LAW360

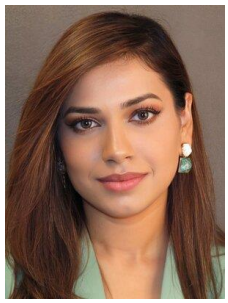
Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

A Look At New Calif. Cybersecurity, Risk Assessment Rules

By **Hannah Levin, Phillip Wiese and Rimsha Syeda** (August 22, 2025, 4:41 PM EDT)


Hannah Levin


Phillip Wiese


Rimsha Syeda

The California Privacy Protection Agency Board unanimously voted on July 24 to finalize a package of regulations related to automated decision-making technology, or ADMT; cybersecurity audits; and risk assessments.

The long-awaited regulations establish additional requirements on certain businesses operating in California, and are now pending final review by the California Office of Administrative Law.

Requirements established by the new regulations include the following:

- ADMT is now limited to technology that makes significant decisions about consumers without human involvement — when companies use ADMT in that way, they must provide consumers with certain rights, including notice of the use of ADMT, the right to opt out and the right to appeal ADMT decisions.

- Businesses must complete an annual cybersecurity audit when their processing of personal information imposes a significant risk on consumer privacy and certify their audit to the CCPA.

- Businesses must also maintain updated risk assessments when their use of personal information could be a significant risk to consumer privacy.

Additionally, the CPPA revised certain existing regulations under the California Consumer Privacy Act. We first describe the changes to the regulations, and then provide takeaways and action items for timely compliance.

Automated Decision-Making Technology

Under the new regulations, the CPPA defines what constitutes ADMT amid its growing use and associated data security risks. ADMT is defined in the new rules as technology that processes personal information "to replace human decisionmaking or substantially replace human decisionmaking."

"Substantially replace human decisionmaking" is defined as when a business uses the technology to make a decision "without human involvement."

The regulations state that human involvement means the human reviewer (1) knows how to interpret the technology's output, (2) affirmatively reviews the technology's output to make a decision, and (3) has actual authority to make or change the technology's decision based on his or her own analysis.

Next, the rules limit the reach of the ADMT provisions only to companies that use ADMT to make a significant decision about consumers. ADMT provisions require human oversight in significant decisions. A significant decision is one that relates to financial or lending services, housing, education, employment or healthcare services.

If the definition applies, a business needs to provide consumers with certain rights. In particular, a business must provide notice of its use of ADMT, which must be displayed at or before the point of collection. The notice must describe what personal information will be used in the ADMT technology and the purposes for which the technology will be used.

Additionally, a business must allow a consumer to opt out of its use of ADMT and appeal any decisions made using that technology, both of which must be disclosed in the ADMT notice.

Of note, early versions of this rule included restrictions on the use of artificial intelligence technology more generally. Those highly controversial ADMT restrictions on AI were removed from the final rule package to allow the California Legislature to weigh in prior to any further CPPA rulemaking.

Cybersecurity Audits

The CPPA also adopted rules required by the California Privacy Rights Act, which amended the CCPA, defining the scope of businesses' mandatory annual cybersecurity audits.

Cybersecurity audits must be performed where processing of consumers' personal information may be a "significant risk" to consumers' security — that is, if the business derives 50% of its annual revenue from selling or sharing personal information, has annual gross revenues exceeding $26,625,000, or annually processes personal information of more than 250,000 consumers or sensitive personal information of more than 50,000 consumers.

Under the new rules, cybersecurity audits must follow standardized procedures and be completed by an independent auditor knowledgeable about cybersecurity and cybersecurity audits. The auditor can be internal or external, but if the business uses an internal auditor, that individual must report to a member of the business's executive management team who does not have cybersecurity responsibility.

The rules establish a number of categories of information that the auditor must review, if applicable, including the following:

- Authentication/passwords;
- Encryption of personal information;
- Account management and access controls;
- Inventory of personal information;
- Vulnerability scanning and penetration testing;
- Audit log management;
- Network monitoring and defenses;
- Cybersecurity awareness and education;

- Retention schedules; and
- Incident response management.

