CALIFORNIA PRIVACY PROTECTION AGENCY
2101 ARENA BLVD.
SACRAMENTO, CA 95834
cppa.ca.gov

Date: July 11, 2024

To: California Privacy Protection Agency Board
(Meeting of July 16, 2024)

From: Maureen Mahoney
Deputy Director of Policy & Legislation
California Privacy Protection Agency

Subject: Agenda Item 7— Legislative Update and Possible Authorization for CPPA's Positions on Pending Legislation. AB 2930, Automated decision tools (Bauer-Kahan, as amended July 3, 2024)

AB 2930 seeks to provide new protections regarding automated decision tools (ADTs). It places obligations on deployers and developers of these tools, which can include businesses, non-profits, and government agencies, and gives consumers certain rights. For example, consumers are provided notice and opt-out rights with respect to ADTs. Deployers of these tools are prohibited from using ADTs in a manner that results in unlawful algorithmic discrimination. Both deployers and developers are required to provide impact assessments under certain circumstances.

In its current form, the bill's provisions have significant overlap with the California Privacy Protection Agency's (CPPA) draft regulations on automated decisionmaking technology and risk assessments, which apply to businesses that meet a certain threshold.[1] The CPPA, however, does not have enforcement or rulemaking authority over the substantive provisions of AB 2930.

To encourage harmony and consistency between the bill and CPPA's draft regulations, staff recommends that the Agency Board support the bill if it is amended to:

- Provide CPPA with enforcement authority with respect to the bill;
- Provide CPPA with optional rulemaking authority over certain sections of the bill;
- Expand the opt-out, which currently only covers fully automated decisions, to also cover decisions in which ADTs played a substantial role;

[1] California Privacy Protection Agency, Draft Risk Assessment and Automated Decisionmaking Technology Regulations (March 2024), https://cppa.ca.gov/meetings/materials/20240308_item4_draft_risk.pdf.

- Tighten exemptions, including for cybersecurity-related technology and the exemption for impact assessments from public records requests; and
- Clarify that compliance with risk assessment requirements of another law that meet the same requirements is sufficient for compliance with this law.

Background

The California Privacy Protection Agency was established by Proposition 24, the voter initiative that amended the California Consumer Privacy Act (CCPA), and is vested with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act. The CCPA gives California consumers rights with respect to the access, deletion, correction, and sale/sharing of personal information.

California law also requires the CPPA to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security to submit to the Agency on a regular basis a risk assessment with respect to their processing of personal information.[2]

The CPPA is also required to issue regulations governing access and opt-out rights with respect to businesses' use of automated decision-making technology (ADMT), including profiling. The Agency is also required to issue regulations governing businesses' response to ADMT access requests, including to provide meaningful information about the logic involved in such decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer.[3]

The Agency is moving expeditiously to meet the statutory requirements and has issued draft regulations to implement those provisions. Both the risk assessment requirements and ADMT requirements as drafted apply to businesses that meet the CCPA's statutory threshold (those that have annual gross revenues of $25 million, or buy, sell, or share the personal information of 100,000 or more consumers, or generate 50% of more of their annual gross revenues through sale and sharing), when they use ADMT:

- For a significant decision concerning a consumer, meaning a decision using information that's in scope of the CCPA that results in access to, or the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services,
- For extensive profiling, including work or educational profiling, public profiling, and profiling for behavioral advertising, or

[2] Civ. Code § 1798.185(a)(15)(B)
[3] *Id.* at § 1798.185(a)(16)

- Processing the personal information of consumers to train ADMT that is capable of being used for any of the following:
    - For a significant decision concerning a consumer
    - To establish individual identity
    - For physical or biological identification or profiling
    - For the generation of a deepfake.

Additionally, the risk assessment requirements apply to businesses that use personal information to train artificial intelligence in the above situations, and additionally in the training of large language models.

At a high level, the draft regulations, together, require businesses that meet the thresholds to:

- Conduct and submit risk assessments to the CPPA;
- Provide to consumers pre-use notice of ADMT;
- Provide consumers with the right to opt-out of ADMT, subject to certain exemptions;
- Provide access to meaningful information about the logic involved in those decisions; and
- For businesses that use biometric data for a significant decision (such as emotion-assessment technology to analyze performance at work), ensure that it does not discriminate based on protected classes.

