Date of Hearing: April 22, 2025
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 1221 (Bryan) – As Amended April 21, 2025

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 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 and limit workplace surveillance technology in three significant ways: first, by requiring that employers disclose to their employees the types and location of surveillance technology, the data being collected and the reason for the collection; second, by restricting how employers and vendors can use the collected data and the requirement that employees be allowed to access the data that is collected; and third, by prohibiting the use of the most intrusive types of surveillance technology.

The proposed Committee amendments, detailed in Comment #

The bill is supported by a large coalition of labor organizations and is opposed by a similarly large coalition of business groups. The Labor and Employment Committee passed the bill with a 5-0-2 vote.

THIS BILL:

1) Defines the following:

    a) "Agency" means the Labor and Workforce Development Agency or any of its designees.

b) "Authorized representative" means a person or organization appointed by the worker to serve as an agent of the worker, but does not mean a worker's employer.

c) "Employer" means a person or governmental entity that directly or indirectly, or through an agent or any other person, employs or exercises control over the wages, benefits, other compensation, hours, working conditions, access to work or job opportunities, or other terms or conditions of employment, of any worker, including all branches of state government, 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. "Employer" includes an employer's labor contractor.

d) "Employment-related decision" means a decision by an employer that impacts wages, wage setting, benefits, compensation, hours, work schedule, performance evaluation, hiring, discipline, promotion, termination, job tasks, skill requirements, responsibilities, assignment of work, access to work and training opportunities, productivity requirements, workplace health and safety, and any other terms or conditions of employment.

e) "Public prosecutor" means the Attorney General, a district attorney, a city attorney, a county counsel, or any other city or county prosecutor.

f) "Neural data" means information that is generated by measuring the activity of an individual's central or peripheral nervous system, and that is not inferred from nonneural information.

g) "Vendor" means a third party, subcontractor, or entity engaged by an employer or an employer's labor contractor to provide software, technology, or a related service that is used to collect, store, analyze, or interpret worker data or worker information.

h) "Worker" means a natural person, an employee of, or an independent contractor providing service to, or through, a business or a state or local governmental entity in a workplace.

i) "Worker data" means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a covered worker, regardless of how the information is collected, inferred, or obtained.

j) "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 that are also 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 that utilizes a photo-optical system or other means.

2) Requires, at least 30 days before introducing a workplace surveillance tool, an employer to provide to any worker that will be directly or indirectly affected a plain language, written notice, pursuant to 6) below, in the language in which routine communications and other information are provided by the employer to workers.

3) Authorizes the employer to provide the notice via a simple and easy-to-use method, including an email, a hyperlink, or another written format, but requires the notice to be separate from any other communication and prohibits the notice from containing any information on another subject.

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

5) Requires an employer to maintain an updated list of all workplace surveillance tools in use and provide the notice described above to any worker hired after the date on which the employer complied with 1) above.

6) Requires an employer to provide additional notice to workers within 30 days of any significant updates or changes made to the workplace surveillance tool or in how the employer is using the workplace surveillance tool.

7) Requires the notices described above to contain all of the following information:

    a) A description of the worker data to be collected, the intended purpose of the workplace surveillance tool, and how this form of worker surveillance is necessary to meet that purpose.

    b) A description of the specific activities, locations, communications, and job roles that will be electronically monitored and the technologies that will be used.

    c) The frequency of surveillance and worker data collection.

    d) A description of where, how, and for how long worker data will be stored.

    e) Information about who is authorized to access the worker data gathered and under what conditions, including the names of vendors.

    f) Whether the workplace surveillance tool will be used to make employment-related decisions and which decisions those will be.

    g) The right of a worker to access and correct worker data collected by the workplace surveillance tool.

    h) A written policy informing the worker about how they can access their data.

