

---

## OLR Bill Analysis

### sSB 1484

#### ***AN ACT IMPLEMENTING ARTIFICIAL INTELLIGENCE PROTECTIONS FOR EMPLOYEES.***

#### **SUMMARY**

This bill generally expands the current law on employer use of electronic monitoring and surveillance, and sets new limits on an employer's use of high-risk artificial intelligence (AI) systems to make consequential decisions about employees.

It broadens the current electronic monitoring and surveillance laws to, among other things:

1. specify when employer electronic monitoring is allowed (e.g., to ensure the quality of goods and services or protect the employer's facilities) and prohibited (e.g., to get employee medical history or biometric information);
2. cover an employer getting employee data from a third party; and
3. expand the information that must be included on employer notices about the monitoring.

The bill also limits an employer's use of high-risk AI systems to make consequential decisions (e.g., decisions that could impact an employee's hiring, termination, or compensation). Among other things, these provisions:

1. require employers to (a) have an impact assessment of the system before deploying it and (b) give employees certain information about the system and its use and
2. allow employees to (a) appeal decisions made by the system under certain circumstances, and (b) bring a lawsuit for violations of these provisions.

The bill also prohibits state agencies from using high-risk AI systems without specific authorization in law for a function that (1) is related to delivering public assistance benefits or (2) will impact people's rights, safety, or welfare. It prohibits state agencies from acquiring a high-risk AI system without specific authorization in law and requires an impact assessment for those that are acquired.

Lastly, for state and municipal employees, the bill explicitly makes an employer's use of AI systems a mandatory subject of collective bargaining (§§ 7 & 8).

EFFECTIVE DATE: October 1, 2025

## **ELECTRONIC MONITORING AND SURVEILLANCE**

### ***Electronic Monitoring (§ 1)***

The state's electronic monitoring law generally requires employers, including the state and its political subdivisions, to notify employees who may be subject to electronic monitoring. Under current law, "electronic monitoring" is collecting information on the employer's premises about employee activities or communications by any means other than direct observation (e.g., by computer, camera, or photo-optical systems). The bill expands the covered electronic monitoring to also include getting employee data from a third party. As under current law, it does not include collecting information (1) for security purposes on the employer's public premises or (2) that is prohibited by law.

The bill also prohibits employers who use electronic monitoring from selling, transferring, or disclosing employee information collected through electronic monitoring, unless they must do so to comply with a state or federal law, or an AI impact assessment (see § 3).

***Prohibited Monitoring.*** The bill also prohibits employers from using electronic monitoring to do the following:

1. threaten the health, safety, and welfare of employees or the general public;
2. monitor employees who are not doing work-related tasks;

3. get information about an employee's (a) medical history; (b) biometric information consisting of data generated by electronic measurements of an employee's unique physical characteristics used to authenticate the employee's identity, such as a fingerprint, voice print, or retina or iris image; or (c) race, religion, national origin, sex, gender identity, sexual orientation, genetic information, ancestry, or status as a veteran or member of any class protected under the state anti-discrimination laws; or
4. punish employees for activities protected by state or federal law.

It also prohibits employers from requiring employees to wear a monitoring device or install an application for location tracking on their personal device.

***Allowed Monitoring.*** The bill allows employers to use electronic monitoring only to do the following:

1. ensure the quality of good and services;
2. periodically assess employee performance;
3. ensure compliance with state or federal law;
4. protect employees' health, safety, and welfare;
5. protect the employer's facilities or computer networks; or
6. administer wages and benefits.

Under the bill, an employer who engages in these types of electronic monitoring must (1) narrowly tailor them to accomplish the intended purpose in a way that is least invasive to employees and (2) maintain reasonable data security practices to protect confidentiality of employees' information and limit access to it.

***Expanded Notice.*** The bill also expands the information required in the prior written notice about electronic monitoring that employers must give their employees. Current law requires this notice to inform potentially affected employees about the types of monitoring that may

occur. The bill also requires it to inform them about the intended use of any information collected by the monitoring, how it will be collected and stored, and for how long. It must also state the employee's rights under the law and be provided in plain language, English, and the employee's primary language.

Current law allows employers to meet the prior written notice requirement by posting the notice conspicuously in a readily available place. The bill instead requires employers to meet the notice requirement by giving the prior written notice to each employee and meeting this posting requirement.

***Enforcement.*** As under current law, the labor commissioner may levy civil penalties on employers who violate the electronic monitoring law, with penalties of up to \$500 for a first offense, up to \$1,000 for a second offense, and up to \$3,000 for a third or subsequent offense.

