UPDATED
COST DRIVER

April 14, 2025

To: Members, Assembly Privacy and Consumer Protection Committee

SUBJECT: AB 1221 (BRYAN): WORKPLACE SURVEILLANCE TOOLS
OPPOSE/COST DRIVER – AS AMENDED MARCH 28, 2025

The California Chamber of Commerce and the organizations listed below respectfully **OPPOSE AB 1221 (Bryan)** as a **COST DRIVER. AB 1221's** sweeping definitions requirements would inhibit everything from workplace safety to privacy to ongoing litigation. Any misstep or error in implementation would result in a

costly private right of action for businesses of all sizes and would also have costly implications on state and local entities, who are both employers and third parties under the bill's broad provisions.

AB 1221's Notice Requirements Raise Several Concerns

As a general matter, we do not object to the concept of disclosing information about surveillance when that surveillance can result in employee discipline or termination. However, we have concerns with the breadth of the notices required under **AB 1221**. Examples include:

1. Employers would be required to notify workers about the "specific" locations of workplace surveillance tools. We are concerned by this language because, for example, that would require employers to tell employees specifically where security cameras or anti-theft tools are placed. Telling an employee exactly where they can be detected by a camera or where anti-theft measures are located may defeat their very purpose. Further, there are some industries such as finance that are legally required to monitor certain employee activities such as financial transactions. This is often done by a "secret shopper" type surveillance to ensure that the employee is complying with the law at all times.

2. **AB 1221** requires employers to provide notice of the names of "who" is authorized to access the data, including any "vendors", and "under what conditions" they have the worker data. The definition of vendor is broad and includes not only subcontractors, but also any "third party" or "entity" engaged by either the employer or the employer's labor contractor for a variety of purposes.

   As defined, it would include, for example, a law firm or insurance company where there is an employee claim at issue. A law firm representing the employer for purposes of an investigation or litigation would be given data such as emails or security footage about not only the plaintiff, but also other employees for purposes of assessing the claim or responding to discovery requests. In other words, that firm could be said to be collecting, storing, analyzing, or interpreting worker data. As a result, **AB 1221** would require the employer to notify every single employee copied on an email that has been turned over to counsel and "under what conditions" counsel has the email. This would compromise the integrity and confidentiality of any ongoing workplace investigation or litigation.

   Under the bill, a vendor may also encompass a company working on a confidential project. One company considering merging with another may need to send employee-related information as part of due diligence before the deal is made public or has been finalized. Another example is where companies engage vendors to assess pay scales and payroll. If an employer engages with a company to run a pay data audit to determine whether their pay is on par with pay in their industry or region, the employer would have to give every employee a 30-day notice before doing so and notify employees that they are running that study. There are legitimate reasons why HR may not want to roll out that news to employees until the study is completed and decisions are made about the results.

3. There must be an exemption to **AB 1221's** notice provisions where notice would undermine litigation, investigations, or safety and security. It is common for employers to suddenly monitor employee conduct as part of an investigation. Our members must do this for incidents such as suspected fraud or employees engaging in inappropriate conduct via their work computers. Providing a 30-day notice in those scenarios may not only be impossible, but it also undermines the purpose of the investigation.

AB 1221's Restrictions on Transferring Data are Unworkable

Proposed Section 1552(a) provides that an employer cannot transfer any worker data, *including deidentified or aggregated* data to any third party unless the "vendor"[1] is under contract and agrees to, among other things, agree to be jointly and severally liable for any data breaches. As raised in Footnote 1, we are assuming the language does in fact put this restriction on all third parties who receive the data (not only "vendors"). That would include, for example, state agencies when they receive any worker information as part of required reporting (*e.g.*, annual pay data reports submitted to the Civil Rights Department) or investigations or litigation.

Existing law addresses the circumstances under which a company should be liable for a data breach, including under the Customer Records Act (see Civil Code Section 1798.80 et seq.), and most recently, created additional liability under the California Consumer Privacy Act (CCPA).[2] The CCPA does not automatically impose (or expressly address for that matter) joint liability between two contracting entities regarding consumer data breaches and there is no rationale to do so here with employee data. But even in the absence of an express joint and several liability provision, the duties of a business under the CCPA statute, could potentially extend to service providers or contractors of a business.[3] Any newly created liability for breaches of worker data should mirror existing legal frameworks on this issue. If joint and several liability is a contract term that the employer wishes to include in their contract with a third party, they are free to do so. It does not need to be a statutory mandate. It also does not make sense when, as discussed above, this provision as written would apply to government entities like the CRD.