8) Prohibits an employer from transferring, selling, disclosing, or licensing worker data, including deidentified or aggregated data, to a vendor including another employer, unless the vendor is under contract to analyze or interpret the worker data, and the contract includes all of the following terms:

    a) The vendor is prohibited from transferring, selling, disclosing, licensing, or otherwise distributing the worker data.

    b) The vendor implements reasonable security procedures to protect the worker data from unauthorized or illegal access, destruction, use, modification, or disclosure.

c) The vendor and employer agree to be jointly and severally liable for breaches experienced by the vendor to the extent the breach involves worker data provided by the employer.

d) The vendor is prohibited from transferring, selling, disclosing, licensing, or otherwise distributing any product that results from the vendor's analysis or interpretation of the worker data, except to provide the agreed-upon product to the employer.

9) Prohibits an employer, or a vendor acting on behalf of an employer, from sharing worker data with another person or governmental agency unless it is necessary to obtain the information for an investigation by a governmental agency in order to conduct an investigation related to failure to comply with a specific state law that the agency is responsible for enforcing.

10) Prohibits an employer or vendor from sharing worker data with law enforcement except pursuant to a valid court order.

11) Requires an employer or vendor to keep worker data secure by preventing unauthorized access and implementing a security system with up-to-date cybersecurity safeguards in place.

12) Requires worker data collected by an employer or a vendor to be accessible only to authorized personnel.

13) Requires an employer, if a data breach occurs, to give notice to workers of the specific categories of data that were impacted in the security breach as soon as possible.

14) Requires a vendor to return to the worker and employer all worker data collected through a workplace surveillance tool in a user-friendly format and delete any remaining copies of the worker data at the end of the vendor's contract with the employer.

15) Requires an employer using data collected from a workplace surveillance tool to make employment-related decisions to retain that worker data for at least five years from the date the worker data was collected.

16) Requires an employer to allow a worker to correct inaccurate worker data and obtain worker data collected by a workplace surveillance tool within five business days of that request.

17) Limits an employer to only collecting, using, and retaining worker data that is reasonably necessary and proportionate to achieve the purposes described in the required disclosure.

18) Prohibits an employer from using a workplace surveillance tool that does any of the following:

a) Prevents compliance with or violates any federal, state, or local law.

b) Identifies, obtains, or infers information about workers engaging in activity protected by state or federal law.

c) Obtains or infers a worker's immigration status, veteran status, ancestral history, religious or political beliefs, health or reproductive status, history, or plan, emotional or psychological state, neural data, sexual or gender orientation, disability, criminal record,

credit history, or status protected under existing regulations on discrimination in employment, as provided.

d) Incorporates facial recognition, gait recognition, neural data collection, or emotion recognition technology.

19) Prohibits an employer from relying primarily on worker data from a workplace surveillance tool to discipline or discharge a worker.

20) Requires that if an employer's use of data collected by a surveillance tool contributes to a disciplinary or discharge decision by the employer, the employer must do all of the following:

a) Use a human reviewer to conduct the employer's investigation and compile corroborating or supporting information for the decision, including evaluations, personnel files, employee work product, or peer reviews.

b) Notify the worker that the decision was made using data collected by a surveillance tool, provide the worker or their authorized representative with an opportunity to access the data and corroborating information, and allow the worker to correct any erroneous worker data. The request to access the data must be made within five days of the notice being received.

c) Make any valid correction of worker data within 24 hours of the worker's request and change the disciplinary or discharge decision if the correction validates a change.

21) Prohibits an employer from discharging, threatening to discharge, demote, suspend, or in any manner discriminating or retaliating against any worker for using, or attempting to use, their rights under the provisions of the bill and establishes a complaint process and an enforcement process either through the Labor Commissioner, the employee, or a public attorney.

22) Provides that the bill's provisions do not preempt any city, county, or city and county ordinance that provides equal or greater protection to workers who are covered by the provisions of this bill.

23) Provides that the provisions of this bill are severable and that, if any provision of this bill or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application.

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) Defines a "consumer" to mean a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier. (Civ. Code § 1798.140.)

