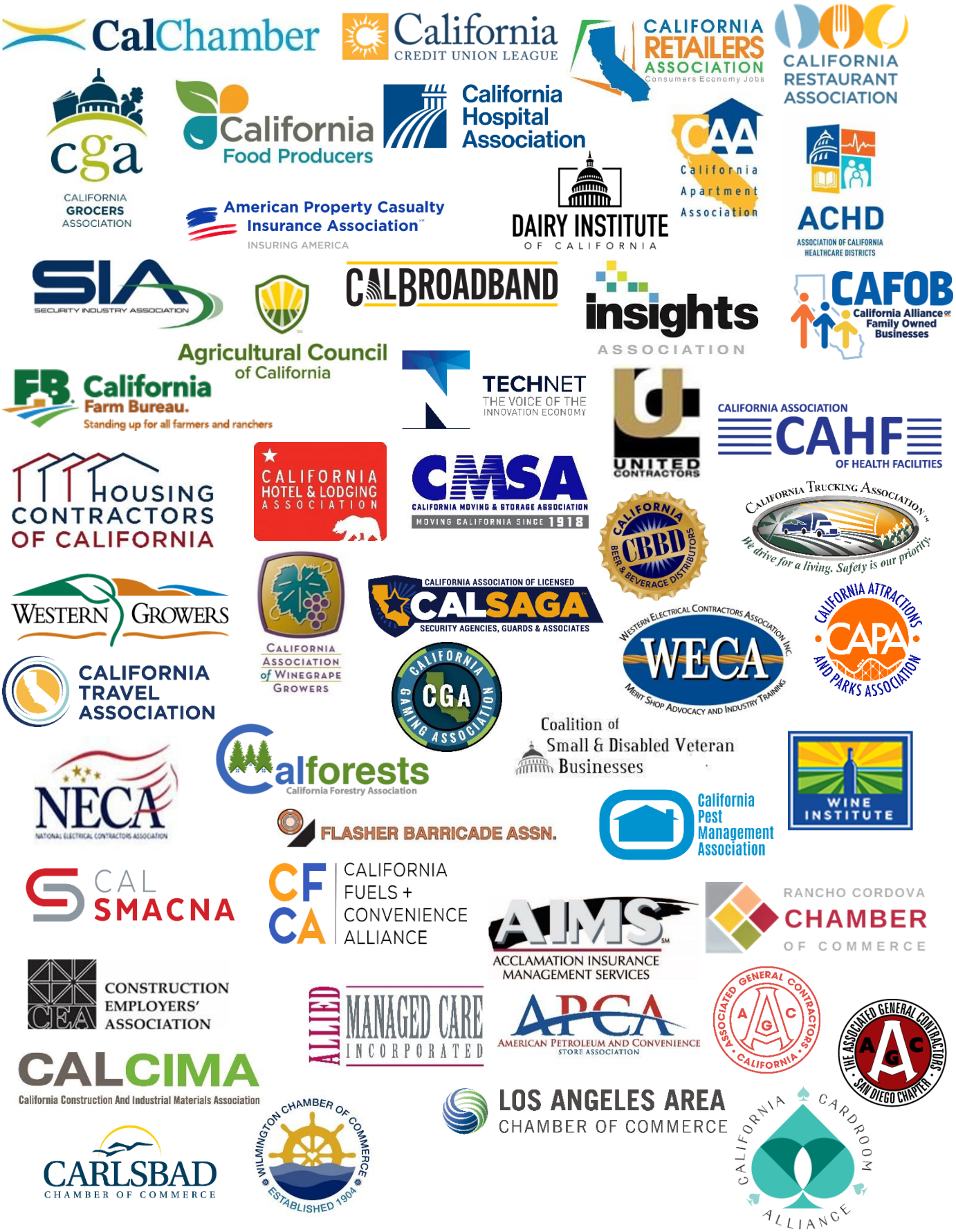
AB 1331 (ELHAWARY) – OPPOSE/COST DRIVER



UPDATED
COST DRIVER

TO: Members, Assembly Privacy and Consumer Protection Committee

SUBJECT: AB 1331 (ELHAWARY) WORKPLACE SURVEILLANCE
OPPOSE – AS AMENDED APRIL 10, 2025

The California Chamber of Commerce and the organizations listed below are respectfully **OPPOSED** to **AB 1331 (Elhawary)** as a **COST DRIVER**. **AB 1331** functionally prohibits the use of surveillance in every California workplace because of its overbroad language and, in doing so, undermines workplace safety. **AB 1331** will increase costs for all businesses, especially small businesses, by making workplaces less safe and exposing businesses to costly litigation for failing to comply with its unworkable provisions.