Proposed Section 1552(b) prohibits sharing worker data with anyone in government unless required to do so by law. That is unworkable given that worker data is effectively *anything* that is even capable of being associated with a worker. This would prohibit something as simple as sharing information about an employee to recommend them for a job with the state to something as vital as sharing information with law enforcement about suspected unlawful activity.

Proposed Section 1552(f) requires any vendor to return worker data collected through a surveillance tool to the worker themselves (and their authorized representative by definition) and delete any remaining copies at the end of the vendor's contract. Again, this is unworkable. A "vendor" as broadly defined would include counsel or third-party discovery vendor performing an investigation or storing/analyzing data or litigation. It would not make sense for them to return that litigation data to the worker themselves. Many contracts do address destruction or return of data, for example e-discovery vendors often have standard protocols.

Finally, deidentified and aggregated data should not be on the same footing as data that can be used to identify an individual. That data has been stripped of things that directly identify specific employees, thus reducing the risk of harm from breaches and misuse. In fact, treating deidentified or aggregated data this way is contrary to other statutes.[4]

---

[1] This may be a typographical error in the bill. That subdivision says the employer cannot transfer data to a "vendor, subcontractor, or other third party, including another employer, unless the **vendor** is under contract . . . ." We are going to assume that the bill does mean to prohibit transfer to any third party, even if they do not meet the definition of "vendor" in the bill.

[2] See California Civil Code Section 1798.150

[3] *See* Section 7051 of the CCPA regulations, stating that the contract required by the CCPA for service providers and contractors must, among other things, require the service provider or contractor to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that it collected pursuant to the written contract with the business—providing the same level of privacy protection as required of businesses by the CCPA and these regulations. For example, the contract may require the service provider or contractor to cooperate with the business in responding to and complying with consumers' requests made pursuant to the CCPA, and to implement reasonable security procedures and practices appropriate to the nature of the personal information […].; *See Barnes v. Hanna Andersson, LLC* , N.D. Cal., Case No. 20-cv-00812.

[4] See, e.g., Civil Code sections 1798.82 and 1798.140(m).

AB 1221's Limitations on the Use of Workplace Surveillance Tools are Unworkable

Proposed Section 1553(a)(2) provides that employers cannot use a workplace surveillance tool that identifies, obtains, or infers information about workers engaging in protected activities. A security camera is going to capture whatever footage it captures. For example, a camera cannot turn itself off during a strike or if an employee chooses to have a meeting with another employee in an open area. If employees are choosing to use their company emails or messaging functions to discuss protected activity, those communications are under cybersecurity programs or likely being stored on a server for purposes of record retention. While we appreciate the intent of not wanting to deter employees from exercising their rights, this is just not practical as written.

Proposed Section 1553(a)(3) provides that a workplace surveillance tool cannot be used to obtain a variety of information about employees, such as religious or political beliefs, veteran status, health status, and more. Given the breadth of "workplace surveillance tools", this is not possible just as a practical matter. For example, job applicants will have volunteer work, military service, or prior jobs on their resume that will include information about these topics. Those resumes will likely be collected when received through databases or even simple email storage systems that may constitute a workplace surveillance tool as defined. Further, many larger employers have affinity groups such as for people of certain religions or mentorship programs for neurodivergent employees, so those meetings will occur over computer platforms or potentially in areas where there are security cameras or require badging in and out. The Fair Employment and Housing Act (FEHA) very clearly outlines which classes of people are protected from discrimination. If an employee believes they've been subject to unlawful discrimination, they already have the right to bring a claim under FEHA.

Proposed Section 1553(a)(4) prohibits any use of facial recognition, gait recognition, or emotion recognition by a workplace surveillance tool. In the age of cell phones, a ban on facial recognition is not practical. For example, it is common for employees to clock in and out on employer-provided cell phones or their own cell phones. Facial recognition can be enabled on cell phones. Some employers may periodically monitor an employee's gait to evaluate the most efficient way to organize a warehouse or an employee's job duties so that the employee can be the most successful.