8) 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:

> 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 or regulate how their data is used. AB 1221 addresses this issue by prohibiting the use of unreliable and potentially discriminatory surveillance technologies—facial, gait, and emotional recognition—and enacting strict data protections.
>
> This bill enacts data protections that prohibit employers from sharing worker data for purposes beyond interpreting it and ensures both employers and third-party entities are held accountable for any misuse or breaches. Additionally, it requires employers to notify workers in advance when introducing surveillance tools in the workplace. AB 1221 establishes transparency and safeguards for worker privacy in the era of digital surveillance.

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

---

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

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 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

---

[2] *Ibid.*
[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

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 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]

4) **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

---

[6] Humanyze: The Future of Workforce & Market Intelligence https://humanyze.com/
[7] https://www.teramind.co/solutions/compliance-management/
[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.*

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 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.

5) **What this bill would do.** This bill makes several significant changes to the use of surveillance technology in the workplace:

1. Requires an employer, at least 30 days before introducing a workplace surveillance tool, to provide a worker who will be affected a written notice that, among other information, includes the following:

    - A description of the worker data to be collected.

    - The intended purpose of the workplace surveillance tool, and how this form of worker surveillance is necessary to meet that purpose.

---

[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/

- A description of the specific activities, locations, communications, and job roles that will be electronically monitored and the technologies that will be used.

- The frequency of surveillance and worker data collection.

2. Creates certain requirements and restrictions related to the use of worker data. Among them:

   - Prohibits an employer from transferring, selling, disclosing, or licensing worker data, including deidentified or aggregated data, except under certain narrow conditions.

   - Requires an employer to take certain cybersecurity measures to ensure the safety of worker data.

   - Requires worker data collected by an employer or a vendor to be accessible only to authorized personnel.

   - Requires an employer to allow a worker to correct inaccurate worker data.

   - Limits an employer to only collecting, using, and retaining worker data that is reasonably necessary and proportionate to achieve the purposes described in the required disclosure.

   - Prohibits an employer from relying primarily on worker data from a surveillance tool to discipline or discharge a worker

3. Prohibits employers from using certain workplace surveillance tools that are capable of or claim to be capable of the following:

   - Obtaining or inferring a worker's immigration status, veteran status, ancestral history, religious or political beliefs, health or reproductive status, history, or plan, emotional or psychological state, neural data, sexual or gender orientation, disability, criminal record, credit history, or status protected under existing regulations on discrimination in employment.

   - Obtaining or inferring information about workers using facial recognition, gait recognition, neural data collection, or emotion recognition technology.

4. Provides for enforcement by the Labor Commissioner, employees and representatives, and public prosecutors, and subjects employers in violation to a civil penalty.

6) **Limitations in California's current privacy protection laws.** In 1972, at the Legislature's urging, the people of California used the initiative process to add "privacy" to the list of "inalienable rights" in the state constitution.[14] Proponents noted the initiative was specifically designed to preserve Californians' private lives and fundamental rights in the face of technological advances. They argued: "The right of privacy is the right to be left alone. . . . It prevents government and business interests from collecting and stockpiling unnecessary

[14] California Proposition 11 (1972), "Constitutional Right to Privacy Amendment."

information about us and from misusing information gathered for one purpose in order to serve other purposes. . . ."[15]

In 2018, the Legislature enacted the California Consumer Privacy Act (CCPA; AB 375 (Chau, Chap. 55, Stats. 2018)), which gave consumers certain rights regarding their personal information,[16] such as the right to: (1) know what personal categories of information about them are collected and sold; (2) request the deletion of personal information; and (3) opt-out of the sale of their personal information, or opt in, in the case of minors under 16 years of age.

Subsequently, in 2020, California voters passed Proposition 24, the California Privacy Rights Act (CPRA), which established additional privacy rights for Californians. Chief among these rights was the right of a consumer to limit a business's use of sensitive personal information.[17] One of the key components of the initiative was establishing that the CCPA was a floor and not a ceiling for privacy protection. Essentially, to protect Californians from any future legislative efforts to weaken statutory protections in the CPRA, Proposition 24 provided that the CPRA's contents may be amended by a majority vote of the Legislature only if the amendments are consistent with and further the purpose and intent of the CPRA, which is to further protect consumers' rights, including the constitutional right of privacy.[18]

At the time, California had the most comprehensive laws in the country when it came to protecting consumers' rights to privacy. Since the passage of the CCPA, however, 19 additional states have passed comprehensive privacy laws. Of those states, 17 have laws that are more privacy protective. 16 states require consumers to "opt in" to the sharing and sale of sensitive information and one state, Maryland, prohibits the sharing of sensitive information entirely.[19] In the states that have come after California, privacy is the default.

