The California Privacy Protection Agency Advances Regulations to Reign in AI, Mandate Security Audits and Risk Assessments, and Update CCPA Obligations

Alysa Z. Hutnik, Aaron J. Burstein, Alexander I. Schneider

October 8, 2024

The California Privacy Protection Agency (CPPA) has signaled it will advance rulemaking at its upcoming November 8 board meeting to place restrictions on the use of automated decision-making technology (ADMT) and impose new obligations to require businesses to conduct cybersecurity audits and risk assessments. The agency has grappled with these issues for more than two years, including soliciting formal comments in a February 2023 invitation for preliminary comments and conducting other stakeholder outreach.

The CCPA grants the CPPA the authority to issue regulations relating to cybersecurity audits, risk assessments, and ADMT, but leaves the details to agency rulemaking. To date, that approach has left a gap with other comprehensive state privacy laws, which give consumers the right to opt out of automated "profiling" and require documenting Data Protection Assessments (*i.e.*, DPIAs). California is one of just three states (along with Colorado and New Jersey) that include rulemaking authority in their comprehensive state privacy laws, placing significant autonomy with the CPPA to determine the state's approach to these issues.

The CPPA also plans to issue rules that update CCPA compliance obligations, including new disclosures when denying privacy rights requests and categorizing children and teen data as "sensitive personal information."

In a stunning assessment, staff of the CPPA estimates the total costs of the latest regulatory initiative to be $3.5 billion in the first year, and an average of $1 billion each subsequent year for the first ten years. The agency defends its approach by alleging that cybersecurity audits will reduce cybercrimes to the tune of $1.5 billion in the first year and $66.3 billion by 2036.

In this blog post, we highlight key updates contained in the CPPA's latest rulemaking initiative.

New Rules for Use of ADMT

Under the CPPA's proposal, the ADMT regulations would be triggered in one of the following three ways:

- First, the regulations can be triggered by "significant decisions concerning the consumer."

These include decisions impacting access to or denial of financial or lending services, housing, insurance, education, criminal justice, employment, healthcare services, or essential goods or services (including groceries, medicines, hygiene products, or fuel). Businesses using ADMT for these significant decisions would be required to provide an adverse significant decision notice to consumers prior to making decisions that deny opportunities or services to the consumer.

- Second, the regulations can be triggered by extensive profiling of the consumer using automated processing, including in their job, at school, in public, or via behavioral advertising. The regulations define "behavioral advertising" to include **both** cross-context behavioral advertising based on activity across the internet **and** first-party behavioral advertising based on activity within a business's own website, apps, or services.

- Third, the regulations can be triggered when training ADMT to generate significant decisions, to establish individual identity, for identification or profiling, or to generate deepfakes (defining deepfakes as "manipulated or synthetic audio, image, or video content that depicts a consumer saying or doing things they did not say or do and that are presented as truthful or authentic without the consumer's knowledge or permission).

The new rules would regulate the use of ADMT through a notice informing the consumer about the use of ADMT, a limited right to opt out of ADMT, and a right to access information about the use of ADMT and the output with respect to the consumer.

The rules provide exceptions and limitations on the right to opt out of ADMT. For example, the right to opt out of the use of ADMT for significant decisions concerning the consumer is not available if the consumer is offered an opportunity to appeal the decision to a human reviewer. The rights to opt out of the use of ADMT for extensive profiling in the workplace or education contexts can also be limited if the business conducts an evaluation to ensure the ADMT is accurate and non-discriminatory.

Mandatory Risk Assessments

The CPPA proposes that businesses that process personal information that "presents significant risk to consumers' privacy" must conduct a risk assessment to determine whether the risks to consumers' privacy outweigh the benefits to the consumer, the business, other stakeholders, and the public. The types of activities that could involve "significant risk" are broadly defined in the rulemaking proposal, including:

- Processing activities involving the sale or sharing of personal information.

- Processing activities involving the processing of sensitive personal information (other than in certain employment or benefits contexts).

- Processing activities involving a significant decision concerning a consumer, extensive profiling (including for behavioral advertising), or training ADMT. All three of these categories trigger ADMT rules, as we've discussed above.

The proposed regulations list the types of information that must be included in the risk assessments, including processing details (*i.e.*, identification of the purpose of the processing, the categories of personal information that will be processed, and how the business collects, uses, and discloses the information); the benefits of the processing including in particular expected profits for the business; possible negative impacts to consumer privacy; and how the business will safeguard against possible negative impacts.

