Insights, News & Events

THE 3 BIGGEST CONCERNS FOR CALIFORNIA EMPLOYERS ABOUT SWEEPING EMPLOYEE SURVEILLANCE BILL

Insights
Mar 3, 2025

California employers should be paying close attention to a pending bill that would significantly restrict how employers use workplace surveillance tools. If enacted, AB 1331 would prohibit employers from using workplace surveillance tools to monitor workers in "private, off-duty areas" including breakrooms, cafeterias, and lounges – as well as a worker's residence, personal vehicle, or property (unless "strictly necessary"). One of the most controversial parts of AB 1331 would be its requirement for employer to disable workplace surveillance tools during off-duty hours, including rest and break periods, notwithstanding any cybersecurity concerns or the fact that rest breaks for non-exempt employees are paid so employees typically are not clocking out for such breaks. The bill makes no distinction between exempt and non-exempt employees, or those in management or executive positions. Even worse is that this bill would deprive all employees of any right or choice to consent to surveillance. What do employers need to know about this pending bill, and what are the three biggest concerns you should have about this proposal?

Quick Background on Bill

AB 1331 represents a significant departure compared to the way other states are approaching the current trend of workplace surveillance. New York, Connecticut, and Delaware, for example, have employee surveillance laws that only mandate transparency and disclosure. While they require private employers to notify employees about monitoring and also require employers to obtain an

Related People

Risa B. Boerner, CIPP/US, CIPM

Partner

610.230.2132

Usama Kahf, CIPP/US

Partner

949.798.2118

acknowledgement from employees confirming their understanding of the company's practices, such surveillance is not outright prohibited.

AB 1331 goes beyond the traditional notice and consent model by directly restricting the use of monitoring technology. Notably, the bill does not include exceptions for situations where employees are notified or have provided consent. As a result, employers would be required to disable critical security and compliance tools during certain times and in specific locations that exceed those in which employees have traditionally been considered to have a reasonable expectation of privacy — a requirement that no other state law currently imposes.

3 Biggest Concerns

This significant departure from existing frameworks presents several challenges for California employers. Here are the three biggest concerns employers should keep in mind if AB 1331 is enacted:

1. AB 1331's Overbroad and Overinclusive Scope Would Create Major Compliance Headaches for Employers

AB 1331 would impose blanket prohibitions that will be difficult – if not impossible – for many employers to comply with. "Workplace surveillance tools" are defined in the bill as "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, by means other than direct observation by a person." This definition is so broad that it would encompass all:

- Video and audio surveillance
- Electronic work tracking systems
- Geolocation monitoring
- Biometric scanning
- Cybersecurity and IT security tools

This goes beyond tools that are specifically made and used for monitoring, surveillance, and tracking to cover any hardware or software that collects data about an employee. Sweeping in critical cybersecurity tools should be troubling,

Chelsea Viola
Associate
213.403.9626

Service Focus

Consumer Privacy Team

Privacy and Cyber

Resource Hubs

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills

as the bill would prohibit use of such tools in all areas deemed to be "private" (which is itself broader than what the law had previously considered to be private areas in the workplace) and during off-duty hours without exception for cybersecurity needs or considerations. Only the part of the bill that would prohibit the monitoring of a worker's residence, personal vehicle, or property owned, leased, or used by a worker includes a single exception for where the monitoring is "strictly necessary," which is an undefined standard that is likely to lead to litigation.

The bill would also require employers to disable surveillance tools during rest and break periods, which poses a significant logistical problem. Unlike meal breaks, rest breaks in California are paid – meaning non-exempt employees remain on the clock and do not clock out. Existing law also only requires employers to "authorize and permit" non-exempt employees to take rest breaks within certain frequencies depending on the length of their shift, but the law does not require employers to actually police the taking of rest breaks and to require employees to take their rest breaks. As a result, many employers give non-exempt employees discretion to decide when to take their rest breaks and do not have a way of knowing or being alerted to when an employee is on their rest break. This makes it unclear how employers could feasibly comply with a requirement to suspend all monitoring during those periods.

For example, would employers need to disable GPS tracking on a company vehicle every time a driver takes a 10-minute break? Should you stop cybersecurity monitoring when a remote worker steps away from their laptop? The bill provides no clear guidance on whether and how its restrictions would apply to remote workers, leaving employers to navigate a complex and potentially impractical compliance landscape — a burden that becomes even heavier for larger companies managing numerous systems and worksites.

Additionally, the bill makes no distinction between exempt and non-exempt employees, and in the context of exempt employees, such as members of management or those exempt under the administrative, professional, or computer professional exemptions, there will be confusion over when such employees are "off duty" or on "breaks."

