JOB KILLER

April 25, 2022

TO: Members, Assembly Privacy and Consumer Protection Committee

SUBJECT: AB 1651 (KALRA) WORKER RIGHTS: WORKPLACE TECHNOLOGY ACCOUNTABILITY ACT
OPPOSE/ JOB KILLER – AS AMENDED APRIL 18, 2022
SCHEDULED FOR HEARING – APRIL 27, 2022

The California Chamber of Commerce and the organizations listed below respectfully **OPPOSE AB 1651 (Kalra)** as a **JOB KILLER. AB 1651** imposes overly broad requirements on both public and private employers of all sizes, contains unworkable mandates that would in fact invade worker privacy and chill new technologies, and buries employers and employees alike in vast amounts of red tape, and ignores contradictory mandates already in the law. The bill's punitive enforcement section subjects even the most well-intentioned employer to egregious penalties for any minor, technical violations that will, without question, lead to businesses shutting down and the loss of jobs.

AB 1651 Undermines the Integrity of the Legislature by Attempting to Shortcut the Legislative Process

In 2018, the landmark California Consumer Privacy Act (CCPA) was enacted to provide consumers extensive information and control over personal information (PI) collection practices and usage of their personal information. The following year, the definition of "consumer" was clarified to simultaneously exempt individuals when acting in their capacity as employees, but also expressly preserve certain rights for employees, such as the right to receive notice about what information is collected about them. A sunset was added to that exemption to encourage stakeholders to revisit the issue of appropriate employee privacy rights. Each time the sunset has come up for review, the business community has done outreach to labor and employee organizations to discuss extension in advance of any legislation moving forward.

This last year has been no different. For months, CalChamber operated in good faith to maintain open lines of communication around the sunset provisions and expressed a desire to work with the sponsors of this bill to enact strong, but workable, employee protections including on issues regarding employee monitoring and automated decision systems (ADS)**.** We were told by **AB 1651**'s sponsors that we would be provided language of their proposal in advance of it going into print. Instead, 48 hours before the Assembly Labor and Employment Committee hearing and 24 hours before the last regularly scheduled Assembly Privacy and Consumer Protection Committee hearing, this 33 page bill was introduced. It is full of redundancies, unworkable prohibitions that at times even undermine privacy rights, and a heavy handed private right of action that is assured to put well-intentioned companies out of business. It applies to businesses of every size as well as public entities. Buried underneath upwards of 20 notices, many of which contain numerous subparts and elements, are the beginnings of tangible privacy rights on which CalChamber and others could have provided constructive feedback to avoid unnecessary harms had the proponents chosen to likewise respond to us in good faith.

Stated plainly, there was no reason for the proponents of this legislation to draft this bill in the dark, precluding an open, honest, transparent discussion around the public policy set forth in this legislation. CalChamber, our members, and our coalition partners continue to review the many operational and legal problems contained in **AB 1651**. However, we provide this feedback in an effort to help differentiate between the workable, or potentially workable, elements of this bill from those that undermine employee privacy rights or that would result in untenable public policy, since members of the Privacy Committee are being jammed by these late amendments and must consider this legislation under extraordinarily tight timelines.

AB 1651's Restrictions Around Collection, Storage, Analysis and Interpretation of Worker Data Are Unreasonable, Unworkable, and Counterproductive to Ensuring Worker Privacy

AB 1651 imposes untenable mandates on employers that will ultimately reduce employee privacy. Proposed Section 1533 provides that an employer may not "collect, store, analyze, or interpret worker data" unless it is "strictly necessary" to accomplish at least one of the following:

1) Allowing a worker to accomplish an essential job function.
2) Monitoring production processes or quality.
3) Assessment of worker performance.
4) Ensuring compliance with employment, labor, or other relevant laws.
5) Protecting the health, safety, or security of workers.
6) Administering wages and benefits.
7) Additional purposes to enable business operations as determined by the labor agency.

The listed allowable reasons are too limited, and the standard by which an employer must evaluate if they can collect, store, analyze, or interpret worker data for the permissible purposes is far too stringent.[1]

[1] By contrast, under the CPRA, consumers have the right to direct a business to limit the use of their sensitive PI to that which is "necessary" to perform the services or provide the goods reasonably expected by the average consumer who requests those goods or services. (See Civ. Code Sec. 1798.121.) For other types of PI, the collection, use, retention and sharing must be reasonably necessary and proportionate to achieve the purposes for which the PI was collected or processed as a general matter. (See Civ. Code Sec. 1798.100.)

Even more problematic is that this section could require employers to engage in overly invasive reviews of every single document or communication produced by an employee to determine if it falls under one of these categories. Not only is that nonsensical and practically impossible, but it also reduces an employee's privacy. Under this bill, if an employee uses their work email to send a personal email, the bill seems to require the employer to actively read those emails. The employer would then be required to delete that email because it would not qualify under one of the above categories. Having that email saved through Outlook or another email system to their server or even locally to a work-issued computer could be a violation of this proposed law. Specifically, each violation of Section 1533 would be subject to a $20,000 fine.

