Date of Hearing: April 22, 2025
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 1331 (Elhawary) – As Amended April 10, 2025

PROPOSED AMENDMENTS

SUBJECT: Workplace surveillance

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 has 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, 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 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 prohibit employers from using a workplace surveillance tool to monitor workers in off-duty areas, including their personal residence and vehicle, and during off-duty hours. The bill provides a civil penalty for each employee per violation. Committee amendments, outlined in Comment #8, are largely clarifying in nature.

The bill is sponsored by a large coalition of labor organizations and is opposed by a similarly large coalition of business groups. This bill has been referred to three committees. The Labor and Employment Committee has primary jurisdiction. That Committee passed the bill on a 5-0-2 vote. This Committee is the second committee to analyze and hear this bill. If the bill passes this Committee, it will next be heard in the Judiciary Committee.

THIS BILL:

1) Defines "employer" to mean a person who directly or indirectly, or through an agent or any other person, employs or exercises control over the wages, benefits, other compensation, hours, working conditions, access to work or job opportunities, or other terms or conditions of employment, of any worker. "Employer" includes:

    a) An employer's labor contractor.

b) Private and public entities, including state and local government.

2) Defines “worker” to mean an employee of, or an independent contractor providing service to, or through, a business or a state or local governmental entity in a workplace.

3) Defines “worker data” to mean 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.

4) Defines “workplace surveillance tool” to mean a 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 capable of passively surveilling workers, by means other than direct observation by a person, including, but not limited to, video or audio surveillance, electronic work pace tracking, geolocation, electromagnetic tracking, photoelectronic tracking, or utilization of a photo-optical system or other means.

5) Defines “public prosecutor” to mean the Attorney General, a district attorney, a city attorney, a county counsel, or any other city or county prosecutor.

6) Prohibits an employer from using workplace surveillance tools to monitor or surveil workers in off-duty areas, including:

a) Bathrooms

b) Locker rooms

c) Changing areas

d) Breakrooms

e) Designated smoking areas

f) Lactation spaces

g) Employee cafeterias

h) Lounges

i) Other areas where workers congregate while off-duty but on work premises.

7) Prohibits employers from collecting data on the frequency of use of the off-duty areas.

8) Authorizes workers to disable or leave behind any workplace surveillance tools on their person or in their possession when entering off-duty areas or during off-duty hours for any tools in their residence or vehicle, including any owned, leased, or used by a worker.

9) Prohibits an employer from requiring that a worker physically implant a surveillance device in their body.

10) Notwithstanding 7) through 9), an employer may use routine workplace surveillance in a work area not listed in 6), even if an employee is present, as long as the employee knows the tool is in use.

11) Prohibits an employer from denying an employee the rights under these provisions or from discharging, threatening to discharge, demoting, suspending, or in any manner discriminating against an employee for using, or attempting to use, the employee's rights under these provisions, filing a complaint with the Department of Industrial Relations (DIR) or alleging a violation of these provisions, cooperating in an investigation or prosecution of an alleged violation of these provisions, or opposing any policy or practice or act that is prohibited by these provisions.

12) States that, in addition to any other remedy, an employer who violates these provisions shall be subject to a civil penalty of $500 per employee for each violation.

13) Requires the Labor Commissioner (LC) to enforce the above provisions, including investigating an alleged violation, and ordering appropriate temporary relief to mitigate a violation or maintain the status quo pending the completion of a full investigation or hearing through the LC's existing procedures, including issuing a citation and filing a civil action against an employer who denies employee rights described in 11) above. If a citation is issued, the LC's existing procedures for issuing, contesting, and enforcing judgments for citations and civil penalties shall be utilized.

14) Provides that, as an alternative to the penalty described in 12) above, any employee who has suffered a violation may bring a civil action in a court of competent jurisdiction for damages caused by that adverse action, including punitive damages, and for reasonable attorney's fees as part of the costs of any such action for damages.

15) Authorizes, in any civil action brought pursuant to 14) above, an employee or the employee's exclusive representative to petition the superior court in any county wherein the violation in question is alleged to have occurred, or wherein the person resides or transacts business, for appropriate temporary or preliminary injunctive relief.

16) Authorizes any public prosecutor to institute an action for a violation of these provisions, including an action seeking injunctive relief.