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.

Substantively, **AB 1331** is intended to ban surveillance of individual employees at inappropriate times or places, but uses unnecessarily overbroad language to do so, causing impractical results. **AB 1331** limits the use of "workplace surveillance tools," which is broadly defined to include *any tool* that collects or even "facilitates" the collection of "worker data." "Worker data" is defined as any information that is reasonably capable of being associated with a worker. In other words, **AB 1331** would limit the use of anything from old-school security cameras and keycards to cybersecurity tools and GPS tracking. In fact, the definition is so broad that even non-tracking devices such as *an email storage system* could fall under the bill.

In addition, AB 1331 restricts the use of "workplace surveillance tools" in three ways.[1] First, workplace surveillance tools cannot be used to monitor "private, off-duty areas," which is inappropriately defined to include even non-private, high traffic areas like cafeterias, breakrooms, and smoking areas. Second, workplace surveillance tools cannot be used to monitor a worker's residence, personal vehicle, or any property used by a worker unless it is strictly necessary. Third, workplace surveillance tools must be disabled during all "off-duty hours", including meal or rest breaks – though the fact that different workers have different off-duty hours and rest breaks is not contemplated by the bill. Moreover, the bill's provisions apply broadly, covering all companies in California, regardless of size or industry type.

AB 1331 Makes Workplaces Less Safe

AB 1331's sweeping provisions undermine security tools used by any company in California, including in sensitive industries such as healthcare, private schools/daycare, or financial institutions with access to consumer data. Some examples include:

- **Limitations on Use of Surveillance That Improve Safety and Security: AB 1331** severely restricts the use of basic security measures. For instance, employers like financial institutions or hospitals are highly regulated *because* theft of property or data would be detrimental to the individuals they serve. Similarly, hospitals must comply with strict cybersecurity requirements, including those under HIPAA and maintain a safe environment for health care workers, patients, and visitors. Their premises and computer systems must be monitored at all times for those systems to be effective, including locations where employees may congregate while off-duty. Further, the moment an employee goes on break, it would be illegal for them to have their key card swipes be tracked if they are on the premises. For agricultural employers, monitoring who is handling certain items or who is in specific areas is necessary for food-safety protocols. And, because of the breadth of **AB 1331**'s definitions, even a mundane function like a small company storing a personal email sent using a work email account could count as using a workplace surveillance tool during off-duty hours that a worker would be allowed to disable.

  Fundamentally, **AB 1331** prohibits the very mechanisms which employers are being *encouraged* or in some instances *required* to use to protect their employees under the new workplace violence standard, including any video or audio surveillance.[2] If an employee asked for a security camera due to a prior incident or feeling unsafe, **AB 1331** predetermines whether those cameras could even be allowed. For example, the employer could never put a camera in any area where workers "congregate while off-duty" or in a "designated smoking area" which could even just be outside the back door of a restaurant where members of the public are walking. If an incident occurred in an

[1] The fourth prohibition on physically implanting devices is not relevant here as we have no objection to that provision.
[2] *See* Labor Code Section 6401.9 (c)(2)(G) (requiring employers to have "[e]ffective procedures to respond to actual … workplace violence emergencies, including … effective means to alert employees of the presence, location, and nature of workplace violence emergencies.") Cal/OSHA is working on regulations that may include asking employees what types of measures could be implemented to deter future workplace violence incidents. Under **AB 1331**, an employer may not be allowed to implement any measure that qualifies as a "workplace surveillance tool" even where employees specifically ask for it.

employee break room or cafeteria, **AB 1331** prohibits the employer from ever putting a camera in there regardless of whether employees request it. Members of the public who entrust their safety and security to entities like hospitals, daycares, or schools that are caring for their loved ones would surely be uncomfortable knowing that workers with access to vulnerable populations and sensitive data are legally *not* allowed to be watched in areas where members of those populations may be. AB 1331 makes it difficult to use tools in high-traffic areas or review footage where there are allegations by employees or members of the public about assaults, harassment, theft, or other incidents. For example, it is not uncommon for places like healthcare facilities or schools to receive threats or have suspicious personnel on their premises. In those moments, security footage and monitoring of where people are becomes critical to the safety of both employees and the public. There are also certain companies with access to classified data or materials that require consistent monitoring of where people are for security purposes.