AB 2930 Summary

Key definitions: "consequential decision" means a decision or judgment that has a legal, material, or similarly significant effect on an individual's life relating to access to government benefits or services, assignments of penalties by government, or the impact of, access to, or the cost, terms, or availability of, any of the following:

- Employment with respect to all of the following: (A) Pay or promotion (B) Hiring or termination (C) Automated task allocation that limits, segregates, or classifies employees for the purpose of assignment or determining material terms of conditions of employment
- Education and vocational training as it relates to all of the following (A) Assessment or placement (B) Detecting student cheating or plagiarism (C) Accreditation (D) Certification (E) Admissions or enrollment (F) Discipline (G) Evaluation (H) Financial aid or scholarships
- Housing or lodging, including rental or short-term housing or lodging
- All of the following essential utilities: (A) Electricity (B) Heat (C) Water (D) Internet or telecommunications access (E) Transportation
- Family planning
- Adoption services, reproductive services, or assessments related to child protective services

- Health care or health insurance, including mental health care, dental or vision
- Financial services
- All of the following aspects of the criminal justice system: (A) Risk assessments for pretrial hearings (B) Sentencing (C) Parole
- Legal services
- Private arbitration
- Mediation
- Voting

"Deployer" means a person, partnership, local government agency, developer, corporation or any contractor or agent of those entities, that uses an automated decision tool to make a consequential decision.

"Developer" means a person, partnership, state or local government agency, or corporation that designs, codes or produces an automated decision tool or substantially modifies an artificial intelligence system or services for the intended purpose of making, or being a substantial factor in making, consequential decisions, whether for its own use or for use by a third party.

"Substantial factor" means an element of a decision-making process that is capable of altering the outcome of the process.

Amends the Business and Professions code:

- Requires deployers of automated decision tools (ADTs), defined as "an artificial intelligence system or service that makes a consequential decision, or is a substantial factor in making consequential decisions," to:
    - Refrain from using ADTs in a manner that results in unlawful algorithmic discrimination.
    - Perform an impact assessment on any ADT before it is first deployed and annually thereafter.
    - If first used prior to January 1, 2025, perform impact assessments on ADTs prior to January 1, 2026 and annually thereafter; and provide to CPPA within 30 days upon request.
    - Refrain from using the ADT if an impact assessment identifies a reasonable risk of algorithmic discrimination.
    - Provide notice to consumers subject to the decision that the ADT is being used to make, or is a controlling factor in making, a consequential decision, at or before the point that it is used to make a consequential legal decision;
    - If technologically feasible, accommodate a natural person's request to not be subject to the automated decision tool, where a consequential decision is made based solely on the output of an automated decision tool, and to use an alternative decision process or accommodation.

- Requires developers of automated decision tools (ADTs) to:
    - Provide deployers with a statement regarding intended uses and documentation regarding known limitations, foreseeable risks of discrimination, type of data used to train the tool, and a description of how it was evaluated for validity;
    - On or before January 1, 2025, and annually thereafter, complete and document an assessment of any automated decision tool that it designs, codes, or produces that includes specified elements, including pursuant to any significant update; and provide to CPPA within 30 days of request;
    - Not make available to potential deployers an ADT if an impact assessment performed by a deployer identifies a reasonable risk of algorithmic discrimination;
    - If the developer is a state government entity, provide CPPA, by January 1, 2026, with a list of ADTs initially deployed prior to January 1, 2025.
- Requires developers or deployers to:
    - Develop a governance program that contains reasonable administrative and technical safeguards to manage the reasonably foreseeable risks of unlawful discrimination associated with the use or intended use of an automated decision tool; and
    - Make publicly available, in a readily accessible manner, a clear policy that summarizes the types of ADT currently in use or made available to others by the deployer or developer; and how they manage the resulting reasonably foreseeable risks of algorithmic discrimination.
- Requires CPPA to:
    - By January 1, 2027, establish a staggered schedule identifying when each state government deployer shall comply with the provisions of the bill for each tool deployed by the state government deployer, with full compliance by January 1, 2031.
- Enforcement
    - CPPA can bring administrative fines (maximum $10,000 per violation per day) for failing to complete the required impact assessments.
    - CPPA may provide impact assessments to the Attorney General, district attorneys, county counsels, city attorneys, city prosecutors in certain situations, and the Civil Rights Division.
    - The Attorney General, district attorneys, county counsels, city attorneys, city prosecutors in certain situations, and the Civil Rights Division (but not the CPPA) can bring civil actions against a deployer or developer for violations.
    - Provides a 45-day cure period for injunctive relief.
- Exemptions
    - For cybersecurity-related technology, "including technology designed to detect, protect against, or respond to security incidents, identify theft, fraud, harassment, malicious or deceptive activities or any illegal