17) Provides that the above provisions do not preempt any local law that provides equal or greater protection to workers.

18) States that the above provisions are severable, as described.

19) Provides that these provisions do not limit the authority of the Attorney General, a district attorney, or a city attorney, either upon their own complaint or the complaint of any person acting for themselves or the general public, to prosecute actions, either civil or criminal, for violations of these provisions, or to enforce the provisions independently and without specific direction of the LC or the Division of Labor Standards Enforcement.

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: "AB 1331 is an important step in securing a worker's right to privacy while new invasive surveillance technologies are being used by employers." In background information provided to the Committee, the author further notes:

> As technology's capabilities have increased, employer surveillance of workers has increased. Recent reports from ExpressVPN found that close to 80% of employers use monitoring software to track employee performance. With employer surveillance on the rise, workers have limited access to spaces in their workplace, and homes that are not under constant surveillance. Employers use workplace surveillance to track, monitor, manage, and prevent workers from advocating for their rights. The new surveillance state at the workplace has proven to increase psychological distress, stress, and lower job satisfaction among workers.
>
> Surveillance is used to monitor and increase productivity, but increasingly employers are using sophisticated tools to monitor worker sentiment to prevent workers from unionizing or advocating for their rights. Often the only time workers can gather to talk about wages and working conditions are in break rooms, bathrooms, or other off-duty times at the workplace. These are opportunities for workers to identify potential labor law violations or to exercise their right to organize.

2) **The evolution of workplace surveillance.** Employers surveilling their workers, both during and after work hours, is far from a new phenomenon. For almost 200 years, if not longer, employers have been watching their employees' activities. The roots of employers actively

surveilling their workers in the United States can be traced back to the counting of the North-Western Police Agency, later known as the Pinkerton National Detective Agency, in 1855. The agency was borne out of employers' desire for more control over their employees, both inside and outside of work. Pinkerton detectives fulfilled that need. Among the roles played by the detectives were monitoring workers who were deemed to be a threat to an employer's interests; infiltrating and busting unions; and enforcing company rules.[1]

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

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

Over the last 40 years, advances in technology have allowed employers to surveil their workers in ways that could only have been imagined in science fiction novels. Punch cards have given way to biometric scans, key cards and workplace badges are giving way to Radio Frequency Identity (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, everyone is most 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. Some employers required their employees to keep their cameras and microphones on during the workday.[4] For those who could not work remotely during the pandemic, especially in blue-color trades, workers were subject to mandatory health screenings, temperature checks, and, in some cases, social distancing sensors that allowed employers to track when, for how long, and which employees were together and not practicing the required social distancing.

3) **Where workers find themselves now.** 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

---

[1] Ifeoma Ajunwa, et al. "Limitless Worker Surveillance" *105 California Law Review 735* (2017) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746211
[2] *Ibid.*
[3] *Ibid.*
[4] Wilneida Negrón and Aiha Nguyen, "The Long Shadow of Workplace Surveillance" *Stanford Social Innovation Review* (Sep. 6, 2023) https://ssir.org/articles/entry/the_long_shadow_of_workplace_surveillance#

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."[5]

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

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."[6] 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.[7] 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.[8] 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.[9]

Oxfam, an international organization focused on fighting global poverty, conducted an investigation into the workplace surveillance practices at both Amazon and Walmart warehouses

---

[5] *Ibid.*
[6] 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/
[7] *Ibid.*
[8] 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/
[9] *Ibid.*

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."[10] 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.** In order to establish some workplace surveillance guidelines, this bill prohibits the use of surveillance tools in off duty areas, including:

- Bathrooms
- Locker rooms
- Changing areas
- Breakrooms
- Designated smoking areas
- Lactation spaces
- Employee cafeterias
- Lounges
- Other areas where workers congregate while off-duty but on work premises.

This prohibition also includes collecting data on the frequency of use of those areas. The prohibition does not apply to the use of surveillance tools in common work areas, other than those listed above, so long as the tools are routine workplace surveillance tools and employees are made aware that the tools are being used.

In addition, employers are prohibited from surveilling a worker's residence, personal vehicle, or property owned, leased, or used by the worker, *unless the surveillance is strictly necessary.* The

---

[10] *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/

bill provides workers with the right to turn off or leave behind any surveillance tools that are on their person or in their possession during off-duty hours or in off-duty areas at the workplace. The bill also prohibits employers from requiring that workers physically implant a device in their body that collects or transmits data.