### ***Electronic Surveillance (§ 2)***

Current law generally prohibits employers from using an electronic surveillance device or system (e.g., audio recordings, closed circuit TV) to record or monitor employee activities in areas designed for employees' health or personal comfort, or for safely keeping their possessions (e.g., rest rooms, locker rooms, lounges). The bill expands this prohibition to also cover any property owned or leased by an employee, such as the employee's residence or vehicle.

## **§§ 3-5 — AI USE IN EMPLOYMENT**

The bill generally requires employers using a high-risk AI system to make consequential decisions to (1) have an impact assessment of it completed by an impartial third party, (2) meet certain notice requirements, and (3) have human oversight over the system by designating an internal reviewer with certain expertise and authority. (It does not specify whether these provisions cover the state and other public employers.)

### ***Definitions (§ 3)***

Under the bill, an "artificial intelligence system" is a machine-based

system that, for any explicit or implicit objective, infers from the inputs it receives how to generate outputs such as content, decisions, predictions, or recommendations that can influence physical or virtual environments.

A “high-risk” AI system is an AI system that makes, or is a substantial factor in making, a consequential decision. It does not include an AI system meant to do a narrow procedural task or detect decision making patterns, or deviations from them, unless it is meant to replace or influence an assessment previously done by a human without sufficient human review. Unless it makes, or is a substantial factor in making, a consequential decision, a high-risk AI system also excludes:

1. anti-fraud technology that does not use facial recognition technology;
2. AI-enabled video game technology;
3. anti-malware, anti-virus, calculator, cybersecurity, database, data storage, firewall, Internet domain registration, Internet-web-site loading, networking, robocall-filtering, spam-filtering, spellchecking, spreadsheet, web-caching, web-hosting, or similar technology;
4. technology that performs tasks exclusively related to an entity’s internal management affairs, such as ordering office supplies or processing payments; or
5. technology that (a) communicates with consumers in natural language to give users information, make referrals or recommendations, and answer questions, and (b) is subject to an accepted use policy that prohibits generating discriminatory or harmful content.

A “consequential decision” is a decision or judgment that has a legal, material, or similarly significant effect on an individual’s:

1. employment, such as decisions or judgments made (a) about hiring, termination, compensation, promotion, hours, duties,

productivity requirements, workplace health and safety, or other conditions of employment or (b) through an automated task allocation that limits, segregates, or classifies employees for assigning or determining material terms or conditions of employment;

2. education or vocational training, such as decisions or judgments made on assessments, student cheating or plagiarism detection, accreditation, certification, admissions, or financial aid or scholarships;
3. provision or denial, or terms and conditions, of (a) financial lending or credit services; (b) housing or lodging, including rentals or short-term housing or lodging; (c) insurance; or (d) legal services; or
4. provision or denial of essential government services or health care services.

A “substantial factor” in a consequential decision is an AI-generated factor that alters the decision’s outcome. It can include using AI to generate content, decisions, predictions, or recommendations about someone that are used to make a consequential decision about him or her. It does not include AI output when an individual was involved in the data processing that produced the output and that person (1) meaningfully considered the data as part of the data processing and (2) was authorized to change or influence the output produced by the data processing.

### ***Impact Assessment (§ 3)***

The bill requires employers, before deploying a high-risk AI system, to have an impact assessment of it completed by an impartial third party at least one year before deploying it (or by October 1, 2026, if it deployed before October 1, 2025). The assessment must at least include the following information about the system, to the extent known by, or available to, the employer or contracted third party:

1. a statement about its intended purpose and use cases,

deployment context, and benefits;

2. any metrics used to evaluate its performance and known limitations; and
3. analyses of its (a) error rates, (b) known or reasonably foreseeable risks of algorithmic discrimination, (c) accessibility, (d) potential impacts on employees' rights under any state or federal law, and (e) negative impacts on employees' job quality or well-being.

Under the bill, "algorithmic discrimination" is any condition in which using an AI system results in an unlawful differential treatment or impact that disfavors an individual or group of individuals based on their actual or perceived age, color, disability, ethnicity, genetic information, limited proficiency in the English language, national origin, race, religion, reproductive health, sex, gender identity, veteran status, or other classification protected under state or federal laws. It does not include:

1. a developer or deployer's offer, license, or use of a high-risk AI solely for (a) self-testing to identify, mitigate, or prevent discrimination or otherwise ensure compliance with state and federal law or (b) expanding an applicant, customer, or participant pool to increase diversity or redress historic discrimination or
2. an act of omission by, or on behalf of, a private club or other establishment not in fact open to the public under Title II of the federal Civil Rights Act (i.e. exempt from the act's equal access requirements for public accommodations).