The requirement to delete any data that does not fall under one of the above categories raises significant concerns regarding preservation of evidence. This measure could frustrate an employer's efforts to rid the workplace of sexual harassers. An inappropriate email or text message that would help prove a harassment victim's case may be required to be deleted under this requirement. Emails, calendar appointments, or other documents that could help support a worker's claim for unpaid wages could be deleted. Again, this section has unintended consequences that will hurt *workers*. Further, because this would apply to public employers, it also undermines the California Public Records Act and likely violates Article 1, Section 3 of the California Constitution.

Further, determining whether a piece of worker data falls under any of the above is nearly impossible. For example, as explained further down in this letter, "essential job function" is vague, ever-changing, and subjective. Category seven is completely dependent on future regulations adopted by the labor agency. That is not required to be done under **AB 1651** until 2024, if it is in fact completed by that date. Employers will be required to make determinations about whether they are allowed to store data long before those regulations are in place. Their vendors will also be required to make these decisions not only regarding existing products and features, but also those in development, with the employer jointly and severally liable for any good faith errors.

The use of "analyze" or "interpret" here is also a Catch-22. As previously stated, to comply with this proposed section the employer could be <u>required</u> to analyze all of an employee's documents and communications. By doing that, they are already in violation of this section.

<u>AB 1651 Fails to Recognize Beneficial and Necessary Uses of Biometric, Health and Wellness Data That Would be in Furtherance of Worker Rights, Privacy and Data Security Interests</u>

Proposed Section 1533 also places limitations on the ability to transfer or disclose biometric, health, or wellness data unless required by law. However, the bill fails to recognize that there are many instances in which transferring or disclosing this information is either beneficial or necessary to protect the privacy and safety of the employee, of other employees, or the public. For example, if an employee requests a reasonable accommodation, medical leave, or has a workers' compensation claim, there must be exchanges of information regarding that employee's health information with entities that would be considered third parties under **AB 1651**. By way of another example, employers need to be able to conduct background checks, and this bill could preclude them from doing so unless required by law.

AB 1651 requires an employer or vendor to delete biometric, health, or wellness data when the initial purpose for collection has been satisfied or upon the worker's termination or resignation unless there is a "reasonable interest" in keeping the data, which is undefined. This is problematic for several reasons. First, it is in direct conflict with the Cal/OSHA regulation that requires employers to keep employee medical records for the length of employment plus <u>30 years</u>. (*See* 8 CCR 3204(d).) Second, this data could be necessary for litigation or a pre-litigation dispute. This is especially true considering that information is relevant to a broad scope of claims such as leave-related claims, reasonable accommodation, wage and hour, and workers' compensation claims, etc. Many of those claims carry a three or four year statute of limitations. Again, simply directing an employer to immediately delete all of this data has negative unintended consequences on both workers and employers.

AB 1651 prohibits employers or vendors from relying on biometric or wellness data as a basis for an employment-related decision. Again, this has negative unintended consequences for the worker. First, it is unclear what "wellness" data means, but is likely relevant to accommodation requests, leave requests, and

workers' compensation claims. This bill would effectively preclude reliance on a background check using biometric data in making decisions around hiring as well.

Biometric data has significant beneficial uses both for employers, workers, and the broader public. It, for example, serves as fraud prevention for security related purposes such as controlling door access within a secure workplace, helping better protect data by more accurately authenticating an individual attempting to access a database or system, and enabling background checks through fingerprinting. It is also often used to identify employees as they clock into work for large employers. It is more secure because it prevents any manipulation by an employee or their supervisor. It is not used for any nefarious purpose as implied by the bill, simply to ensure workers are accurately clocked in and out. We are more than willing to discuss the use of this data, disclosures, and how to ensure this data is secure, but an outright ban is unnecessary and will have negative consequences.

AB 1651's Right of Access is Both Problematic and Invasive of Worker Privacy

Proposed Section 1531 allows a worker to request information about data collected about them. While we are agreeable to making such disclosures as a general matter, we believe it is wholly unnecessary given the employee's right to receive notice about what information is collected about them under the CPRA. (See Civ. Code Sec. 1798.100.) That aside, this section contains several problematic provisions. First, "sources" is not defined in (a)(2). It is therefore unclear whether the employer is required to summarize the sources from which the data is collected, or actually turn over every piece of data. If the latter, this could be impossible to comply with because it would require copying every single email, text message, calendar invite, chat, Slack message, browser search history, physical documents in an employee's office, etc. This would result in thousands of documents for many workers and may include confidential, proprietary, or privileged information. Second, disclosing the names of "vendors or third parties" is also likely to include confidential, proprietary, or privileged information. An employer who sends an employee's emails to opposing counsel because it is relevant to e-discovery in a legal claim by another employee or regarding a business contract could be required to divulge that. One company considering merging with another may need to send labor-related information as part of due diligence before the deal is made public or has been finalized. There must be exceptions in any disclosure requirements for such information. And finally, the Legislature should give strong consideration to the granularity of the information to be provided here. Even if a business is not monitoring this data whatsoever, it would have to go about collecting the data that exists on its servers, on the desktops of employee computers, and hard copies of any documents in at an employee's office or desk to respond to an access request. That would actually be more invasive of employee privacy.

