SENATE COMMITTEE ON APPROPRIATIONS
Senator Anna Caballero, Chair
2025 - 2026 Regular Session

SB 468 (Becker) - High-risk artificial intelligence systems: duty to protect personal information

Version: February 19, 2025
Urgency: No
Hearing Date: May 5, 2025

Policy Vote: JUD. 11 - 0
Mandate: No
Consultant: Liah Burnley

Bill Summary: SB 468 imposes a duty on businesses that deploy high-risk AI systems to protect personal information and maintain a comprehensive information security program.

Fiscal Impact:

- **Department of Justice (DOJ):** DOJ indicates annual costs (Unfair Competition Law Fund, General Fund) of $600 thousand or less to enforce compliance with this bill under the Unfair Competition Law. DOJ notes that implementation of this bill will be dependent upon the appropriation of funds. The DOJ will be unable to absorb the costs to comply with or implement the requirements of the bill within existing budgeted resources. The Consumer Protection Section (CPS) within the Public Rights Division anticipates increased workloads in enforcing SB 468 beginning on January 1, 2026, and ongoing. The workload includes investigating and prosecuting violations of not adhering to SB 468. The Section will require 1.0 Deputy Attorney General, 1.0 Legal Secretary and $150,000 in external consultants which will have an impact to the Unfair Competition Law Fund.

- **Trial Courts:** Unknown, potentially significant cost to the state funded trial court system (Trial Court Trust Fund, General Fund) to additional adjudicate civil actions brought under the Unfair Competition Law as a result of this bill. Expanding civil penalties and creating new causes of action could lead to lengthier and more complex court proceedings with attendant workload and resource costs to the court. The fiscal impact of this bill to the courts will depend on many unknown factors, including the number of cases filed and the factors unique to each case. An eight-hour court day costs approximately $10,500 in staff in workload. If court days exceed 10, costs to the trial courts could reach hundreds of thousands of dollars. In 2023–24, over 4.8 million cases were filed statewide in the superior courts. Filings increased over the past year, driven mostly by misdemeanors and infractions, and civil limited cases. The increase in filings from the previous year is greater than 5% for civil limited and unlimited, appellate division appeals, juvenile delinquency, misdemeanors and infractions, and probate. While the courts are not funded on a workload basis, an increase in workload could result in delayed court services and would put pressure on the General Fund to fund additional staff and resources and to increase the amount appropriated to backfill for trial court operations. The Governor's 2025-26 budget proposes a $40 million ongoing increase in discretionary funding from the General Fund to help pay for increased trial court operation costs

beginning in 2025-26.

- **California Privacy Protection Agency (CPPA):** The CPPA anticipates it will incur rulemaking costs (General Fund). CPPA notes that it expects these costs will be absorbable in the near term. However, the agency may require additional resources if recurring rulemaking is necessary to further clarify statutory requirements, or to amend existing requirements due to new or emerging technologies, business practices, or based on requests from agencies enforcing this bill.
- **State and Local Agencies:** Unknown, potentially significant, possibly reimbursable, ongoing costs (local funds, General Fund) to state and local agencies due to the requirements on deployers and developers in this bill. Notably, this bill applies to state and local agencies, as specified, and the businesses that they contract with. Any costs incurred by software developers could be passed on to agencies, should they become a deployer technology that uses AI. In the aggregate, ongoing costs may be in the millions of dollars.

Background: High-risk automated decision systems (ADS) powered by AI are being increasingly deployed in a multitude of contexts, including employment, housing, education, and health care. Major transparency and fairness concerns have been raised about the use of ADS to make consequential decisions, essentially determinations with significant legal or other material effect on people's lives. One particularly concerning aspect is the amount of consumers' personal information being handled by these systems that may not adequately be protected by existing cybersecurity laws and measures.