Finally, the bill provides various remedies for workers if their employer denies their rights under this bill or discharges, demotes, or suspends them. These remedies include the right to file a complaint with the Department of Industrial Relations or bring a civil action against the employer.

6) **Concerns raised by the opposition.** A coalition of business associations led by the California Chamber of Commerce argues that the language is overbroad and undermines workplace safety. Specifically, as it relates to the jurisdiction of this Committee, they write:

> **AB 1331 Is So Broad that It Applies to Every Business in California and Nearly Every Piece of Technology Used by Those Businesses.** There are many scenarios in which companies monitor their workplace, publicly accessible areas, company-owned property, and consumer data for safety and security-related purposes, including preventing theft or security breaches as well as keeping employees and customers safe. For example, hospitals use security cameras to ensure patients are safe and deter theft of medical equipment and medications. Manufacturers use key card systems to keep track of which employees are entering facilities with classified or proprietary information. Contractors use anti-theft measures to ensure expensive equipment is not stolen. Accounting firms use cybersecurity systems to protect consumer financial data.

The April 10th amendments to the bill allow employers to use routine workplace surveillance tools in any area not considered an off-duty space for employees, even if employees are present, as long as the employees are notified of the existence of the tools. This amendment should alleviate the concerns outlined by the opposition. Nothing in the bill would stop businesses from using theft prevention devices, security cameras, or key card systems. In addition, for workers who work remotely or drive company vehicles, surveillance tools are allowed as long as they are strictly necessary.

The coalition further notes:

> **Complying with AB 1331's Provisions Relating to Turning Tools Off and On Is Impossible.** Proposed subdivision (b)'s requirement (that all tools in the employee's possession be disabled during off-duty hours, including breaks) is impossible to implement. Different employees will have different schedules, meaning these tools would be turned off and on throughout the day, undermining their very purpose as described above. Regarding company vehicles, it is not uncommon for employees utilizing a vehicle to sit in that vehicle during a break. Safety or geolocation systems in those vehicles are often installed in a way that they cannot simply be turned off and on.
>
> Functionally, the only way to guarantee compliance is not to use certain systems at all or to give every employee access to those systems to turn them off and on – an outcome that will cause employers to violate existing laws related to workplace safety, sexual harassment prevention and cybersecurity requirements.

The April 10th amendments to the bill remove the blanket requirement that surveillance tools be disabled during off-duty hours. Instead workers are given the right to disable or leave behind tools that are on their person or in their possession during off-duty hours and in off-duty areas.

In addition, opponents raise the concern that "worker data" is defined as any information that is reasonably capable of being associated with a worker and is overly broad. The author may wish to consider narrowing the definition to ensure that it does not limit legitimate workplace information that constitutes work product or is necessary for payroll or other essential personnel or administrative purposes.

7) **Analysis.** This Committee has heard and analyzed a number of bills seeking to protect the privacy of people in California from intrusive surveillance and collection of their sensitive personal information. Particularly, the Legislature in recent years has prioritized protecting the privacy of individuals who may be most at risk, including immigrants and those seeking reproductive and gender affirming care. Importantly, in the same hearing as this bill, the Committee will be considering AB 1355 (Ward), which aims to prohibit the collection, sale, and sharing of individual's location data, except under certain narrow circumstances.

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. Given that starting point, ensuring that Californians do not have to give up their fundamental privacy rights in their workplace by limiting the most intrusive surveillance technologies and allowing workers to retain their rights while on their own personal time and in their own private spaces is in keeping with this Committee's efforts to strengthen Californians' right to privacy.

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

> **1561.** (d) Notwithstanding subdivisions (a) to (c), inclusive, an employer may use ~~**routine**~~ workplace surveillance tools ***that passively surveil workers in an area*** not listed in paragraph (1) of subdivision (a) even if an ~~**employee**~~ ***off-duty worker*** may be present, as long as the employer makes ~~**employee**~~ ***workers*** aware in advance that a workplace surveillance tool.