The CPPA adopted a phased timeline for these cybersecurity audits based on business size:

- For businesses with gross revenue of more than $100 million, the audit must cover the year 2027;

- For businesses with gross revenue between $50 million and $100 million, the audit must cover 2028; and

- For businesses with gross revenue less than $50 million, the audit must cover 2029.

All audits must be completed annually thereafter, and an annual certification of completion must be submitted to the CCPA by April 1 following the reporting period.

Risk Assessments

The CPPA also finalized rules related to businesses' risk assessments. Under the new rules, businesses must complete a risk assessment when there is a "significant risk" to consumer privacy, which includes

- Selling or sharing personal information;

- Processing sensitive information;

- Using ADMT for significant decisions; and

- Using automated processing to infer personal characteristics during education, job seeking, employment or independent contracting.

Businesses are obligated to update their risk assessments at least every three years and submit a summary report to the CPPA. The rules also acknowledge that businesses may rely on risk assessments prepared for another purpose so long as those assessments meet the new regulations.

Businesses will have until Dec. 31, 2027, to complete their risk assessments, with the first summary reports due to the CPPA by April 1, 2028.

CCPA Revisions

Finally, the CPPA included certain changes and updates to the CCPA regulations it previously issued, including imposing the following requirements:

- Any requests to opt out must be the same or fewer steps than the method to opt in (e.g., for cookie management).

- Links to a company's privacy policy must be on any webpage that collects personal information.

- Consumers may request from companies their personal information collected beyond the prior 12 months, to the extent it exists.

Next Steps

The rules now head to the California Office of Administrative Law for approval before taking effect. The Office of Administrative Law has 30 days to approve the rules.

In the meantime, businesses may want to evaluate application and start developing processes to ensure compliance with these new regulations. While these new rules are less onerous than some of the draft rules that were offered, and while the CPPA provided lead time for phased implementation, compliance may still require substantial planning and updates to existing systems.

Key Takeaways and Recommended Actions

First, businesses that use ADMT for significant decisions without meaningful human review should inventory and catalog uses of in-scope ADMT, revise their privacy policies, and implement systems to provide notice of their ADMT usage.

Second, businesses should plan to operationalize enhanced consumer rights, focusing on potential compliance gaps in how businesses process opt-out signals. The rules reflect California regulators' ongoing attention to ensuring that consumers can easily understand their CCPA rights, with particular focus on opt-out rights.

Businesses may wish to proactively evaluate their systems for receiving and honoring global privacy control signals and other user-enabled opt-out requests. In-house or outside legal counsel may support this process by reviewing implementation plans and advising on areas where the design, language or technical configurations may fall short of regulatory expectations.

Third, businesses that process consumer personal information with significant risk should begin identifying the categories of information to be covered by a cybersecurity audit and consider engaging qualified auditors, given that the audit process will likely take time and refinement.

Fourth, businesses required to conduct risk assessments should begin analyzing their internal processes to ensure all regulatory elements are addressed well before the end of 2027. Of note, legal counsel may want to consider that the CPPA permits businesses to conduct one risk assessment to comply with multiple state consumer privacy laws.

Nonetheless, the CPPA's new regulations have many more requirements than other consumer privacy laws and require integration into the businesses' broader CCPA compliance.

And lastly, businesses should keep in mind that the CPPA or the California attorney general may require a business to submit a risk assessment report at any time. Upon request, a business must submit the risk assessment report within 30 calendar days. Of note, the CPPA is part of a consortium of privacy regulators with other state attorneys general and may share certain information with them.

Hannah Levin is a partner, and Phillip Wiese and Rimsha Syeda are associates, at Morgan Lewis & Bockius LLP.

Morgan Lewis partner Ezra Church contributed to this article.