The CCPA, on the other hand, relies on consumers actively exercising their rights to "opt out" of the sharing and sale of their personal information and the sharing, sale and use of their sensitive personal information. The challenge is that in order to exercise those rights, consumers must first find the businesses that have collected their personal information and then find a way to contact the company to exercise those rights. It is likely that the average consumer often does not even realize that their personal information is being harvested, used to micro target them for advertising, and sold as a commodity to other companies.

As it pertains to this bill, it is unlikely that the Legislature and the voters contemplated the proliferation of location data brokers and the constant surveillance of everyone in the United States when considering the CCPA and the CPRA. The location intelligence market in the United States was estimated to be around $3 billion in 2020, the year voters approved the

---

[15] *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP REPOSITORY (1972), pp. 26–27, https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props.
[16] Civ. Code § 1798.140(v). See **EXISTING LAW** #14(a) for definition.
[17] Civ. Code § 1798.140(ae). See **EXISTING LAW** #14(b) for definition.
[18] Ballot Pamphlet. Primary Elec. (Nov. 3, 2020) text of Prop. 24, p. 74
[19] A comparison chart of state privacy laws can be accessed at https://45555314.fs1.hubspotusercontent-na1.net/hubfs/45555314/Slides%20and%20one-pagers/US%20state%20law%20comparison%20chart_2024_July_1.pdf.

CPRA.[20] By 2025, it has nearly doubled and is expected to grow to over $12 billion by 2030.[21] Globally, the market revenue was over $21 billion and is estimated to grow to approximately $54 billion by 2030. Fortunately, as noted above, the proponents of the CPRA and the voters understood that the Legislature may need to move beyond the CCPA in order to continue to protect Californians' right to privacy.

7) **Concerns raised by the opposition.** A coalition of business organization has raised a number of concerns about the requirements placed on employers by the bill. Among those concerns are the following that are under this Committee's purview:

- *The breadth of notices required.* Disclosing to workers the location of workplace surveillance tools may defeat the purpose of these tools if they are being used for anti-theft or other security measures. Requiring employers to disclose who is authorized to access the data also raises concerns in the event that the surveillance data is being accessed for an investigation, a "confidential project," or litigation.

The author may wish to work with the opposition to determine whether or not there may be narrow circumstances when it is necessary to withhold disclosure of the location of certain surveillance tools or the purpose of those tools.

- *Unworkable restrictions on transferring data.* Given that the current definition of worker data is very broad and includes anything that is capable of being associated with a worker, restricting the sharing of data with anyone in government unless the employer is required to do so for purposes of an investigation or a court order could prohibit something as simple as sharing information about an employee in a job recommendation. Prohibiting the disclosure of deidentified and aggregated data places data that has been stripped of any identifiable information on the same footing as worker data that can identify and individual.

The current definition of "worker data" and "workplace surveillance tool" are broad and include virtually any data that can be associated with a worker through any device that collects that data. Going forward, the author may wish to consider clarifying that the bill is not intended to capture information that is freely provided by the worker, nor is it intended to stop an employer from sharing information, such as serving as a reference for another job, at the request of the worker. One of the primary pillars of the State's privacy laws is that individuals have a right to control how and with whom their personal information is shared. Clarifying that an employer may disclose information when requested by the worker or if the worker provides affirmative consent, may help mitigate any unintended restrictions.