activity, preserve the integrity or security of systems, or investigate, report, or prosecute those responsible for those actions."
    - For deployers with fewer than 55 employees unless the ADT impacts more than 999 people.
    - Deployers are exempted from the impact assessment requirement if the deployer uses the tool only for its intended use as determined by the developer; does not make any substantial modifications; and developer has done its impact assessment and required documentation.
    - Impact assessments are exempt from public records access requests.
    - Trade secrets are exempt from disclosure, though if the developer or deployer withholds information on the grounds that it is a trade secret, the developer or deployer must notify the relevant entity or natural person and provide a basis for the withholding.

Analysis

The bill as written potentially invites uncertainty and inconsistency. There is a great deal of overlap between AB 2930 and the Agency's draft ADMT and risk assessment regulations. Both generally require covered entities to perform risk assessments and provide notice and opt-out rights with respect to automated decision-making.

If this bill were to be adopted in its current form, a separate and overlapping set of requirements would apply for businesses covered by both AB 2930 and the CCPA. This would cause a great deal of confusion and could make it difficult for businesses to comply. The problems will only get worse if AB 2930 is adopted and then amended in the future—creating the potential for further divergence and conflicting requirements.

To help address this, staff has provided technical assistance to the author on an earlier draft of the bill, to harmonize the bill with the draft regulations, for example to:

- Expand the bill's notice requirements to include explanation of the logic of the ADMT, key parameters, and intended output;
- Provide CPPA with enforcement authority with respect to the bill;
- Provide CPPA with optional rulemaking authority over certain sections of the bill;
- Expand the opt-out to cover not only fully-automated decisions, but also decisions in which ADTs played a substantial role;
- Tighten exemptions, including for cybersecurity-related technology; and
- Clarify that compliance with risk assessment requirements of another law that meet these same requirements is sufficient for compliance with this law.

The author has received staff's suggested amendments described above and has said more time is needed to consider them. While the June 24, 2024 version of the bill reflected improvements to the notice requirements of the bill, the other suggestions are not yet reflected in the bill.

Finally, if the bill were to pass, the Agency would certainly need additional resources to meet the requirement to establish a staggered schedule identifying when each state government deployer must comply with the provisions of the bill, which could prove time consuming and complex depending on the circumstances of state departments.

Recommendation

CPPA staff recommends that the Board support the bill if it is amended to:

- Provide CPPA with enforcement authority with respect to the bill;
- Provide CPPA with optional rulemaking authority over certain sections of the bill;
- Expand the opt-out to cover not only fully-automated decisions, but also decisions in which ADTs played a substantial role;
- Tighten exemptions, including for cybersecurity-related technology and the exemption for impact assessments from public records requests; and
- Clarify that compliance with risk assessment requirements of another law that meet these same requirements is sufficient for compliance with this law.

Public support/opposition

Please note that these are positions registered on the June 24, 2024 version of the bill, per the Senate Judiciary Committee analysis, and may not necessarily reflect positions on the July 3, 2024 version of the bill.[4]

<u>Support</u>

American Federation of Musicians, Local 7
California Employment Lawyers Association
Center for Democracy and Technology
Center on Race and Digital Justice
Consumer Reports
East Bay Community Law Center
Economic Security California Action
Equal Rights Advocates
The Greenlining Institute

[4] Senate Judiciary Committee Analysis at 21 (June 30, 2024), https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=202320240AB2930.

Legal Aid at Work
Rise Economy
Secure Justice
Techequity Collaborative

Opposition

ACLU California Action
Advanced Medical Technology Association
American Council of Life Insurers
American Property Casualty Insurance Association
America's Physician Groups
Association of California Life & Health Insurance Companies
California Association of Health Plans
California Bankers Association
California Community Banking Network
California Credit Union League
California Financial Services Association
California Hospital Association
California Life Sciences
California Medical Association
California Mortgage Bankers Association
Consumer Technology Association
Electronic Frontier Foundation
Google
Kaiser Permanente
Mortgage Bankers Association
National Association of Mutual Insurance Companies
Orange County Business Council
Pacific Association of Domestic Insurance Companies
Personal Insurance Federation of California
Sutter Health
Verizon Communications