AB 1651's Right to Correct Undermines Confidentiality Interests of Employees and Hamstrings Employers From Taking Action Against Employees Who Have Been Found to Engage in Serious Misconduct

The so-called right to correct in proposed Section 1532 is problematic. It is not limited to situations in which the employee can objectively verify that data is inaccurate. It would apply to items like performance reviews or human resources investigations. For example, consider if a worker is the subject of a human resources investigation for misconduct. If the worker disputes the outcome, the worker could require the employer to: 1) re-investigate the situation, 2) re-explain the evidence supporting the outcome, and, most concerning, 3) disclose the source of the information. "Source" is undefined and would surely be argued in court to mean the exact names of individuals. Human resources investigations are generally kept confidential to preserve the integrity of the investigation as well as protect all witnesses involved. No worker will feel safe making a complaint or participating in an investigation if the person at issue can subsequently require the employer to disclose all source names to them and the information they provided.

The employer is also prohibited from making any employment-related decision while the accuracy of worker data is being re-investigated. This bill appears to prohibit an employee who is found to have engaged in serious misconduct therefore from being promptly disciplined, reassigned, or terminated, to the detriment of other workers.

Furthermore, unlike the right of correction in the CPRA, there is no recognition that the right of correction does not extend to data about the worker that belongs to, or that the business maintains on behalf of,

another person. Meaning, what would happen if a worker wants to correct what they believe to be inaccurate information about them in the emails or text messages of another worker?

AB 1651's Electronic Monitoring Prohibitions are Laudable but Overreaching, and Need Significant Narrowing to Avoid Detrimental Outcomes

During our meetings with the sponsors earlier this year, we were told that restricting employer monitoring of workers outside of working hours was the primary issue they sought to address, and we agreed that this is a concept we are supportive of discussing. We remain committed to engage on this topic, but do have concerns with the proposed language in **AB 1651**.

AB 1651 Will Effectively Chill Any Use of Electronics to Help Manage Employees

Proposed Section 1543 prohibits electronic monitoring unless it is "strictly necessary" to accomplish the purpose at issue and is the "least invasive means" that could reasonably be used. This is such a high standard that it could effectively chill the use of any monitoring. Devices used to track where a delivery driver is or where a technician on a house call is, are generally agreed to be beneficial to all involved: customers know when to expect these services, companies can monitor drivers for purposes of scheduling, and it enhances safety for the driver in case they need roadside assistance or an unexpected event occurs while completing their duties. Recording customer service calls ensures quality control as well as assists other customer service representatives who help a customer because they can review prior interactions with that customer. Yet, with such a high bar, these devices could inevitably be challenged in court as to whether that is "strictly necessary" or the "least invasive means". As a matter of public policy, many would agree that some of these monitoring functions may not be strictly necessary, but the benefit they provide to customers, the worker, and the employer make them preferable and acceptable practices.

Further, the breadth of the definition would include standard cybersecurity tools that companies use to prevent breaches and data loss (which they would be required to do under this bill), protect their own confidential data, as well as personal data of employees and customers. Even if this technology falls under the "allowable purposes," it would first be subject to approval by the labor agency which has absolutely no expertise in this issue area and will likely take months or years to approve these systems given that every company in California must submit for approval.

Proposed Section 1543(b) provides a list of prohibited practices. We generally agree with the intent of these prohibitions but would propose the following changes at this time, noting again the short time our members have had to analyze this:

> *(2) The monitoring of workers who are off-duty and not performing work-related tasks.* We generally agree with this, but believe additional clarifications are necessary. For example, it is foreseeable that a worker who is off-duty and who has not yet left the premises may be caught on security footage. Or consider a worker who logs in after hours to make changes to their health insurance benefits - the employer would be prohibited from using standard security protocols to ensure the correct person is accessing that worker's account. Such "electronic monitoring" should be permissible.
>
> (4) *Audio-visual monitoring of bathrooms or other similarly private areas, including locker rooms, changing areas, breakrooms, smoking areas, employee cafeterias, and lounges, including data collection on the frequency of use of those private areas.* We believe breakrooms, smoking areas, employee cafeterias, and lounges are quasi-public areas that should be allowed to include security cameras if the employer so chooses, which is consistent with Labor Code Section 435. This is for the safety of the workers and the public, especially when you consider that this may include the outside of the building or parking lot if that is where employees choose to take smoking breaks. Further, this type of technology was used during the pandemic to manage capacity in those spaces for purposes of social distancing.
>
> (5) *Audio-visual monitoring of a workplace in a worker's residence, a worker's personal vehicle, or property owned or leased by a worker, unless that audio-visual monitoring is strictly necessary*