Proposed Law:

- Includes the following definitions:
    - "Artificial intelligence" has the same meaning as that term is defined in Section 11546.45.5 of the Government Code.
    - "Business" has the same meaning as that term is defined in Section 1798.140.
    - "Consumer" has the same meaning as that term is defined in Section 1798.140.
    - "Covered deployer" means a business that deploys a high-risk artificial intelligence system that processes personal information.
    - "Deploy" means to put into effect or commercialize.
    - "Deployer" means a person doing business in this state that deploys a high-risk artificial intelligence system.
    - "High-risk artificial intelligence system" has the same meaning as "high-risk automated decision system," as that term is defined in Section 11546.45.5 of the Government Code.

  - "Personal information" has the same meaning as that term is defined in Section 1798.140.

  - "Processes" or "processing" have the same meaning as "processing," as that term is defined in Section 1798.140.

- States that a covered deployer conducting business in this state shall have a duty to protect personal information held by the covered deployer.

- Requires a covered deployer whose high-risk artificial intelligence systems process personal information to develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate for all of the following:

  - The covered deployer's size, scope, and type of business.

  - The amount of resources available to the covered deployer.

  - The amount of data stored by the covered deployer.

  - The need for security and confidentiality of personal information stored by the covered deployer.

- States that the comprehensive information security program shall meet all of the following requirements:

  - The program shall incorporate safeguards that are consistent with the safeguards for the protection of personal information and information of a similar character under state or federal laws and regulations applicable to the covered deployer.

  - The program shall include the designation of one or more employees of the covered deployer to maintain the program.

  - The program shall require the identification and assessment of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any electronic, paper, or other record containing personal information, and the establishment of a process for evaluating and improving, as necessary, the effectiveness of the current safeguards for limiting those risks, including by all of the following:

    - Requiring ongoing employee and contractor education and training, including education and training for temporary employees and contractors of the covered deployer, on the proper use of security procedures and protocols and the importance of personal information security.

    - Mandating employee compliance with policies and procedures established under the program.

- Providing a means for detecting and preventing security system failures.

- The program shall include security policies for the covered deployer's employees relating to the storage, access, and transportation of records containing personal information outside of the covered deployer's physical business premises.

- The program shall provide disciplinary measures for violations of a policy or procedure established under the program.

- The program shall include measures for preventing a terminated employee from accessing records containing personal information.

- The program shall provide policies for the supervision of third-party service providers that include both of the following:

  - Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information consistent with applicable law.

  - Requiring third-party service providers by contract to implement and maintain appropriate security measures for personal information.

- The program shall provide reasonable restrictions on physical access to records containing personal information, including by requiring the records containing the data to be stored in a locked facility, storage area, or container.

- The program shall include regular monitoring to ensure that the program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information and, as necessary, upgrading information safeguards to limit the risk of unauthorized access to or unauthorized use of personal information.

- The program shall require the regular review of the scope of the program's security measures that must occur both annually and Whenever there is a material change in the covered deployer's business practices that may reasonably affect the security or integrity of records containing personal information.

- The program shall require the documentation of responsive actions taken in connection with any incident involving a breach of security, including a mandatory postincident review of each event and the actions taken, if any, in response to that event to make changes in business practices relating to protection of personal information.

- The program shall, to the extent feasible, include all of the following procedures and protocols with respect to computer system security requirements or procedures and protocols providing a higher degree of security, for the protection of personal information:

  - The use of secure user authentication protocols that include all of the control of user login credentials and other identifiers. The use of a reasonably secure method of assigning and selecting passwords or using unique identifier technologies, which may include biometrics or token devices. The control of data security passwords to ensure that the passwords are kept in a location and a format that do not compromise the security of the data the passwords protect.) The restriction of access to only active users and active user accounts. The blocking of access to user credentials or identification after multiple unsuccessful attempts to gain access.

  - The use of secure access control measures that include both of the following: The restriction of access to records and files containing personal information to only employees or contractors who need access to that personal information to perform the job duties of the employees or contractors. The assignment of a unique identification and a password to each employee or contractor with access to a computer containing personal information, that may not be a vendor-supplied default password, or the use of another protocol reasonably designed to maintain the integrity of the security of the access controls to personal information.

  - The encryption of both of the following: Transmitted records and files containing personal information that will travel across public networks. Data containing personal information that is transmitted wirelessly.