In addition, the Judiciary Committee has requested the following amendment:

> **1562.** (e) In addition to other remedies as may be provided by the laws of this state or its subdivisions, ***this part may also be enforced by a public prosecutor pursuant to Chapter 8 (commencing with Section 180 of Division 1).*** ~~**any public prosecutor may also institute an action for a violation of this part, including an action seeking injunctive relief.**~~

ARGUMENTS IN SUPPORT: The California Labor Federation, sponsors of the bill, and a broad coalition of labor organizations, argue:

> Workplace surveillance is not a new phenomenon. Employers have surveilled workers for decades with traditional cameras and microphones. However, today's workplace surveillance capabilities differ in scale, speed, and invasiveness. Employers now have access to a plethora of tools such as wearable devices to monitor worker biometrics, speech, and location, as well as heat and retina tracking technology. With the use of these powerful surveillance tools, workers have limited access to spaces in their workplace and homes that are not under constant surveillance. Areas such as restrooms, lactation spaces, and worker lounges are not protected from being surveilled with advanced technology that does not rely solely on

traditional audio or visual recordings. The new surveillance state at the workplace has proven to increase the likelihood of discrimination, harassment, and psychological distress of workers.

To protect worker privacy in sensitive areas and from developing implantable technology, AB 1331 will update and expand existing workplace privacy laws to address new surveillance technology. AB 1331 will prohibit the use of surveillance tools, such as wearable devices and heat sensing cameras, from being used to monitor private spaces like a restroom, lactation space, or breakroom. AB 1331 also prohibits employers from surveilling workers during non-work hours and limits employer surveillance of a worker's home or vehicle to what is strictly necessary for the job. Lastly, AB 1331 prohibits employers from requiring workers to implant or embed tracking devices in their body to ensure state law is ahead of technology being developed and tested currently.

The California Professional Firefighters write in support:

The explosion of AI programs and applications in recent years has upended many industries and professions, replacing human workers and developing faster than regulatory and oversight bodies have been able to keep pace. But even when AI is not taking the role of a human in the workplace in many cases it is still being implemented in ways that can have significant, life-altering consequences for the people it touches. The implementation of AI in workplace monitoring software, often in increasingly invasive ways and without the knowledge or consent of the workers it is monitoring, can result in the loss of employment for actions taken in what was believed to be private.

AB 1331 would prohibit the usage of surveillance devices and technology in spaces that can reasonably be assumed to be private, including restrooms, locker rooms, lounges, and others. It would also prohibit employers from monitoring employee's private property and vehicles, ensuring that workers are able to fully leave the workplace when they are off-duty and not forced to worry about their employer intruding on private moments. While data monitoring and digital surveillance is increasing in all of our lives, it is crucial that the right to privacy for workers is preserved and that employers are not given free access to every moment of their employees' lives.

ARGUMENTS IN OPPOSITION: In opposition to the bill, a coalition of county organizations argue:

We understand the reasonable concerns one could have about the slow creep of surveillance tools into every aspect of daily life and appreciate that one could imagine the appropriate limits are needed to prevent employers from snooping into the private lives of their employees. However, the scope of this bill is vast and would deem banal tools used for everyday work, including badge access, collaboration tools like Teams or Slack, or GPS tools used to track fleets, to be "surveillance tools". Under AB 1331, any device that collects or facilitates collection of data of an employee's movements, actions, communications, or behaviors, is deemed a surveillance tool that cannot be used in "off-duty areas," or can be turned off during "off-duty" hours.

AB 1331 will needlessly endanger public workforces and severely impair our ability to prevent and investigate instances of workplace violence. The bill prohibits local agencies from using a surveillance tool in any "off-duty area," defined to include breakrooms,

smoking areas, cafeterias, and lounges. How could public agencies mitigate or investigate workplace violence dangers if they cannot even monitor common areas like cafeterias? How can we keep our employees safe from the public if we cannot monitor public spaces like smoking areas?

To make matters worse, AB 1331 applies not only to surveillance of employees, but also the public. Section 1561(a) would prohibit local agencies from using routine surveillance tools in "off-duty areas," including designated smoking areas and areas where workers congregate while off-duty but on work premises. This section would effectively require public agencies to disable security cameras or other basic security tools in areas where they are needed to keep building entrances secure.