2. Limiting Surveillance Could Undermine Workplace Safety and Anti-Harassment Efforts

AB 1331 would prohibit employers from monitoring breakrooms, employee lounges, and cafeterias – areas where surveillance is often used to ensure workplace safety and prevent misconduct. These areas have never previously been deemed by law to be "private" areas akin to restrooms, locker rooms, and changing rooms where employees have a reasonable expectation of privacy. The bill would expand what is considered private beyond an individual's personal space where they would engage in personal activities to areas where workers congregate or interact with each other whether they are on break or not. This restriction could have unintended consequences, such as:

- ***Hindering investigations into workplace harassment or discrimination***. Without surveillance footage, employers may struggle to respond to complaints of inappropriate conduct that occur in these shared spaces.
- ***Reducing security measures in high-traffic areas***. Many employers use surveillance to prevent theft, workplace violence, or unauthorized access to restricted areas.
- ***Creating conflicts with federal and state anti-harassment obligations.*** Employers have a duty to maintain a safe, harassment-free workplace under Title VII of the Civil Rights Act and California's Fair Employment and Housing Act (FEHA), among other laws. If surveillance tools are restricted in break areas, employers may face greater challenges in enforcing these obligations.

Courts have generally upheld the use of security cameras in common areas in workplaces, recognizing that employees do not have a reasonable expectation of privacy in areas like breakrooms or cafeterias. AB 1331's restrictions would therefore go beyond established legal norms, making it harder for employers to maintain a safe and compliant workplace.

3. AB 1331 Conflicts with Legitimate Business Needs such as Cybersecurity, Remote Work Supervision, and Safeguarding Employer Property

Employers rely on surveillance and monitoring tools for a variety of legitimate business purposes, many of which would be disrupted by AB 1331. The bill's broad language would interfere with:

- ***Tracking company vehicles.*** Many businesses use GPS monitoring to ensure that company vehicles are being used appropriately and safely.
- ***Managing remote employees.*** Electronic monitoring tools help employers ensure that remote employees are working during scheduled hours, prevent unauthorized data access, and maintain cybersecurity.
- ***Protecting trade secrets and confidential information.*** Employers use IT security tools to monitor for suspicious activity, prevent insider threats, and detect potential data breaches. This risk is heightened when employees use personal devices to access employer systems, applications, and networks. The bill would prohibit the monitoring of such personal devices when they are interacting with the employer's systems unless such monitoring is strictly necessary. But even if the monitoring is strictly necessary, it would still be prohibited under this bill without exception for cybersecurity if the employee is "off duty" or on a "break" regardless of whether the employer has any way of knowing when the employee is off duty or on break and regardless of whether the employee is exempt or non-exempt.

The bill provides no carve-out for cybersecurity protections, meaning companies could be at greater risk of cyberattacks or insider threats if required to suspend monitoring at certain times. This could be particularly problematic for industries that handle sensitive customer data, financial information, or proprietary business information.

What Employers Should Do Now

AB 1331 has only just been introduced in the legislature. It will likely be heard in policy committee in late March or early April. While there is never a guarantee that legislation will be enacted into law, AB 1331 has the strong backing of organized labor, increasing the chances of the bill making it to the Governor's desk by September.

And AB 1331 would come with significant risk for violations, carrying penalties of $500 per employee, per violation – an amount that could quickly stack up for larger employers. Under this law, employees could also sue for damages and enforcement actions could be brought by the Attorney General, district attorneys, or city attorneys. This means it is

crucial for California employers to consider the following steps:

1. ***Monitor the bill's progress.*** Given its far-reaching implications, AB 1331 is worth tracking closely as it moves through the legislative process.

2. ***Review current employee monitoring policies.*** You should assess how you currently use surveillance tools and whether they would be impacted by the bill's prohibitions, preparing for potential revision as necessary.

3. ***Join industry advocacy efforts.*** Given the bill's broad reach and potential conflicts, you should consider participating in opportunities to explain its real-world impact to lawmakers and advocate for clearer, more practical legislation.

Conclusion

AB 1331 represents a significant departure from existing employee monitoring laws in other states. The bill's broad scope, operational hurdles, and potential clashes with existing legal requirements make it a key issue for employers to closely monitor in the coming months.

Given the bill's sweeping scope, its passage could fundamentally reshape workplace surveillance practices across California. Fisher Phillips will continue to track developments and provide timely updates. To stay informed, subscribe to our Insight System, and for further guidance, contact your Fisher Phillips attorney, the authors of this Insight, or any member of the firm's Consumer Privacy Team.