to ensure worker health and safety, to verify the security of company or client data, or to accomplish other similarly compelling purposes. Again, we agree with this intent, but the bill's overbreadth has unintended consequences. This provision arguably includes video conferencing systems used between workers who may be working from home. The intent is using those systems to conduct meetings or record presentations, not active monitoring, but because of the breadth of "electronic monitoring," the employer could not require workers to have their cameras on during meetings and may be in violation of this section if the employee chooses to turn on their camera. This provision should consider that workers may be performing job duties in their personal homes or vehicles.

(6) *Electronic monitoring systems that incorporate facial recognition, gait, or emotion recognition technology.* An outright ban on these technologies fails to account for the benefits they can have for workers. For example, some video conferencing products contain facial recognition features that employees can opt into. 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.

Regarding installing applications on personal devices, employers should be able to require the use of some applications if the worker refuses a separate work device. Many workers would rather use their personal phones for work purposes than carry around a second, separate phone, or use their own computers or tablets. As written currently, because no applications may be installed on a personal device, employers will have no choice but to force workers to carry separate devices. If the worker would prefer to use their own device, the employer should then have the ability to mandate certain applications. Again, the bar here of being "strictly necessary" for essential job functions is ripe for litigation. Regarding disabling certain applications or devices, the language should reflect the fact that it may be the worker who needs to actively disable the application or device when they finish working. Instead of saying these applications shall be disabled, the language should provide that workers must be allowed to disable these applications when they are off-duty.

AB 1651 Restrictions on the Use of Electronic Monitoring for Employment-Related Decisions are Overly Prescriptive and Lead to Bizarre Public Policy Outcomes

AB 1651 prohibits an employer from making any hiring, promotion, termination, or disciplinary decisions based solely on electronic monitoring. It requires "independent corroboration" for any such decision, which is undefined. This ban is overreaching. To provide just 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. Promoting a worker who is consistently meeting productivity goals as tracked by a software program.
4. Disciplining an employee based on a recorded call with a customer.
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 to some degree for employment-related decisions. 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 completely micro-manage workers because they must be able to independently corroborate every single thing that a worker does.

AB 1651 Misunderstands Automated Systems and Their Benefits

AB 1651 misunderstands ADS in two fundamental ways. First, it conflates fully and partially automated ADS. A partially automated ADS assists in decision making but doesn't make the decision. In the context of this bill, it's the difference between a system that automatically promotes an employee and one that recommends an employee for a bonus based on work performance. This bill would be better limited to fully automated decision systems. Instead, it inhibits the adoption of technologies that already have human oversight in the decision process by nature of their design.

Second, it overlooks the uses and benefits of ADS and why employers adopt them. These systems allow employers to operate more efficiently, which also benefits workers. By automating certain functions, like keeping track of sales, it allows workers to focus on their essential job functions and can automatically reward them when they achieve goals. Some timekeeping and scheduling software systems help proactively identify wage and hour issues and compensate employees for missed meal and rest periods. ADS serves a crucial role in protecting the public by identifying and tracking product recalls and defects and is capable of identifying retailers throughout the supply chain that may have received or sold a defective product or produce with foodborne illnesses. **AB 1651** would have a chilling effect on the deployment of workplace safety tools that have enabled a higher safety standard in manufacturing, warehousing, transportation and logistics, healthcare, and retail.

Further, proposed Section 1553 prohibits an employer from using an ADS to make an employment related decision that violates the law or makes predictions about workers exercising their legal rights, which we believe are appropriate. However, banning the use of customer ratings as inputs for ADS is unnecessarily prohibitive. Customer service ratings can be a useful and reasonable means of evaluating and rewarding worker performance.

AB 1651's Overly Prescriptive Assessments are Costly to Complete, Require the Disclosure of Proprietary Information, Expose Cybersecurity Risks, and are Ripe for Abuse by Anonymous Disputes

Instead of banning egregious misuses of technology in the workplace, **AB 1651** could make it nearly impossible to adopt new technologies that benefit workers and businesses. It requires employers to make an independent assessment of an ADS and appoint a "designated internal reviewer" to corroborate every ADS output. Again, because these terms are so broadly defined, this means a full-time employee second guessing every automated calculation a spreadsheet makes. Even if the definition were narrowed sufficiently, having a designated internal reviewer with the expertise and free time this bill requires will be extremely costly, untenable for small businesses, and misses the benefit of automating these systems. An ADS can analyze a multitude of factors, using far more inputs than a human can, to reach an output. They achieve these results more consistently than human decision makers while analyzing far more information. It is a waste of resources and time for a human to double check every ADS output.

