

## **New Cybersecurity, Privacy and Automated Decisionmaking Rules Coming Soon to California**

Article By:

Elliot R. Golding

Michael G. Morgan

David P. Saunders

Alya Sulaiman

John C. Ying

Doris Yuen

---

Substantial changes to the California Consumer Privacy Act (CCPA) are coming soon through five sets of proposed regulations governing (1) cybersecurity audits, (2) privacy risk assessments, (3) artificial intelligence/automated decisionmaking technology (ADMT), (4) revisions to existing regulations and (5) new rules for insurance companies. On December 8, 2023, the California Privacy Protection Agency (CPPA) voted to advance the **proposed cybersecurity audit regulations** to formal rulemaking but sent the other regulations back to agency staff to refine. The proposed regulations are expansive and likely to be finalized in 2024, so businesses should start planning now

---

for upcoming changes.

## IN DEPTH

---

### THE CPPA'S DECEMBER 8, 2023, MEETING AND CYBERSECURITY AUDIT REGULATIONS

At its **December 8 meeting**, the CPPA discussed five sets of proposed CCPA regulations about:

1. Privacy risk assessments
2. Cybersecurity audits
3. ADMT
4. Changes to the existing CCPA regulations
5. Rules for insurance companies

The revised cybersecurity audit regulations clarify that they apply to businesses that:

- Derived 50 percent or more of their annual revenues from selling or sharing consumers' personal information in the preceding calendar year; or
- As of January 1 of the calendar year, had annual gross revenues in excess of \$25 million (revenue threshold to be adjusted in the other proposed rules) and in the preceding calendar year (1) processed the personal information of 250,000 or more consumers or households, (2) processed the sensitive personal information or 50,000 or more consumers

---

or (3) processed the personal information of 50,000 or more consumers that the business had actual knowledge were less than 16 years old.

Now that the cybersecurity audit regulations have advanced, the CPPA will publish a “statement of reasons” explaining the rules, economic and fiscal impact statements and formally issue the draft set of regulations for public comment. If past is prologue, the rulemaking process could take six to eight months or longer. However, given the scope and **onerous requirements** of the proposed cybersecurity audit regulations, now is the time for companies to start paying attention.

## **AUTOMATED DECISIONMAKING TECHNOLOGY**

The draft regulations propose requiring businesses using ADMT in the following ways to provide pre-use notice, opt-out and access rights:

- For a decision that produces legal or similarly significant effects on the consumer;
- Profiling a consumer acting in their capacity as an employee, independent contractor, job applicant or student;
- Profiling a consumer while they are in a publicly accessible place;
- Profiling a consumer for behavioral advertising, such as evaluating consumers’ personal preferences and interests to display advertisements to them;
- Profiling a consumer that the business has actual knowledge is under the age of 16; and
- Processing the personal information of consumers to train ADMT.

During the December 8 meeting, the CPPA board and staff were split

---

on how to regulate ADMT, specifically, in the workplace. There are open questions regarding transparency for employees whose employers use ADMT in the workplace as well as potential opt-out rights for certain ADMT use cases in the employment context. The CPPA staff have been tasked with evaluating whether to (a) narrow the scope of these draft regulations or (b) develop more carve-outs from the draft rules.

## **PRIVACY RISK ASSESSMENTS**

Although most of the substantive requirements remain unchanged from **earlier drafts**, many of the latest changes to the privacy risk assessment regulations relate to ADMT. For example, the latest proposal would require risk assessments for a broader range of ADMT, such as biometric identity detection, generation of deepfakes or the operation of generative models like large language models. Among other things, such risk assessments must cover:

- An explanation of why the business wants to use ADMT, including the benefits of ADMT over manual processing;
- A plain language description of the personal information processed by the ADMT;
- A plain language explanation of the steps the business has taken or will take to maintain the quality of the personal information processed by the ADMT;
- A description of the limitations on the ADMT use;
- A plain language description of the logic the ADMT uses, including any assumptions made by it;
- A plain language explanation of how the business evaluates the ADMT for validity, reliability and fairness; and
- A description of the need for human involvement in the business's use of the ADMT.

---

CPPA board members also supported extending to 24 months the initial deadline to submit assessments to the CPPA, but they raised concerns about compliance costs and how certain provisions would survive against [the injunction on California's Age-Appropriate Design Code Act](#). Thus, the board members voted to send these regulations back to the staff to integrate individual board member feedback.

## **CCPA REGULATION CHANGES**

The CPPA also discussed proposed changes to existing CCPA regulations, including:

- The addition of a new Sensitive Personal Information category for information of consumers less than 16 years old;
- The addition of more illustrative examples related to their principles of symmetry in choice and prohibition of dark patterns; and
- Modest adjustments to the “business” revenue threshold for CCPA applicability as well as the range of financial penalties for violations of the CCPA.

The CPPA board voted to require additional staff drafting before formal rulemaking.

## **WHAT'S NEXT?**

The cybersecurity audit regulations will now move to formal rulemaking, which likely means the regulations won't be finalized for a minimum of four to six months. The other draft regulations will go back to the staff for additional work, ensuring that those regulations will not begin rulemaking until next year. Companies would be wise to take this

opportunity to at least benchmark their current readiness against the proposed cybersecurity audit regulations and understand just how much work will be required to become compliant.

© 2025 McDermott Will & Emery

---

National Law Review, Volume XIII, Number 349

Source URL: <https://natlawreview.com/article/new-cybersecurity-privacy-and-automated-decisionmaking-rules-coming-soon-california>