Insights: Alerts

Public comment period officially opens for California privacy and AI regulations; One need not use AI to detect the regulatory overreach.

December 2, 2024

Written by **Jon Neiditz, Henry W. Tharpe**

Public Comment Period Opens. The California Privacy Protection Agency ("CPPA") opened the public comment period on a long in the works update to the California Privacy Protection Act ("CCPA") regulations. Concerned organizations and trade associations must submit comments by January 14 of 2025. Please reach out to Kilpatrick for assistance in drafting comments to the agency or answering any other questions about the CCPA regulations.

Notable Dissent. CPPA board member and CCPA progenitor Alastair Mactaggart voted against advancing the sweeping new regulations. Among other concerns, Mr. Mactaggart noted how the novel risk assessment requirement (which requires submitting the assessments to the agency) lacks material scope limits—potentially flooding the agency with assessments and increasing businesses' regulatory burden. The CCPA statute provides broad rulemaking authority with respect to automated decision opt outs, so potential paths for litigation challenges to the proposed rules' validity remains unclear.

Your Next Steps. Concerned companies should begin by submitting comments to trade associations to walk back proposed rules' requirements. Prior iterations of CCPA rulemaking tell that the notice and comment process can result in material changes walking back the regulations' bite. Note too that promulgating CCPA regulations of this magnitude often requires multiple rounds of notice and comment.

As the rules continue to take shape, companies should also scope compliance with the regulations' novel compliance requirements. First, evaluate if your organization engages in automated decision making (that is not subject to the FCRA, which would be exempt from the CCPA) so that you can start drafting pre-use notices and operationalizing opt outs (which will likely survive the rulemaking in some form). Second, most companies subject to the CCPA could be required to submit privacy risk assessments to the agency. To prepare for that possible requirement, identify any gaps in your existing privacy review process and evaluate whether your current assessments include information that you would prefer not to submit to the agency. Third, identify if your current cybersecurity audit processes meet the proposed rules' substance, auditor and independence requirements—and identify a process for signing and submitting the certification to the CPPA.

CCPA Scope Continues to Expand. CCPA compliance has grown more burdensome given the law's ever-

growing scope. The CCPA was passed in 2018, and updated in 2020, chiefly to address Californians' consumer privacy concerns. Since that passage, however, the law's scope has been amended to include employees' and business contacts' data. The latest round of proposed updates would expand that scope further by using a data privacy law to promulgate detailed cybersecurity audit and AI rules. Every significant business with customers or employees in California would face compliance with such novel assessment requirements.

Moreover, the CCPA continues to require additional notices and new consumer choices, which benefits neither consumers nor businesses. Consumers don't have enough time to absorb notices from and exercise rights with the multitude of businesses who process their personal information. Businesses are stuck preparing numerous privacy notices and policies with everchanging content requirements.

CCPA AI Rules in Context. The CCPA's proposed AI regulations are unique for their broad applicability and detail. First, most of the recently passed California AI legislation is narrowly focused on a certain type of industry (like healthcare) or business practice (like detecting or watermarking AI generated images or providing transparency about what data sets a developer used to train generative AI systems). The CCPA rules, conversely, could apply to all businesses subject to the CCPA that use AI tools for standard business practices (like behavioral advertising or hiring). The regulations are also enforceable by a dedicated regulator, the CPPA, which likely increases the likelihood that they'll be enforced (even if bootstrapped onto an otherwise unrelated privacy enforcement action). Finally, the rules come as industry grapples with how to interpret a separate update to the CCPA, amending the definition of personal information to include information “stored in artificial intelligence systems that are capable of outputting personal information.” Until businesses and regulators achieve consensus on how to operationalize that definitional change, the proposed CCPA regulations create much more tangible requirements for companies developing and deploying AI tools.

Below we highlight the top 10 new additions to consider within the proposed regulations:

1. Introduction of Unbound Automated Decision-Making Technology (ADMT) and Artificial Intelligence (AI) Definitions:

- The proposed regulations introduce profoundly broad definitions for “automated decision-making technology” and “artificial intelligence.”
- Under the proposed regulations, “Automated decision-making technology” means “any technology that processes personal information and uses computation to execute a decision, replace human decision-making, or substantially facilitate human decision-making.” “Artificial intelligence” means a “machine-based system that infers, from the input it receives, how to generate outputs that can influence physical or virtual environments.” That language follows other definitions of AI in California law.
- The breadth of those definitions encompasses many commonplace technologies that go far beyond generative AI.

2. Expansion of Consumer Rights Related to Automated Decision-Making:

- The proposed regulations would give consumers 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.