Proposed Section 1560 requires an employer to complete and submit an Algorithmic Impact Assessment (AIA) before using the system and retroactively for any ADS already in use for each separate position for which the ADS will be used. Because ADS is so broadly defined, a separate AIA will have to be conducted for each spreadsheet, scheduling software, payroll system, or inventory tracker that falls under the definition. Not only is the number of AIAs required by the bill excessive, the requirements are overly prescriptive and focus almost entirely on the possible negative impacts of an ADS without consideration of the benefits.

Proposed Section 1560 (b)(1) requires proprietary information about ADS by asking for a detailed description of the ADS, which in most cases is not information an employer would have or would be at liberty to disclose. The AIA must also include a thorough evaluation of the risks of ADS including the potential for errors, violations of legal rights of affected workers, and potential discriminatory impacts. While all of these are appropriate considerations in developing these systems, this section also requires more subjective evaluations, such as the risk of indirect harms to the physical, mental, or safety of workers, negative economic impacts on workers, and most problematically whether the system would infringe on the dignity and autonomy of affected workers. Subjective standards are difficult to implement and will lead to inconsistent applications across employers and vendors.

The AIA must thoroughly evaluate all of these potential risks, but there is no balancing or consideration of the benefits of these systems. An employer may monitor the speed of its delivery vehicles, which could have privacy concerns that should be accounted for, but which should be outweighed by the benefit to public safety and to drivers by ensuring they are driving the speed limit. In developing ADS, possible negative outcomes should be considered by employers and vendors in order to be mitigated. However, there should similarly be consideration for their benefits and **AB 1651** lacks that balance.

Furthermore, the bill requires the AIA to be completed by an independent assessor at the beginning of the procurement process but also continuously updated thereafter. It is unclear how often "continuously" is intended, but it would be incredibly costly to employ an independent assessor to monitor one ADS that frequently. The bill lays out all the considerations the AIA must incorporate in section 1560, then includes different standards and processes the assessor must consider and complete in section 1562. The bill should either require an AIA or define how an independent assessor should evaluate an ADS, not both.

If completing the AIA and independent assessment were not enough, the employer is required to publish a summary on their website. Due to the specific information required in the AIA, this will likely require the disclosure of proprietary and sensitive information. **AB 1651** requires the AIA to include potential privacy risks, which employers are then required to disclose publicly including their efforts to mitigate those risks. This creates a massive cybersecurity risk, effectively telling hackers which aspects of their systems are most vulnerable and how they are secured.

Proposed Section 1563, which allows a worker to anonymously dispute an AIA and challenge the sufficiency of both the assessment as well as the implementation of the ADS, will create such a barrier to innovation and technology in the workplace that many employers will avoid the adoption of new technology altogether to limit liability. The categories that serve as bases for challenging an AIA are incredibly overbroad, allowing a challenge for whether the AIA was incomplete or inaccurate, whether it failed to balance harms and benefits of ADS (which isn't required in an AIA), and any other reason the AIA was defective or incomplete. This is ripe for abuse. It is one thing to protect a worker from retaliation for reporting issues with the implementation of an ADS or AIA. It is another to allow anonymous reporting with no way to verify whether the person has any evidence or is even an employee. It is easy to imagine corporate rivals or a worker with a grudge abusing this dispute process.

Lastly, prior to an employer or vendor using an ADS or productivity system, they must submit a summary to the labor agency and Cal/OSHA for approval. To the extent that these impact assessments have to be filed with the State of California, it would likely open the door for further audit and legal claims.

The Labor and Workforce Development Agency Should Not Be Required To Review All New Technologies

We also question whether the labor agency is the proper state agency to consider new and developing technologies, which seem to be outside of their jurisdiction and expertise. This bill grants the agency broad discretion without justification. The agency is tasked with reviewing AIAs and all electronic monitoring mechanisms and can require employers to submit additional documentation, require specific mitigation measures, and even prohibit an employer from using an ADS. Proponents have argued that this bill bans very little technology; in reality, this chapter seems to give the labor agency the authority to ban any workplace technology.

Even if the Labor Commissioner and Cal/OSHA were the proper state agency, this sweeping authority is an overreach and would set business back decades. Because these assessments have to be completed for new and existing technologies, the definitions of ADS, electronic monitoring, and other terms are overbroad, and it applies to employers of all sizes, this bill enacts significant barriers to technology in the workplace. There are many applications of technology in the workplace that benefit workers, employers, and the public. However, the costs and burdens of completing an AIA for each use of technology, not to mention the significant litigation risk discussed elsewhere, will mean employers will limit how many systems and technology they implement. This bill will not only inhibit the efficiency and value of businesses but will inevitably lead to less safe, less secure, and more frustrating workplaces, as workers will have fewer safeguards and more redundant administrative work.