AB 1221 Restrictions on the Use of Surveillance Tools for Employment-Related Decisions are Overly Prescriptive and Lead to Bizarre Public Policy Outcomes

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. To provide a few examples, under this language, an employer would be prohibited from:

1. Disciplining an employee based on conduct caught on a security camera, including criminal activity.
2. Disciplining an employee for inappropriate content contained in an email.
3. Disciplining an employee based on a recorded call with a customer.
4. Disciplining an employee where a camera detects them not wearing proper PPE.
5. Disciplining a remote worker who is failing to timely take meal or rest periods (many employers are forced to have such policies because of the rampant shakedown PAGA lawsuits alleging meal and rest break violations).
6. Enforcing policies against working off-the-clock.
7. Disciplining a worker who is speeding in a school zone or consistently deviating from their delivery route.

Employers need to be able to rely on monitoring for clearcut violations of policies and laws. Otherwise, this will result in bizarre public policy outcomes like not being able to discipline a worker for an inappropriate

email or requiring supervisors to micro-manage workers because they must be able to independently corroborate every single thing that a worker does.

AB 1221's Right of Access and Correction is Problematic

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.[5] 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.

AB 1221's Application Should be Narrowed

As defined, a "worker" includes not only employees, but also job applicants, independent contractors, and a worker's "authorized representative." We have several concerns with the breadth of this definition. The first is that independent contractors should not be included. Not only does much of this bill not make sense as applied to independent contractors because they are not employees (for example, lengthy notice requirements), but to the extent a contractor is interested in data collection, that is something that can be agreed to within their contract with a company. With regard to job applicants, some of **AB 1221** would not make sense. For example, the breadth of "workplace surveillance tools" may include computer systems that collect or store resumes or security camera footage when the applicant comes in for an interview. It would not be possible to give an applicant a 30-day notice of use of those systems.

Including an "authorized representative" in the definition of worker implies that employers must provide required notices to attorneys or union representatives and that those people would have the same rights of access and correction as the employee themselves. This compounds our concerns regarding privacy and places a high burden on an employer as far as disseminating the required disclosures. To the extent employees wish to consult with counsel or a union representative regarding an aspect of their employment, they are free to do so.

AB 1221's Retention Period Should be Shorter

AB 1221 requires employers to retain any data collected from a workplace surveillance tool to make employment-related decisions for at least five years. Such a long retention period is counter to privacy protections. The best practice is to retain data for only as long as necessary. The longer data is retained, the greater the risk of a data breach and increased liability for employers. Regardless of how well a business protects its data systems or invests in cybersecurity, no solution can provide absolute security.

AB 1221 Creates a Private Right of Action

Any misstep in interpreting or implementing **AB 1221**'s broad requirements would subject a business of any size to a private right of action, including penalties.

For these and other reasons, we are **OPPOSED** to **AB 1221 (Bryan)** as a **COST DRIVER**.

[5] See Civil Code Section 1798.110, 1798.130, and accompanying regulations, which are available at: California Consumer Privacy Act Regulations

Sincerely,

Ashley Hoffman
Senior Policy Advocate
California Chamber of Commerce

Associated Builders and Contractors of California
Associated General Contractors California
Associated General Contractors San Diego
American Petroleum and Convenience Store Association
California Apartment Association
California Association of Health Facilities (CAHF)
California Association of Sheet Metal and Air Conditioning Contractors National Association
California Association of Winegrape Growers
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 and Lodging Association
California League of Food Producers
California Manufacturers and Technologies Association
California Moving and Storage Association
California Restaurant Association
California Retailers Association
California Trucking Association
Civil Justice Association of California
Construction Employers' Association
Dairy Institute of California
Housing Contractors of California
Insights Association
Los Angeles Area Chamber of Commerce
National Electrical Contractors Association
San Jose Chamber of Commerce
Security Industry Association
TechNet
United Contractors
Western Electrical Contractors Association
Western Growers Association
Wine Institute

cc: Legislative Affairs, Office of the Governor
Kenneth Cruz, Office of Assemblymember Bryan
Consultant, Assembly Privacy and Consumer Protection Committee
Liz Enea, Assembly Republican Caucus

AH:am