- *Unworkable limitations on the use of workplace surveillance tools.* Prohibiting the use of any tool that is capable of identifying, obtaining, or inferring that workers are engaged in protected activities or protected information about workers is not practical. In addition, a ban on the use of facial recognition technology is also not practical when it is common

---

[20] *Global Location Intelligence Industry (2020 to 2027) - Key Market Trends and Drivers,* BusinessWire (May 19, 2021) https://www.businesswire.com/news/home/20210319005168/en/Global-Location-Intelligence-Industry-2020-to-2027---Key-Market-Trends-and-Drivers---ResearchAndMarkets.com
[21] *U.S. Location Intelligence Market Size & Outlook,* Horizon Grandview Research https://www.grandviewresearch.com/horizon/outlook/location-intelligence-market/united-states

for employees to use their phones to clock in and out and that technology may be enabled on those phones.

8) **Support from privacy advocates.** Writing in support of the bill, Oakland Privacy states:

> 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 Assembly Bill 1221 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 Assembly Bill 1221 go beyond the right to know, right to correct, and right to opt-out structure provided by CPRA. They include prompt and informed notice requirements that are delivered within 30 days that include meaningful information about the technological tools being used, the purpose of the surveillance activity, who runs and operates it, what data will be collected, who will have access to it and how it will be used and a right of correction. These parameters include what a best practice "privacy policy" on a consumer website is supposed to provide and maintain 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 mandate 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.

9) **Amendments.** The author has agreed to the following clarifying amendments:

> **1553.** (a) An employer shall not use a workplace surveillance tool that does any of the following:
>
> (1) Prevents compliance with or violates any federal, state, or local law.
>
> (2) Identifies, obtains, or infers information about workers engaging in activity protected by state or federal law.
>
> (3) ~~*Obtains or infers*~~ ***That is used to infer*** a worker's immigration status, veteran status, ancestral history, religious or political beliefs, health or reproductive status, history, or plan, emotional or psychological state, neural data, sexual or gender orientation, disability, criminal record, credit history, or status protected under Section 12940 of the Government Code.

(4) Incorporates facial recognition, ***unless it is used strictly to open a locked device or grant access to locked, secure areas***, gait recognition, *neural data collection*, or emotion recognition technology.

In addition the Judiciary Committee has requested on amendment that was erroneously left out of the previous amendments:

1555. (b) Alternatively to subdivision (a), an employee who has suffered a violation of this part, or the employee's exclusive representative, may bring a civil action in a court of competent jurisdiction for damages caused by that ***violation*** ~~**adverse action**~~, including punitive damages.

ARGUMENTS IN SUPPORT: The California Labor Federation, sponsors of the bill, and a broad coalition of labor advocacy organizations write in support:

Modern surveillance tools can also be invasive given the massive amounts of data they can compile on workers. Rather than just capturing images on camera, these new tools can scrape the internet, measure biometrics, analyze emotions, and mine other data sources to produce output for employers. That gives employers the ability to know the most personal information about workers and to even infer or predict information. For example, Perceptyx – a company that collects and analyzes employee surveys, digital focus groups, and other information – said it could create a "union vulnerability index" so employers can see which group of workers is at highest risk of unionizing.

AB 1221 creates a surveillance and data protection structure for transparency, worker protection, and prohibitions on abusive technologies. The bill allows the use of workplace surveillance tools of all kinds, but enacts strong protections for workers on its use, as well as prohibiting the most invasive and harmful tools.

AB 1221 prohibits the use of the most unreliable and potentially discriminatory types of surveillance—facial, gait, and emotion recognition technology. It also prohibits the use of surveillance tools to obtain or infer protected and personal information about workers, including immigration and health status and the likelihood of unionizing or speaking up against workplace violations.

When employers are introducing or using surveillance tools, AB 1221 requires advance notice to workers, so workers know how, where, and why they are being monitored. The bill enacts data protections that prohibit employers from sharing worker data for purposes beyond data and makes both the employer and third-party entity liable if worker data is breached or misused. Lastly, the bill requires employers to produce corroborating evidence to validate surveillance output before disciplining or firing a worker. This ensures human oversight over surveillance tools that may produce faulty outputs or interpretations. AB 1221 creates strong worker privacy protections and human oversight in the age of pervasive digital surveillance.