AB 1651 is Drowning in Disclosure Notices and Reporting Requirements That are Duplicative, Confusing, and Unproductive

AB 1651 contains upwards of 20 or more disclosure notices or reporting requirements. Proposed Section 1540 includes a notice requirement that has no less than 14 parts relating to electronic monitoring. While this is just one of the many different notice requirements in the bill, it is helpful in illustrating how the bill undermines the actual function and utility of worker notices by overwhelming employees with too much information, and even irrelevant or unnecessary information.

For example, the electronic monitoring notice mandated by proposed Section 1540 must include not only include a description of the specific activities, locations, communications, and job roles that will be electronically monitored, but it must also include the names of any vendors conducting electronic monitoring on the employer's behalf and associated contract language related to that monitoring. The former is information that an average worker would likely find informative, but the latter buries workers in contractual legalese having arguably little value to the worker. (*See* paragraphs (2) and (6) of proposed section 1540.) At the same time, in yet another paragraph of this same notice, the bill requires that the employer provide a description of a vendor or "third party" (which, again, excludes unions) to whom information collected through electronic monitoring will be disclosed or transferred. In doing so it, for the second time in this exact same notice, requires the employer to include the name of the vendor and the purpose of the data transfer. (*See* paragraph (7).)

Rather inexplicably, this notice provision also requires the employer to provide two explanations of the specific authorization for electronic monitoring under two separate statutes, one of which has nothing to do with regulating electronic monitoring but rather has to do with permissible uses of ADS to make employment-related decisions.[2]

All of this is to say, information that would be most pertinent to the user eventually gets lost in the shuffle of over-disclosures and the business is more likely to make inadvertent errors that will land them in costly litigation, which most small businesses would not be able to survive given the aggressive penalties.

AB 1651's Staggering Enforcement Mechanisms and Mandatory Penalties Will be Crippling for Many Businesses

AB 1651's mandatory penalties and enforcement mechanisms are astounding. When the CCPA was drafted, its enforcement was limited in scope given the magnitude of the endeavor and the general understanding that such an undertaking, especially one that will take significant efforts to comply with and may require revisions to existing technology systems, is bound to involve implementation issues. Rather than take that same approach, **AB 1651'**s enforcement chapter is excessively punitive.

The bill provides for a private right of action with penalties ranging between $2,500 and $20,000 per violation. There is no willfulness requirement, so a good faith error subjects a company to the same penalty. "Violation" is not defined, which will surely result in plaintiff's attorneys arguing for the most expansive definition possible in each case, whether that is per employee or per piece of worker data. Those fines apply regardless of business size, so one lawsuit under this Act would easily wipe out a small business.

Because **AB 1651** creates new provisions in the Labor Code, it also falls under the Private Attorneys General Act (PAGA). PAGA allows one worker to sue on behalf of all of a business's workers in California without satisfying class action requirements or demonstrating actual harm. The worker can sue for any violation of the Labor Code as long as they allege they experienced one violation, can forum shop, and can settle their own claims while still acting as the PAGA plaintiff. PAGA is utilized against employers as financial leverage to force employers into costly settlements for minor, innocent mistakes. This Act is a prime candidate for PAGA because, as explained above, it sets employers up to fail through its barrage of notice requirements (most of which also include subparts), overly broad terms, and unrealistic mandates.

[2] Compare paragraph (11), requiring an explanation of why the specific form of electronic monitoring is strictly necessary to accomplish an allowable purpose described in Section 1543 regulating the permissible purposes for electronic monitoring, to paragraph (1), requiring a description "of the allowable purpose that the specific form of electronic monitoring is intended to accomplish" pursuant to a section 1553, under the chapter regulating algorithms.

AB 1651's Data Security Provisions are Unnecessary and Do More Harm Than Good

AB 1651 contains various provisions with implications on data security, and the ability of companies to adequately protect data of their business, including worker data. As noted above, biometric data has significant beneficial uses both for employers, workers, and the broader public, particularly in terms of fraud prevention and security related purposes. From securing workplaces or rooms with sensitive data to authorized personnel, to facilitating background checks for potential employees or contractors, and from ensuring accurate time clocks to providing stronger authentication tools to prevent unauthorized access to servers, files, systems, and more–collecting biometric data is not only *not* inherently nefarious, but it serves to protect against nefarious actors. This bill's definitions and overly restrictive prohibitions fail to recognize the beneficial purposes of this data and promote public policy that would, in reality, create more harm than good for businesses and workers alike.

Separately, proposed Section 1534 in the bill requires an employer that collects, stores, analyzes, interprets, disseminates, or otherwise uses worker data to undertake "its best efforts" to implement, maintain, and keep up-to-date security protections that are appropriate to the nature of the data, and to protect the data from unauthorized access, destruction, use, modification, or disclosure. The security program must include administrative, technical, and physical safeguards. In the event that an employer becomes aware of a breach of worker data, they must promptly provide written notice to each affected worker. The bill requires that the notice be made in the "most expedient time possible" and must include a description of the specific categories of data that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person, and what steps it will take to address the impact of the data breach on affected workers. Additionally, the bill requires that the employer promptly notify the labor agency in writing of such a breach.