Under AB 1331, employees must be allowed to disable surveillance tools during off-duty hours or when they are entering off-duty areas. It's unclear how these rules would apply to a variety of tools that public employees may be required to use, including emergency alarms for teachers, body cameras for law enforcement, or tools used for public vehicle fleets, including dash cameras, speed monitors, or GPS tracking. Similarly, it's not clear how public agencies can adhere to the rules regarding off-duty hours for positions that are on-call or on standby, including law enforcement, emergency personnel, laboratory safety officers, and others.

Unfortunately, we have seen rising hostility and threats against government entities and their workforces. That includes violence and threats of violence against government employees whose job requires them to serve the public, like library staff, teachers, firefighters, benefits officers, among myriad other examples. It also includes public officials who are frequently targeted with threats or actual violence, including election workers, health officers, and public officials. AB 1331 would result in all of these public servants facing increased vulnerability at a time of strong anti-government sentiment.

To compound all of these concerns, AB 1331 imposes severe financial penalties and allows for private right of action for noncompliance.

REGISTERED SUPPORT / OPPOSITION:

Support

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
Coalition for Humane Immigrant Rights (CHIRLA)

Communications Workers of America, District 9
Community Agency for Resources, Advocacy and Services
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

Opposition

Acclamation Insurance Management Services
Agricultural Council of California
Allied Managed Care
American Petroleum and Convenience Store Association
American Property Casualty Insurance Association
Anaheim Chamber of Commerce
Associated General Contractors
Associated General Contractors San Diego
Association of California Healthcare Districts
Association of Orange County Deputy Sheriff's
Brea Chamber of Commerce
Calbroadband
Calforests
California Alliance of Family Owned Businesses
California Apartment Assocation
California Association of Health Facilities
California Association of Licensed Security Agencies, Guards & Associates
California Association of Sheet Metal & Air Conditioning Contractors National Association
California Association of Winegrape Growers
California Attractions and Parks Association
California Beer and Beverage Distributors
California Cardroom Alliance

California Chamber of Commerce
California Construction and Industrial Materials Association
California Credit Union League
California Farm Bureau
California Fraternal Order of Police
California Fuels and Convenience Alliance
California Gaming Association
California Grocers Association
California Hospital Association
California Hotel & Lodging Association
California League of Food Producers
California Moving and Storage Association
California Pest Management Association
California Restaurant Association
California Retailers Association
California Special Districts Association
California State Association of Counties (CSAC)
California Statewide Law Enforcement Association
California Travel Association
California Trucking Association
Carlsbad Chamber of Commerce
Chino Valley Chamber of Commerce
Coalition of Small and Disabled Veteran Businesses
Colusa County Chamber of Commerce
Construction Employers' Association
Corona Chamber of Commerce
Dairy Institute of California
Dana Point Chamber of Commerce
Flasher Barricade Association
Garden Grove Chamber of Commerce
Greater Coachella Valley Chamber of Commerce
Greater High Desert Chamber of Commerce
Housing Contractors of California
Insights Association
LA Canada Flintridge Chamber of Commerce
Lake Elsinore Valley Chamber of Commerce
League of California Cities
Livermore Valley Chamber of Commerce
Long Beach Area Chamber of Commerce
Long Beach Police Officers Association
Los Angeles Area Chamber of Commerce
Morgan Hill Chamber of Commerce
Murrieta Wildomar Chamber of Commerce
National Electric Contractors Association
Oceanside Chamber of Commerce
Orange County Business Council
Paso Robles Templeton Chamber of Commerce
Public Risk Innovation, Solutions, and Management (PRISM)
Rancho Cordova Area Chamber of Commerce

Rancho Cucamonga Chamber of Commerce
Redondo Beach Chamber of Commerce
Rural County Representatives of California (RCRC)
Sacramento County Deputy Sheriff's Association
San Jose Chamber of Commerce
Santa Barbara South Coast Chamber of Commerce
Santa Clarita Valley Chamber of Commerce
Security Industry Association
Sheriff's Employee Benefits Association (SEBA)
South Bay Association of Chambers of Commerce
Southwest California Legislative Council
Technet
Torrance Area Chamber of Commerce
Tulare Chamber of Commerce
United Contractors
Urban Counties of California (UCC)
Walnut Creek Chamber of Commerce
Western Electrical Contractors Association
Western Growers Association
Wilmington Chamber of Commerce
Wine Institute

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