  - The use of reasonable monitoring of systems for unauthorized use of or access to personal information.

  - The encryption of all personal information stored on laptop computers or other portable devices.

  - For files containing personal information on a system that is connected to the internet, the use of reasonably current firewall protection and operating system security patches that are reasonably designed to maintain the integrity of the personal information.

  - The use of both of the following: A reasonably current version of system security agent software that shall include malware protection and reasonably current patches and virus definitions. A version of a system security agent software that is supportable with current patches and virus definitions, and is set to receive the most current security updates on a regular basis.

- Makes a violation of these provisions by a covered deployer a deceptive trade act or practice under the Unfair Competition Law.

- Authorizes the CPPA to adopt regulations implement and administer these provisions.

Related Legislation: This bill is one of a many of bills related to AI this Legislative Session:

- SB 53 (Weiner) establishes a consortium develop a framework for the creation of a public cloud computing cluster to advance the development of AI that is safe, ethical, equitable, and sustainable. SB 53 is pending on this Committee's suspense file.

- SB 366 (Smallwood Cuevas) creates a study evaluating the impact of AI on worker well-being. SB 366 is pending in the Senate Committee on Labor.

- SB 503 (Weber Pierson) requires developers of patient care decision support tools and health facilities to make reasonable efforts to identify uses of patient care decision support tools in health programs. SB 503 is pending in Senate Judiciary Committee.

- SB 524 (Arreguin) requires law enforcement agencies to note when they use AI on official reports. SB 524 is pending on this Committee's Suspense File.

- SB 579 (Padilla) establishes a mental health and AI working group. SB 579 is pending on this Committee's Suspense File.

- SB 813 (McNerney) establishes a process by which the Attorney General designates, a private entity as a multistakeholder regulatory organization if the entity ensures acceptable mitigation of risk from certified AI models. SB 813 is pending in the Senate Judiciary Committee.

- SB 833 (McNerney) requires a state agency in charge of critical infrastructure that deploys AI to establish a human oversight mechanism. SB 833 is pending in this Committee.

- AB 222 (Bauer-Kahan) requires reporting about energy use related to AI. AB 222 is pending in the Assembly Committee on Privacy and Consumer Protection.

- AB 316 (Krell) prohibits a defendant that used AI from asserting a defense that the AI autonomously caused the harm to the plaintiff. AB 316 is pending in the Assembly Committee on Privacy and Consumer Protection.

- AB 410 (Wilson) requires bots using AI to disclose that they are bots. AB 410 is pending on the Assembly Appropriations Committee Suspense File.

- AB 412 (Bauer Kahan) requires a of a generative AI model to document any copyrighted materials used to train the model. AB 412 is pending in the Senate Judiciary Committee.

- SB 420 (Padilla) regulates high-risk automated decision systems. SB 420 is pending in this Committee.

- AB 489 (Bonta) makes provisions of law that prohibit the use of specified terms, letters, or phrases to falsely indicate or imply possession of a license or certificate to practice a health care profession enforceable against an entity who uses AI. AB 489 is pending in the Assembly Appropriations Committee.

- AB 853 (Wicks) requires a large online platform to retain any available provenance data in content posted on the large online platform. AB 853 is pending in the Senate Judiciary Committee.

- AB 979 (Irwin) develops a California AI Cybersecurity Collaboration Playbook to facilitate information sharing across the AI community. AB 979 is pending in the Assembly Committee on Privacy and Consumer Protection.

- AB 1018 (Bauer-Kahan) regulates automated decision systems. AB 1018 is pending in the Assembly Judiciary Committee.

- AB 1064 (Bauer-Kahan) adopts criteria for determining the level of estimated risk of an AI system on children. AB 1064 is pending in the Assembly Judiciary Committee.

- AB 1159 (Addis) prohibits using student personal information to train AI. AB 1159 is pending in the Assembly Committee on Privacy and Consumer Protection.

- AB 1405 (Bauer-Kahan) establishes a mechanism allowing natural persons to report misconduct by AI auditors. AB 1405 is pending on the Assembly Appropriations Committee Suspense File.

-- END --