- Businesses using this technology would be required to provide clear notice of the ADMT use to consumers and offer an opt out. To operationalize that right, businesses would have to add yet another link to already crowded website footers.
- The new regulations also allow consumers to “access” an ADMT when a business uses this technology. The right would mean a consumer could request information about the businesses' use of ADMT. If the requirement is left unchanged, expect businesses to narrow the scope of responses to such requests to the maximum permitted extent.
- Meeting that access right would be infeasible as the right is currently construed. First, the level of detail is extensive, and would require providing granular information about how the ADMT functions (e.g., the aggregate range of outcomes that the ADTM produces). Second, the response to the access right must be particularized to the specific requestor (e.g., an explanation of how the logic and assumptions of the tool were applied to the consumer's information).

3. Introduction of an ADMT Pre-use Notice:

- Businesses that use ADMT for significant decisions, profiling, or for training ADMT models would be required to provide consumers with clear notice before using ADMT.
- The proposed regulations outline the specific notice requirements that businesses would need to comply with, including requiring language that describes the specific purpose for which the business uses ADMT.

4. Detailed Requirements for Cybersecurity Audits:

- Beginning 24 months after the effective date of the proposed regulations, businesses processing the personal information of 250,000 Californians (among other triggers) would be required to conduct annual cybersecurity audits, detailing the scope, criteria, and specific metrics used for the evaluations.
- A board member or senior executive of the business must then, if the rules are unchanged, certify the cybersecurity audit's completion—and submit the certification to the California Privacy Protection Agency each year.

5. Introduction of Risk Assessments for Data Processing Activities:

- Businesses whose processing of personal information meets certain thresholds would be required to conduct and submit risk assessments to the CPPA before starting the processing. Unfortunately for businesses, those requirements are so broad that many (if not most) must make such submissions.
- One trigger includes selling or sharing personal information, which means that the use of ubiquitous website analytics tools necessitates the risk assessment.
- Any business using ADMT or AI to make significant decisions (including for hiring or behavioral advertising) would also need to submit such assessments to the CPPA.
- The proposed regulations include specific criteria for the risk assessment, including identifying several specific operational elements of the businesses' processing and examples of when a risk assessment may be needed. Businesses should ensure that their current privacy review processes meet those requirements so as to avoid reopening prior assessments.

6. Clarification on the Use of Sensitive Personal Information:

- The proposed regulations broaden the definition of “sensitive personal information” to include the personal information of consumers under the age of 16 (implementing a statutory CCPA update that the legislature passed earlier this year).
- All companies that process teen data should therefore consider the CCPA rules for sensitive information alongside the flood of new state laws addressing how companies use child data (e.g., Maryland, Connecticut, and Colorado).

7. Additional Requirements for Privacy Policies:

- Businesses would be required to provide more information in their privacy policies, such as the new rights surrounding ADMT.
- Businesses should review those new requirements prior to any annual privacy policy updates conducted after the rules take effect.
- The regulations also clarify that mobile apps would be required to include a link to the privacy policy in the application's setting menu. That requirement already exists under industry requirements, so we don't expect that change to create new compliance burdens.

8. Guidelines for the Insurance Sector:

- The proposed regulations clarify that insurance companies meeting the definition of “business” under the CCPA need comply with the CCPA's regulations only with regard to personal information that is not covered under the Insurance Code and its regulations. From our experience, most insurance companies already apply the CCPA as the proposed rules describe (and also rely on CCPA exceptions for data subject to HIPPA or GLBA).
- Information in scope for insurance companies could therefore include personal information collected on the insurance company's website (prior to establishing a customer relationship) or that an insurance company collects from its employees.
- The changes to the CCPA regulations would therefore create significant new compliance obligations for insurance companies with employees and/or business contacts in California. Moreover, without significant changes to the proposed regulations, insurance companies should scope the use of ADMT consuming personal information (such as for a commercial line of insurance) that is not subject to one of the CCPA exceptions for data subject to FCRA, GLBA, or HIPAA.

9. Amendments to Complaint and Enforcement Procedures:

- The proposed regulations provide updates that make enforcing the law more public and streamlined. First, the regulations would allow filing electronic complaints with the California Privacy Protection Agency. Second, the proposed changes remove current language that keeps probable cause determinations out of the public record.

10. More Stringent Requirements for Denials of Requests to Know:

- The proposed regulations place more requirements on businesses that deny a consumer's requests to know. If a business does so, the proposed regulations would require the business to (1) provide a detailed explanation of the basis of the denial; (2) disclose any of the consumer's personal information that is not

subject to the denial; and (3) inform the consumer that they can file a complaint with the Attorney General and provide links to the complaint forms on the business's website.

Related People

Jon Neiditz

t 404.815.6004

jneiditz@ktslaw.com

Henry W. Tharpe

t 404.532.6974

htharpe@ktslaw.com