The CPPA proposes that businesses must submit their risk assessments within 24 months of the effective date of the regulations, and then annually thereafter. A business's "highest-ranking executive who is responsible for oversight of the business's risk assessment compliance" will be required to file a written certification along with the risk assessment.

Cybersecurity Audits

Another new requirement in the proposed regulations is for covered businesses to complete a cybersecurity audit within 24 months of the effective date of the regulations, and then annually thereafter. The audit would be required to assess the company's cybersecurity program and identify any gaps or weaknesses in the program, including the status of efforts to address such gaps or weaknesses. Substantively, audits would assess standard components of a cybersecurity program, including authentication/encryption, zero trust architecture, access controls, personal information inventory and management, secure configuration of hardware and software, scanning for vulnerabilities, audit logs, network monitoring and defenses, use of virus protections, proper configuration of information systems, training, oversight of third parties, data retention and destruction practices, disaster recovery, business continuity, and incident response.

Businesses would be required to use a "qualified, objective, independent" auditor. To ensure a degree of independence, the regulations require internal auditors to report to the company's board of directors or equivalent governing body. Auditors cannot participate in the business activities that they audit.

Businesses would be required to submit an annual certification of completion of a cybersecurity audit —and not the actual audit report—to the CPPA.

Not all businesses would be required to complete an annual audit. The CPPA states that there are two categories of businesses that would be required to conduct annual cybersecurity audits: (1) businesses that derive 50 percent or more of their annual revenues from selling or sharing consumers' personal information, or (2) businesses that in the prior calendar year met the CCPA's annual gross revenue threshold and either processed personal information of at least 250,000 consumers or sensitive personal information of 50,000 consumers. Adjusted for inflation under the recently-passed AB 3286, the gross revenue threshold is now just above $27.9 million according to the CPPA.

Reclassifying children and teen data as "Sensitive Personal Information"

Citing its authority in the CCPA to update or add categories of personal information or sensitive personal information, the CPPA proposes that all personal information of a consumer known to be under 16 years of age will be categorized as sensitive personal information. Even though the CCPA already restricts the sale or sharing personal information of anyone under 16 years of age without consent, the CPPA's latest proposal would also allow minors to opt out of the use or disclosure of their personal information where used to infer characteristics about them. In the draft initial statement of reasons, the CPPA explains that its proposal is aimed at both harmonizing the CCPA with other state laws that treat personal data of a known child under 13 as sensitive data, while also providing expanded protections for consumers ages 13 to 15.

Requirements for responding to privacy rights requests

The CPPA proposes additional changes to the process of submitting and responding to privacy rights requests that may require businesses to update their processes and procedures. Here are some

notable proposed changes:

- **Handling of toll-free requests:** The CPPA proposes that businesses that require the consumer to call a toll-free telephone number to submit a CCPA request must ensure that the individuals handling those phone calls have the knowledge and ability to process the consumer's CCPA requests.
- **Look-back period:** The CPPA will now require businesses to offer a way for consumers to request personal information collected prior to the 12-months preceding the business's receipt of the consumer's request.
- **Denial notice disclosure:** The CPPA wants to see the following or similar language added to every denial of a privacy rights request: "If you believe your privacy rights have been violated, you can submit a complaint to the California Privacy Protection Agency at [link to complaint form] or to the California Attorney General at [link to complaint form]."

Process for finalizing proposed regulations

The CPPA is expected to vote on initiating formal rulemaking on the proposed regulations at its November 8, 2024 board meeting. Members of the public will have 45 days to submit comments to the CPPA once the rulemaking begins. After the comment period closes, the CPPA can then proceed with finalizing the regulations, a process that requires the agency to consider and respond to every comment it receives and to publish a final statement of reasons. If the CPPA makes any substantive changes to the proposed regulations based on the comments that it receives, the CPPA must provide an additional 15 day comment period on the revised version of the regulations.

A recent California 3rd District Court of Appeals decision confirmed that CPPA regulations take effect immediately and do not require a one year waiting period. As a result, once the CPPA finalizes the proposed regulations and files the regulations with the California Secretary of State, the regulations will become effective as follows: January 1, if filed between September 1 and November 30; April 1, if filed between December 1 and February 29; July 1, if filed between March 1 and May 31; and October 1, if filed between June 1 and August 31. The CPPA can also petition for an earlier effective date by demonstrating good cause.