, we want to ensure that there are no unintended consequences that impact legitimate uses of technology. If an employee believes they've been subject to unlawful discrimination, they have the right to bring a claim under FEHA.

Proposed Section 1581(a) prohibits any use of facial recognition, gait recognition, or emotion recognition by a workplace surveillance tool. Again, while we appreciate the intent, there are certain legitimate uses that should be allowed, including:

- Tools used in emergency situations that can determine who is on premises
- Tools that use analytics to detect shouting or calls for help
- In-vehicle tools that may detect unsafe driving behavior
- Logistics tools that assess employees' gait for purposes of evaluating the most efficient way to organize a warehouse or employee job duties
- Tools designed to identify theft, missing persons, or suspicious personnel on premises that would also capture employees or contractors on the premises
- Tools that flag inappropriate behavior during customer interactions

We understand there are scenarios where there should be guardrails about how the tools should be used or when they can be used for an adverse employment action, but a blanket prohibition would impact legitimate uses of certain technologies.

<u>Independent Contractors Should Not Be Included in The Definition of "Worker"</u>

The bill's definition of "worker" includes independent contractors, which should be removed from the bill. Contractors are often limited-term workers who are performing a specific job for a company. By definition they are very different from an employee. Their contract will dictate the terms of that job and any job-specific requirements. This trend of treating them the same as employees in every new bill is at odds with prior legislation and court decisions. Further, their inclusion in such a broad bill compounds the bill's administrative burden on businesses and state and local governments.

REGISTERED SUPPORT / OPPOSITION:

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
American Federation of State, County and Municipal Employees (AFSCME), Afl-cio 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 Sheet Metal, Air, Rail and Transportation Workers - Transportation Division (SMART-TD)
California State Legislative Board of the Smart - Transportation Division
California State University Employees Union, Seiu Local 2579
California Teachers Association
Central Coast Labor Council
Central Labor Council, Fresno-madera-tulare-kings Counties, Afl-cio
Engineers and Scientists of California, Ifpte Local 20, Afl-cio
Inland Empire Labor Council, Afl-cio
North Bay Labor Council
North Valley Labor Federation
Oakland Privacy
Orange County Labor Federation, Afl-cio
Privacy Rights Clearinghouse
San Mateo County Central Labor Council
Service Employees International Union, California State Council
Teamsters California
Tech Equity
Techequity Collaborative
Unite Here, Afl-cio
Utility Workers Union of America, Afl-cio
What We Will

Opposition

American Petroleum and Convenience Store Association Apca
Associated General Contractors of California
Associated General Contractors San Diego
Association of California Healthcare Districts (ACHD)
Building Owners and Managers Association of California
California Apartment Assocation
California Assisted Living Association
California Association of Joint Powers Authorities (CAJPA)

California Association of Sheet Metal & Air Conditioning Contractors National Association
California Attractions and Parks Association
California Automatic Vendors Council
California Business Properties Association
California Chamber of Commerce
California Craft Brewers Association
California Distributors Association
California Farm Bureau
California Grocers Association
California Hospital Association
California Landscape Contractor's Association
California Landscape Contractors Association
California League of Food Producers
California Legislative Conference of Plumbing, Heating & Piping Industry
California Manufacturers and Technology Association
California Manufactures & Technology Association
California Moving and Storage Association
California Restaurant Association
California Retailers Association
California Special Districts Association
California State Association of Counties (CSAC)
California Trucking Association
California's Credit Unions
Civil Justice Association of California (CJAC)
Construction Employers Association
County Health Executives Association of California (CHEAC)
County of Fresno
Finishing Contractors Association of Southern California
League of California Cities
Los Angeles Area Chamber of Commerce
National Association of Independent Property Owners
National Automatic Merchandising Association
National Electrical Contractors Association (NECA)
Northern California Allied Trades
Public Risk Innovation, Solutions, and Management (PRISM)
Resource Recovery Coalition of California
Rural County Representatives of California (RCRC)
Security Industry Association
Self Storage Association
Shrm California
Technet
United Contractors (UCON)
Urban Counties of California (UCC)
Valley Industry and Commerce Association (VICA)
Wall and Ceiling Alliance
Western Growers
Western Line Constructors Chapter, Inc., Neca, INC.
Western Painting and Coating Contractors Association

Western Wall and Ceiling Contractors Association (WWCCA)
Wine Institute

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