First, it is unclear what meets the standard of "best efforts" or what would constitute "unauthorized access" under this bill. Second, this is both vague and wholly unnecessary without additional definitions and given existing data privacy laws. California's existing Customer Records Act already requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. (*See* Civ. Code Sec. 1798.81.5.) Furthermore, under the existing breach notification law (DBNL), any person or business that conducts business in California that owns or licenses computerized data with personal information to disclose any breach of the security of the system to California's residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Additionally, any time a single breach affects more than 500 California residents, an electronic sample copy of that notification must be provided to the Attorney General (AG). (*See* Civ. Code Sec. 1798.82.)

Of these issues, most problematic is that an "unauthorized access" would seemingly constitute a data breach for purposes of **AB 1651,** which we believe would do more harm than good. Unlike the CPRA, the bill fails to recognize that "unauthorized access" itself is not enough to constitute an actionable data breach, unless there is <u>also</u> some form of exfiltration, theft or disclosure that results from the business's duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information. (*See* Civ. Code Sec. 1798.150.) Meaning, under the CPRA, if an employee inadvertently accessed a file for the wrong "J. Smith", it would not be a "data breach" if the employee recognized the error and immediately closed out of the file. As a matter of public policy, this strikes a much more appropriate balance because no actual harm will have resulted to the worker whose file was inadvertently accessed. In contrast, under **AB 1651**, that same activity could be considered a breach. This would trigger a slew of potential data breach notifications with the possibility that no data was exfiltrated, stolen, compromised, or even disclosed. When the CPRA's predecessor, the CCPA, was being considered in the Legislature, there was a significant amount of time spent deliberating on what would constitute a data breach, as a result of which this body determined that *access* alone would not constitute a data security breach notification but, rather, that *access* **and** *exfiltration, theft, or disclosure* was necessary. The importance of this additional qualifier ensures that notifications occur only once data is determined to have been exposed to a cybersecurity threat. Notably, employees already can bring a private right of action under the CPRA for data breaches, rendering these provisions completely unnecessary.

AB 1651's Vendor Regulations are Unclear and Unfounded

AB 1651 extends to an employer's vendor (an entity engaged by the employer the employer's labor contractors to provide software, technology, or related service used to collect, store, analyze or interpret worker data) various notice and disclosure requirements as well as limitations upon electronic monitoring and the ability to transfer, disclose, collect, store, analyze or interpret worker data. It also holds the employer jointly and severally liable for failure of the vendor to comply with the requirements of the bill. (*See* proposed sections 1535, 1545, 1555, and 1564). Problematically, the bill requires a vendor, upon termination of a contract with the employer, to return all worker data to the employer and to delete the worker data. At minimum, the obligations should be clarified as it is not clear how a vendor can simultaneously delete data (and potentially evidence) and return the data to the employer at the same time.

More broadly, by applying to vendors, this bill will impede the creation and adoption of technology in the workplace. It will impact not only current products and features created by California companies, but also affect many that are currently in development. As noted elsewhere, there are many applications of technology in the workplace that benefit workers, employers, and the public. However, this bill takes a Luddite view on technology, assuming every application or use is nefarious and harmful.

AB 1651's Overly Broad and Vague Definitions Exacerbate Unintended Consequences and Undermine Worker Privacy Rights

The many definitions in **AB 1651** are overbroad and vague, resulting in the bill's provisions being over-reaching with troublesome unintended consequences. Some even undermine workers privacy rights. Several examples include:

- "Automated Decision System (ADS)" or "algorithm": By defining ADS as any computational process that "makes or assists an employment-related decision" this bill will apply to an immense number of software, programs, and applications. This includes something as simple as a spreadsheet an employer uses to track sales or other business functions, scheduling software, payroll systems, project management systems, messaging applications, inventory trackers, and automated workplace climate controls.

- "Automated Decision System (ADS) output": The application to "any information" and not just a recommendation or decision means that in Chapter Five employers have to hire an independent assessor to monitor the calculations a spreadsheet or computing software makes, which is a waste of time, resources, and undercuts the value of the automated system.

- "Biometric data". This definition tracks the voter approved California Privacy Rights Act (CPRA) definition from 2020 in all but one pivotal way: **AB 1651** includes an individual's physiological, biological, or behavioral characteristic that *can be used* (as opposed to "is used or is intended to be used") to establish individual identity. Meaning, if the business deidentifies this information or keeps it in aggregate form, it is not identifiable information and should not be treated as such, even if the information, *theoretically*, could potentially be reidentified or disaggregated with significant efforts. This only amplifies the unintended harms caused by such a broad ban on the transfer or disclosure of this information, as discussed above.

