May 8, 2025

AI Deregulatory Trends Continue; CPPA Board Proposes Revised Draft Regulations on Automated Decision-Making Technology, Risk Assessments, and Cybersecurity Audits

by Henry W. Tharpe

The California Privacy Protection Agency ("CPPA") Board released newly modified draft regulations addressing automated decision-making technology ("ADMT"), risk assessments, and cybersecurity audits under the California Consumer Privacy Act ("CCPA"). The Board voted to initiate a second round of public comment on these revised regulations, with the comment period closing on June 2, 2025. This extended comment period, longer than the statutory minimum of 15 days, reflects the CPPA's efforts to accommodate input from both industry stakeholders and civil society groups. The revised draft regulations walk back the prior rules extensive new obligations—a welcome change for businesses currently overloaded by divergent state privacy frameworks. Below, we outline the key updates and implications for businesses. See our previous alert on these proposed rules here.

Key Updates to the Proposed Regulations

1. Narrowed Scope of Automated Decision-Making Technology (ADMT)

The proposed regulations refined the definition of ADMT to apply only to systems that "substantially replace" human decision-making, rather than those that "substantially facilitate" it. The deletion of references to "Artificial Intelligence" further streamlines the scope, leaving space for the California legislature to craft a comprehensive state AI law, such as the proposed Colorado Artificial Intelligence Act. Under the proposed regulations, "substantially replace human decision making" means "a business uses the technology's output to make a decision without human involvement."

2. Elimination of Certain ADMT Opt-Out Rights

The new regulations also narrow the scope of consumers' right to opt out of automated decision making. In the previous draft of the regulations, consumers were granted the right to opt-out of ADMT used by businesses for a myriad of standard business practices, like profiling for behavioral advertising (which can include first party advertising), hiring and firing, and identity verification. The opt-out rights that have been removed in this round of proposed regulations include: workplace profiling, education profiling, profiling through observation in public places, the training of ADMT systems, and certain advertising. That change brings the CPPA rules closer to the scope of profiling opt outs arising under other state privacy laws.

3. Streamlined Pre-Use Notice Requirements

Businesses leveraging ADMT can now bundle “pre-use” notices with existing CCPA notices at the point of collection, relieving businesses from having to offer yet another CCPA notice. Such pre-use notices are required when businesses use ADMT to make “significant decisions” regarding a customer. Under the new proposed regulations, “significant decision” means a decision that results in the provision or denial of, financial or lending services, housing, education enrollment or opportunities, employment or independent contracting opportunities or compensation, or healthcare services. The new regulations also removed other pre-use notice triggers such as profiling, or for training ADMT models. Given the myriad of notices required under the CCPA, businesses typically streamline notices to the extent possible.

4. Revisions to Cybersecurity Audit Requirements

The draft regulations modify cybersecurity audit requirements to streamline reporting and certification obligations. Specifically:

- A member of the business’s executive management team who is directly responsible for cybersecurity compliance now certifies the completion of audits instead of a board member.
- The CPPA consolidated requirements for reporting to the agency.

The CPPA Board is also considering adjusting deadlines for cybersecurity audits based on business revenue thresholds. For example, businesses grossing over $100 million may face an accelerated audit deadline on January 1, 2028 while smaller businesses retain more time to comply, up to January 1, 2030.

5. Simplified Risk Assessment Requirements

Under the previous version of the regulations, businesses whose processing of personal information met certain thresholds would be required to conduct and submit risk assessments to the CPPA before starting the processing. One trigger included selling or sharing personal information, which means that the use of ubiquitous website analytics tools necessitates the risk assessment. The revised regulations remove certain onerous requirements, such as the former obligation to detail mitigation measures to ensure the “quality” of personal information processed by ADMT systems. Businesses are now required to “identify and document” the personal information processed, aligning the rules more closely with Colorado’s AI Act. Businesses can now also use risk assessments conducted for another purpose to satisfy their obligations under these proposed regulations such assessment contains the necessary information or could be supplemented with such. Additionally, the new draft provides hypothetical examples to help businesses understand compliance requirements, particularly for those already adhering to similar laws in other states.

Next Steps for Businesses

1. Submit Comments

Businesses and trade associations should submit comments on the revised draft regulations by June 2. Public input has historically led to material changes in CCPA rulemaking.

2. Evaluate Compliance Readiness

Businesses should begin preparing for compliance with the revised regulations by:

- Assessing ADMT Use: Evaluate whether your organization uses ADMT systems that substantially replace human decision-making. If so, ensure your processes align with the updated pre-use notice requirements and that you have the technical capabilities to effectuate any opt outs that apply.
- Reviewing Cybersecurity Audit Processes: Verify that your organization's cybersecurity audit processes meet the streamlined certification and reporting requirements. Consider adjusting internal deadlines based on anticipated changes to compliance timelines.
- Streamlining Risk Assessments: Align existing privacy review processes with the simplified risk assessment requirements to avoid reopening prior assessments unnecessarily.

The CPPA Board has until November 2025 to finalize the regulations and submit them to the Office of Administrative Law for approval. Given the ongoing nature of this rulemaking, businesses should anticipate further revisions and additional rounds of public comment. For assistance in submitting comments, evaluating compliance requirements, or navigating the complexities of the CCPA, please reach out to Kilpatrick Townsend. Our team is here to help you stay ahead of regulatory developments and ensure your organization remains compliant.