Recent amendments add subdivision (d), which provides that an employer may use surveillance tools outside of the "off-duty" locations listed as long as the employee is made aware. While we are not opposed to the general principle of disclosures regarding the use of tools, the details matter. For example, a financial institution should not be required to disclose the location of every single security camera, otherwise they would be effectively telling employees and contractors where theft could go undetected.

- **Monitoring of Property:** It is common for employees to utilize company property, for example computers, phones, vehicles, or industry-specific equipment including construction tools. Company-owned vehicles often include tools that measure driving speed or may include cameras to help determine the cause in the event of an accident. Being aware of whether an employee is driving recklessly or defending an employee in a road accident are all legitimate, beneficial uses of these types of systems. Employees may also take those items home with them, especially if their job requires them to travel to other locations outside of one central workplace location. It is well established policy that employees have a reduced right to privacy when using employer-owned or paid equipment.[3] As a result of **AB 1331**, anti-theft measures or geolocation devices used to track customer shipments or used for purposes of wage and hour compliance would now all be required to be disabled by the worker during breaks or after work. That requirement renders anti-theft measures completely useless. Regarding proposed subdivision (b), whether monitoring of that property is "strictly necessary" will be tested through expensive litigation.

- **AB 1331 Conflicts with Cal/OSHA Regulations and Other Labor Code Provisions, Including SB 553:** Cal/OSHA's heat safety regulations[4] ***require*** employers to monitor employees when they are on cool-down rest periods for safety. Tools such as cameras allow multiple groups of workers who may be spread out in different areas or cooling rooms to be more effectively watched for signs of heat-related illnesses. Surveilling those areas would violate **AB 1331** because that would be using a workplace surveillance tool in an area where employees congregate during breaks. Similarly, Cal/OSHA's workplace violence standard[5] also requires California employers to attempt to keep workers safe by improving visibility in and around the workplace – with a particular emphasis on being able to observe the location and actions of human threats and convey them to employees. Many employers have attempted to comply with these obligations by utilizing a combination of security cameras and other tracking mechanisms to observe parts of the workplace that staff cannot easily see and ensure that any individual entering a non-publicly accessible area is authorized to be there. Similarly, these same tools help employers identify a potential threat – such as an armed individual on the premises – and convey that location to employees and law enforcement. As described above, there are many scenarios in which cameras may be used in areas where employees congregate, such as outside of a restaurant or healthcare facility.

[3] *See*, *e.g.*, *TBG Ins. Services Corp. v. Superior Court*, 96 Cal.App.4th 443 (2002).
[4] Title 8, Section 3395 for outdoor heat, and Section 3396 for indoor heat
[5] Cal/OSHA is in ongoing rulemaking to create a regulatory text, but is presently enforcing from Labor Code 6401.9, created by Senator Cortese's SB 553 (2023)

- **Cybersecurity: AB 1331** requires every workplace surveillance tool that is in an employee's possession to be capable of being disabled during specified times such as meal breaks or off-duty hours. Such systems are located on items like computers that employees use. The success of any cybersecurity program, including ransomware defense, relies extensively on computer monitoring technology. Those systems are running all the time and are critical to quickly identifying attacks and detecting differences between benign behavior and attacks. Many companies utilize software to determine where users logging in are located to help detect potentially malicious behavior. These tools are designed for continuous background monitoring and are not meant to be switched off and on. Under **AB 1331**, the employer would be required to suspend cybersecurity monitoring every single time an employee goes on break or in cases where a remote employee steps away from their laptop. Not only does suspending monitoring undermine its very purpose, but also it is infeasible to turn those systems off and on every time a single employee stops working for just one minute. Practically, to comply with this bill the employer would be required to allow every worker themselves to turn those systems off and on, which raises its own security concerns. Similarly, the breadth of AB 1331's definition of workplace surveillance tools includes something like a server collecting incoming and outgoing emails. Turning those tools off and on negates their very purpose.