- "Data" or "Worker Data": This includes any information that relates to or could reasonably be linked (directly or indirectly) to a worker including any document, email, text message, or other writing the employee ever creates, any document on which their name appears (such as payroll or an employee roster), as well as all physical documents in the employee's office. It also includes HR information, such as performance evaluations, data collected or generated to mitigate the spread of infectious diseases such as COVID-19 or to comply with public health measures, and data that includes customer interaction and ratings. Such "worker data" would be subject to a right of correction, easily leading to scenarios wherein an employee seeks to "correct" their poor performance evaluation or customer ratings.

- "Electronic monitoring". This broad definition includes collection of information concerning worker activities and communications by any means other than direct observation, including the use of a computer, telephone, wire, radio, camera, electromagnetic, photoelectronic, or photo-optical system. As a result, the bill captures standard cybersecurity tools that companies use to prevent security breaches and data loss, and to protect both the business's own confidential data, as well as the personal data of their employees and customers. This hampers critical efforts to protect both personal and confidential data from malicious actors and results in *less* protection of employee data.

- "Essential Job Functions": This is a vague, subjective standard. It is not uncommon for employees' job duties to evolve and change day to day depending on circumstances. Indeed, this term is consistently litigated over in reasonable accommodation litigation under the Fair Employment and Housing Act (FEHA). As explained above, its use in this bill creates an impossible standard for employers to follow. Additionally, its use throughout the bill results in unnecessarily narrow circumstances under which certain data can be collected, when monitoring can occur, and when ADS can be used.

- "Third party": This definition, understandably, excludes the employer and a vendor or service provider to the employer, such as those providing health care coverage, or payroll services. Rather inexplicably, however, it also exempts a labor or employee organization within the meaning of state or federal law. Such a blanket exemption for the sponsors of this legislation from privacy law protections, such as the proposed limitations placed on transferring data to third parties by this bill, is inconsistent with and undermines worker privacy and control over their own data. Another concern is that it would *include* legal counsel or a CPA. Its use in the bill would therefore require disclosure of when certain information is sent to those entities, which will likely compromise ongoing legal actions and is likely to result in divulgence of privileged, confidential, or proprietary information.

- "Worker": This definition includes an "authorized representative". As explained in more detail above, this means an attorney or union has the same rights under **AB 1651** as a worker, and that worker data provided to a union or the plaintiff's attorney is not subject to the same restrictions or disclosures as worker data provided to anyone else. The definition may also be too broad in attempting to go beyond employees and further cover independent contractors, job applicants, and subcontractors.

- "Worker Information System (WIS)". This definition encompasses any process that involves worker data--whether it is automated or not. Collection, recording, organization, structuring, storage, and disclosure of worker data, among other things, all constitute a process that involves worker data. Effectively, everything would be a WIS. For example, it would include the employer's email system (even when there is no "behind the scenes" monitoring by the employer), as well as any spreadsheet or software in which the employer makes weekly inputs. The inclusion of non-automated services also means pen and paper systems.

As described in more detail above, these problematic definitions make the scope of the bill untenable and lead to outcomes that contravene the bill's intent and sound public policy.

For these reasons, we respectfully oppose **AB 1651 (Kalra)** as a **JOB KILLER**.

Sincerely,

Ronak Daylami
Policy Advocate
California Chamber of Commerce
on behalf of

Ashley Hoffman
Policy Advocate
California Chamber of Commerce
on behalf of

American Association of Advertising Agencies (4A's)
American Property Casualty Insurance Association
American Staffing Association
Association of California Healthcare Districts
Association of California Life and Health Insurance Companies
Association of Claims Professionals
Association of National Advertisers
Auto Care Association
California Association of Collectors, Inc.
California Association of Joint Powers Authorities
California Association of Winegrape Growers
California Attractions and Parks Association
California Bankers Association
California Business and Industrial Alliance
California Business Properties Association
California Business Roundtable
California Chamber of Commerce
California Credit Union League
California Employment Law Council
California Grocers Association
California Hospital Association
California Hotel & Lodging Association
California Land Title Association
California New Car Dealers Association
California Retailers Association
California Special Districts Association
California State Association of Counties
California Trucking Association
CAWA, Representing the Automotive Parts Industry
Chino Valley Chamber of Commerce
Chubb
Civil Justice Association of California
Consumer Data Industry Association
Electronic Transactions Association
Family Business Association of California
Housing Contractors of California
Insights Association
National Association of Mutual Insurance Companies
National Federation of Independent Business
National Payroll Reporting Consortium
Oceanside Chamber of Commerce
Official Police Garages of Los Angeles
Pacific Association of Domestic Insurance Companies
Professional Background Screening Association
Public Risk Innovation, Solutions, and Management
Santa Maria Valley Chamber of Commerce
Silicon Valley Leadership Group
TechNet
The Doctors Company
Western Electrical Contractors Association, Inc.

cc: Legislative Affairs, Office of the Governor
Megan Lane, Office of Assemblymember Kalra
Nichole Rapier Rocha, Assembly Privacy and Consumer Protection Committee
Elizabeth Enea, Consultant, Senate Republican Caucus