WILSON SONSINI

CPPA Board Opens Draft Regulations for Public Comment

CONTRIBUTORS


Malcolm Yeary


Angela Guo


Eddie Holman

ALERTS

May 8, 2025

Key Changes to Upcoming AI, Risk Assessment, and Cybersecurity Regulations

On May 1, 2025, the California Privacy Protection Agency (CPPA) Board met again to discuss updates to the latest draft California Consumer Privacy Act (CCPA) regulations related to automated decision-making technology (ADMT), cybersecurity audits, risk assessments, and an assortment of other updates to existing regulations. These latest updates come after the CPPA first released draft regulations on these topics in July 2024 and initiated the formal rulemaking in November 2024, as analyzed in a prior alert. In April 2025, the Board continued to grapple with public concerns and received hundreds of public comments on the prior draft regulations, an analysis of which can be found in this recent client alert. At the CPPA meeting last week, CPPA staff proposed significant changes to the prior draft, on which the Board provided more feedback and agreed to open the regulations for public comment as soon as this week and closing June 2, 2025.

CPPA Board Discussion of Substantive Updates to Draft Regulations

- *Definition of ADMT and "significant decision"*: The latest draft regulations significantly narrow the definition of "ADMT" to any technology that processes personal information and uses computation to *replace or substantially replace* human decision making. "Substantially replace" means a business uses the ADMT's output to make a decision without a human reviewer to interpret or review the output and have the authority to make or change the decision. Businesses that use ADMT to make a "significant decision" concerning a consumer would be subject to ADMT obligations. "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. Public comments during the meeting raised concerns about the narrowed scope of covered ADMT systems effectively allowing employers to self-certify themselves out of coverage. In contrast to the public comments, Chair Jennifer Urban and the Board seemed receptive to the narrowed scope.
- *"Behavioral advertising," "training," "work or educational profiling," "public profiling," and "hiring decisions" thresholds*: The latest draft regulations remove the "training," "work or education profiling," "public profiling," and "behavioral advertising" thresholds for ADMT obligations. In the case of "hiring decisions" that trigger ADMT requirements, Board Member Alastair Mactaggart advocated for further narrowing the language from "ensures" that the ADMT works as intended and does not unlawfully discriminate to "makes reasonable efforts to ensure." He noted that it may be difficult for small businesses in the gig economy to ensure that all of their services, especially those they obtain from third parties, are strictly following anti-discrimination laws. The rest of the Board and staff pushed back on Mactaggart's suggested narrowing, citing numerous other current anti-discrimination laws and the ease of making decisions on a neutral basis.
- *Pre-use notice and notice at collection requirements for ADMT*: The latest draft regulations make it clear that a business may provide its ADMT pre-use notice in its general CCPA notice at collection. Chair Urban clarified that although the Board is comfortable with this approach, businesses should

- *Pre-use notice and notice at collection requirements for ADMT*: The latest draft regulations make it clear that a business may provide its ADMT pre-use notice in its general CCPA notice at collection. Chair Urban clarified that although the Board is comfortable with this approach, businesses should not bury the pre-use notice by overwhelming the consumer with a flurry of notices. She noted that the greatest push back to the pre-use notice section of the April draft regulations was the requirement for an explanation of how generated output may be used for behavioral advertising, which was eliminated in the latest draft regulations. Although the Board seems settled on this approach, Chair Urban called for additional public comments and guidance to ensure effective communication of pre-use notices.
- *Cybersecurity audits*: The latest draft regulations propose a longer, phased implementation of the cybersecurity audit requirements over a three-year period, with deadlines determined by annual gross revenue. CPPA staff presented the Board with two options. Option 1, which is currently in the latest draft regulations, would subject businesses with annual revenue above $100 million to an April 1, 2028, deadline, and smaller businesses to the requirement over the course of the following two years. Option 2 would subject businesses with annual revenue above $1 billion to the April 1, 2028, deadline, and smaller businesses to the requirement over the course of the following three years. The Board discussed at length the difference between the two options and asked staff for more concrete economic analysis by the July 24, 2025, meeting. Board Member Drew Liebert nearly proposed a formal motion to require the cybersecurity audits sooner, citing the prevalence of cybercrime and noting that it would not be difficult for large companies to comply since they already have cybersecurity practices in place. In the end, the Board agreed to release the draft regulations for public comment with Option 1 and reserved the final decision for the July meeting.
- *Risk assessments*: The latest draft regulations introduce a new term, "risk assessment report," to clarify what information must be documented for a risk assessment and submitted to the CPPA or Attorney General upon request. CPPA staff revised thresholds for risk assessments, simplified annual risk assessment submission requirements, and provided guidance for businesses to develop internal crosswalks to comply with the requirements of the draft regulations and the Colorado Privacy Act. Board Member Dr. Brandie Nonnecke raised concerns about the lack of standardization for adequate risk assessments, and staff recognized that the agency will learn from future developments how to amend the draft regulations. The draft regulations further eliminated "work or education profiling" and "public profiling" as triggers for risk assessments. In lieu of "public profiling," staff proposed an alternate associated definition that would trigger a risk assessment only if processing a consumer's sensitive location data. Sensitive locations include, among other places, healthcare facilities, educational institutions, and places of worship. Board Member Mactaggart emphasized the need to clarify the rest of the thresholds for risk assessments, arguing that the current language could trigger unnecessary risk assessments for routine automated processes, such as basic HR functions like evaluating ID swipes to track employees' office attendance or work hours.
- *First-year costs of latest CCPA regulations*: In response to the Board's request from the April CPPA meeting, staff prepared an updated preliminary economic analysis of the first-year cost of the draft regulations. The analysis compares new first-year costs of approximately $1.2 billion to the approximately $3.5 billion first year costs that would have been imposed on California businesses under the April draft regulations. The economic analysis concludes that the latest draft regulations would produce a 64 percent cost savings over the previous version. There are two features of the latest draft regulations that contribute to this significant cost reduction. First, the revised definition of ADMT and the limited scope of "significant decision" would apply to significantly fewer CPPA-regulated businesses. Second, the new cybersecurity audit requirements are narrower, and with Option 1 of the phased-in timing, the draft regulations give the business community more time to adapt and prepare for audits.

Next Steps

The CPPA Board voted 5-0 to authorize the staff to release the latest draft regulations for public comment and discuss those comments during its next meeting on July 24, 2025. Staff emphasized that the Board must submit the regulations by November 2025 to avoid having to issue a new public notice, a new initial statement of reasons, a new Standardized Regulatory Impact Assessment, and a new 45-day comment period. Additionally, staff explained that if the California Office of Administrative Law rejects the regulations, the Board would have 120 days to fix the regulations. Board Member Mactaggart pushed for a longer public comment period to give the business community more time to digest the significant updates to the draft regulations, even at the risk of running into the 120-day cure period. The Board now faces the difficult task of incorporating public comments into the draft regulations and finalizing them before November, or risk facing legal challenges from businesses and trade groups for exceeding their statutory and constitutional authority with the draft regulations.

Wilson Sonsini routinely helps companies navigate complex privacy and data security issues. For more information or advice concerning your CCPA compliance efforts, please contact Tracy Shapiro, Eddie Holman, Yeji Kim, Malcolm Yeary, Angela Guo, or any member of the firm's Data, Privacy, and Cybersecurity practice. For more information or advice concerning your compliance efforts related to ADMT or artificial intelligence, please contact Scott McKinney, Eddie Holman, Maneesha Mithal, or any member of the firm's Artificial Intelligence and Machine Learning team.