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.

Independent Contractors Should Not Be Included

The bill's definition of "worker" includes independent contractors, which should be removed from the bill. The above concerns are even more prominent when involving independent contractors. Contractors are often limited-term workers who are coming onto an employer's premises to do a specific job. They are new to the workplace, and often are not previously known to the employer (or its employees, customers, patients, residents, pupils, etc.), so potential security risks are heightened. And, similar to the exempt employees discussed above, the very nature of an independent contractor means that the company does not have control over their schedule. They can likely come and go as they please or take breaks at any time or place – making it impossible for an employer to even know when **AB 1331**'s overbroad prohibitions would go into effect. Functionally, the company would need to give contractors access to all surveillance tools and provide them with the ability to disable the tools, which is unsafe and impractical.

AB 1331 Puts Employers in a Catch 22 – Stop Using Security Systems or Be Sued

AB 1331's private right of action is inappropriate – particularly when it is difficult to even imagine how an employer could successfully comply with **AB 1331**. **AB 1331** puts employers in a no-win scenario – shut down all surveillance at all times (and make their workplace less safe), or face lawsuits because they will inevitably fail to comply with **AB 1331's** impractical requirements.

In sum, there has been no effort to tailor **AB 1331** to create a workable bill appropriate for today's workplace. Its broad application would be detrimental to public safety and is a "lose-lose" situation for both employers and their employees.

For these reasons, we strongly **OPPOSE AB 1331 (Elhawary).**

Sincerely,

Ashley Hoffman
Senior Policy Advocate
California Chamber of Commerce

Acclamation Insurance Management Services (AIMS)
Agricultural Council of California
Allied Managed Care (AMC)
American Petroleum and Convenience Store Association
American Property Casualty Insurance Association
Anaheim Chamber of Commerce
Associated General Contractors California
Associated General Contractors San Diego
Association of California Healthcare Districts
Brea Chamber of Commerce
CalBroadband
Calforests
California Alliance of Family Owned Businesses (CAFOB)
California Apartment Association
California Association of Health Facilities (CAHF)
California Association of Licensed Security Agencies, Guards & Associates
California Association of Sheet Metal and Air Conditioning Contractors National Association
California Association of Winegrape Growers
California Attractions and Parks Association
California Beer & Beverage Distributors
California Card Room Alliance
California Chamber of Commerce
California Construction and Industrial Materials Association
California Credit Union League
California Farm Bureau
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 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 (FBA)
Garden Grove Chamber of Commerce

Greater Coachella Valley Chamber of Commerce
Greater High Desert Chamber of Commerce
Housing Contractors of California
Insights Association
La Cañada Flintridge Chamber of Commerce
Lake Elsinore Valley Chamber of Commerce
Livermore Valley Chamber of Commerce
Long Beach Area Chamber of Commerce
Los Angeles Area Chamber of Commerce
Morgan Hill Chamber of Commerce
Murrieta/Wildomar Chamber of Commerce
National Electrical Contractors Association
Oceanside Chamber of Commerce
Orange County Business Council
Paso Robles and Templeton Chamber of Commerce
Rancho Cordova Area Chamber of Commerce
Rancho Cucamonga Chamber of Commerce
Redondo Beach Chamber of Commerce
San Jose Chamber of Commerce
Santa Barbara South Coast Chamber of Commerce
Santa Clarita Valley Chamber of Commerce
Security Industry Association
South Bay Association of Chambers of Commerce
Southwest California Legislative Council
TechNet
Torrance Area Chamber of Commerce
Tulare Chamber of Commerce
United Contractors
Walnut Creek Chamber & Visitors Bureau
Western Electrical Contractors Association
Western Growers Association
Wilmington Chamber of Commerce
Wine Institute

cc: Legislative Affairs, Office of the Governor
Sean Porter, Office of Assemblymember of Elhawary
Consultant, Assembly Privacy and Consumer Protection Committee
Liz Enea, Assembly Republican Caucus

AH:am