ARGUMENTS IN OPPOSITION: In addition to the concerns discussed previously, the opposition coalition also notes:

AB 1221 prohibits an employer from making any termination or disciplinary decisions based "primarily" on data received from an electronic surveillance tool. As we read this language, if a security camera caught an employee engaging in unsafe or unlawful conduct, even if a

manager reviewed the tape, the evidence for termination would "primarily" be the security footage. Therefore, practically speaking, this would require human corroboration in scenarios where it is unnecessary.

In addition they argue:

Proposed Section 1552(h) allows a worker to access and correct worker data collected by its workplace surveillance tool. Given the breadth of the definitions in the bill, it is unclear whether the employer would be required to, upon request, turn over a copy of every single email, text message, calendar invite, chat, Slack message, browser search history, or security camera footage, etc. This would result in thousands of documents for many workers and would necessarily include information about other employees and/or confidential, proprietary, or privileged information. It is also unclear what it means to "correct" information. For example, the CCPA contains clear guidelines regarding how and under what circumstances a consumer can request access to data or correct inaccurate data. Importantly, the CCPA and accompanying regulations include exceptions as well as make clear that data should only be provided "upon receipt of a verifiable consumer request from the consumer" to prevent bad actors from obtaining private data. This is another reason why an "authorized representative" should not be in the definition of "worker" and given this right to access other people's information, which is discussed in more detail below.

REGISTERED SUPPORT / OPPOSITION:

Support

California Labor Federation (Sponsor)
Afscme California
California Alliance for Retired Americans (CARA)
California Coalition for Worker Power
California Employment Lawyers Association
California Federation of Labor Unions, Afl-cio
California Federation of Teachers Afl-cio
California Immigrant Policy Center
California Nurses Association
California Professional Firefighters
California School Employees Association
California State Legislative Board of the Smart - Transportation Division
California Teamsters Public Affairs Council
Center for Inclusive Change
Cft- a Union of Educators & Classified Professionals, Aft, Afl-cio
Coalition for Humane Immigrant Rights (CHIRLA)
Communications Workers of America, District 9
Community Agency for Resources, Advocacy and Services
Consumer Attorneys of California
Consumer Federation of California
International Lawyers Assisting Workers (ILAW) Network
Laane
National Employment Law Project
National Union of Healthcare Workers (NUHW)

Northern California District Council of the International Longshore and Warehouse Union (ILWU)
Oakland Privacy
Pillars of the Community
Powerswitch Action
Rise Economy
San Diego Black Workers Center
Secure Justice
Seiu California State Council
Surveillance Resistance Lab
Techequity Action
The Workers Lab
Unite Here, Local 11
United Food and Commercial Workers, Western States Council
Workers' Algorithm Observatory
Working Partnerships USA
Worksafe

Oppose

American Petroleum and Convenience Store Association
Associated Builders and Contractors of California
Associated General Contractors
Associated General Contractors San Diego
California Alliance of Family Owned Businesses
California Apartment Association
California Apartment Association
California Association of Health Facilities
California Association of Sheet Metal & Air Conditioning Contractors National Association
California Association of Winegrape Growers
California Bankers Association
California Cardroom Alliance
California Chamber of Commerce
California Credit Union League
California Farm Bureau
California Gaming Association
California Grocers Association
California Hospital Association
California Hotel & Lodging Association
California League of Food Producers
California Manufacturers and Technology Association
California Moving and Storage Association
California Restaurant Association
California Retailers Association
California Trucking Association
Civil Justice Association of California (CJAC)
Construction Employers' Association
Dairy Institute of California
Housing Contractors of California

Insights Association
Los Angeles Area Chamber of Commerce
National Electric Contractors Association
National Electrical Contractors Association (NECA)
San Jose Chamber of Commerce
Security Industry Association
Society for Human Resource Management
Technet
United Contractors
Western Electrical Contractors Association
Western Growers Association
Wine Institute

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