### ***Notice Requirements (§3)***

Starting October 1, 2026, the bill requires employers to notify an employee before using a high-risk AI system to make, or be a substantial factor in making, a consequential decision about the employee. The employer must give the employee the following:

1. a statement disclosing the system's purpose and the nature of the

consequential decision;

2. what, if any, employee data the system will collect;
3. the results of the most recent impact assessment;
4. the right to opt out of any automated decision-making based on the employee's personal data and information on how the employee may request an alternative decision-making process;
5. information on how the employee may request a reevaluation of any consequential decision the system makes in whole or in part (see below); and
6. a plain language description of the system.

In addition, starting on October 1, 2026, if the employer's use of a high-risk AI system makes, or is a substantial factor in making, a consequential decision that is adverse to an employee, the employer must give the employee:

1. a statement disclosing the main reason or reasons for the decision, including (a) how the system contributed to the decision, (b) the type of data it processed in making the decision, and (c) the data's source, and
2. an opportunity to (a) examine the personal data the system processed in making, or used as a substantial factor in making, the decision; (b) correct any incorrect personal data; and (c) appeal the decision if it is based upon inaccurate personal data, considering both the data's nature and why it was processed.

The appeal must allow for human review.

The bill requires employers to give these notices, statements, information, descriptions, and instructions (1) directly to employees; (2) in plain language; (3) in all languages that the employer, in its ordinary course of business, uses in contracts, disclaimers, sale announcements, and other information for consumers; and (4) in a format accessible to



employees with disabilities.

### ***Human Oversight (§ 3)***

Starting October 1, 2026, the bill requires an employer using a high-risk AI system to make, or be a substantial factor in making, a consequential decision about an employee to implement human oversight over the system by designating at least one internal reviewer who has expertise in operating the system. The internal reviewer must be (1) familiar with the system's most recent impact assessment and the data processing that produced the system's output, (2) authorized to change or influence the system's output, and (3) given the time and resources to evaluate the system's outputs.

Under the bill, the internal reviewer must verify the accuracy of employee data input into the system, such as performance evaluations, employee work product, personnel files, and peer reviews, and consider the system's output.

### ***Job Protections for Certain Employees (§ 4)***

The bill prohibits employers from discharging, retaliating, or discriminating, or taking any adverse action against certain employees for refusing to follow a consequential decision output made by a high-risk AI system. More specifically the prohibition applies to employees who (1) hold independent judgment and discretion in doing their work under a license or certification required by the state as a condition of employment for their position, (2) reasonably believed that the output may cause algorithmic discrimination and notified the employer about it, and (3) reasonably believed that there was not enough time to correct the action before a consequential decision needed to be made.

### ***Lawsuits (§ 5)***

The bill allows an employee aggrieved by a violation of its provisions on AI use in employment (§§ 3 & 4) to bring a civil action in Superior Court to recover damages and equitable relief, plus costs and attorney's fees.

## **§ 6 — AI USE BY STATE AGENCIES**

The bill prohibits state agencies, or entities acting on their behalf, from using or applying, directly or indirectly, a high-risk AI system for any function that (1) is related to the agency's delivering public assistance benefits to people in the state or (2) will have a material impact on the rights, civil liberties, safety, or welfare of people in the state, unless the use or application is specifically authorized by law. (The bill does not define the "state agencies" subject to these provisions.)

The bill also prohibits state agencies from authorizing a procurement, purchase, or acquisition of a high-risk AI system that uses or relies on automated decision making systems, unless it is specifically authorized by law.

If the agency has this authorization, the bill requires it to contract with an impartial third party to complete an impact assessment as required by the bill (see § 3). Under the bill, the agency must submit the completed assessment to the administrative services commissioner, in a form and way she sets, and post it on the agency's website at least 60 days before deploying the system. The agency may redact the assessment to remove anyone's personally identifiable information.

### **BACKGROUND**

#### ***Related Bills***

sSB 2, favorably reported by the General Law Committee, establishes a framework for regulating AI and includes other AI-related provisions, such as those requiring (1) high-risk AI system developers to use reasonable care to protect consumers from risks of algorithmic discrimination and (2) state agencies to study how generative AI may be incorporated to improve efficiencies.

sSB 10 (File 419), § 5, favorably reported by the Insurance and Real Estate Committee, prohibits health carriers from using AI or algorithms in place of a clinical peer to evaluate the clinical appropriateness of an adverse determination.

SB 1248 (File 330), favorably reported by the General Law Committee,

requires various AI-related reviews, programs, and funds, including establishing an AI regulatory sandbox program. It also specifies that it is generally not a defense to any civil or administrative claim or action that an AI system committed or was used in furthering the act or omission the claim or action is based on.

### **COMMITTEE ACTION**

Labor and Public Employees Committee

Joint Favorable Substitute

Yea 9      Nay 4      (03/20/2025)