

**Grenda, Rianna@CPPA**

---

**From:** Ebbink, Benjamin <bebbink@fisherphillips.com>  
**Sent:** Monday, June 2, 2025 6:44 AM  
**To:** Regulations@CPPA  
**Subject:** Public Comments on CCPA Updates, Cyber Risk, ADMT and Insurance Regulations  
**Attachments:** NAPEO Comments to CPPA ADMT Regulations (6.2.2025).pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Attached please find public comments on behalf of the National Association of Professional Employer Organizations (NAPEO).



**Benjamin M. Ebbink**

Partner

Fisher & Phillips LLP

621 Capitol Mall | Suite 2400 | Sacramento, CA 95814

bebbink@fisherphillips.com | O: (916) 210-0407 | F: (916) 210-0401

[vCard](#) | [Bio](#) | [Website](#) *On the Front Lines of Workplace Law<sup>SM</sup>*

---

*This message may contain confidential and privileged information. If it has been sent to you in error, please reply to advise the sender of the error, then immediately delete this message.*

June 2, 2025

*Submitted via email to [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)*

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
2101 Arena Boulevard  
Sacramento, CA 95834

**Re: Public Comment on CCPA Updates, Cyber, Risk, ADMT and Insurance Regulations**

Dear California Privacy Protection Agency:

On behalf of the National Association of Professional Employer Organizations (NAPEO), thank you for the opportunity to submit comments on the proposed regulations related to CCPA updates, cyber risk, automated-decisionmaking technology (ADMT) and insurance regulations.

We appreciate the focus and attention devoted to these issues and the recent significant changes made to the proposed regulations, but we have remaining concerns with provisions of the proposed regulations as discussed in further detail below.

NAPEO is the voice of the PEO industry. Professional employer organizations (PEOs) provide human resource services to small and mid-size businesses—paying wages and taxes under the PEO's EIN, offering workers' compensation and risk management services, and providing compliance assistance with employment-related rules and regulations. In addition, many PEOs provide HR technology systems and access to 401(k) plans, health, dental, and life insurance, dependent care, and other benefits. In doing so, PEOs help businesses take care of employees by enabling them to offer Fortune 500-level benefits at an affordable cost and providing access to experienced HR professionals. PEOs also help business owners and executives save time by taking administrative and HR related tasks off their plates, allowing them to focus on the success of their businesses.

Across the U.S., PEOs provide services to 200,000 small and mid-sized businesses, employing 4.5 million people. More than 21,000 California businesses – employing more than 470,000 people partner with a PEO.

**Concerns Regarding Competing, Inconsistent and Conflicting Regulation of AI and ADMT**

AI and the use of ADMT is an active area of focus by legislators and regulators in California. While we appreciate the attention brought to this important area (particularly in the employment context), we remain concerned that uncoordinated approaches to regulation of the same issue will result in competing, inconsistent and conflicting provisions that are difficult for businesses to implement.

For example, the California Civil Rights Department (CRD) recently approved regulations that seek to incorporate provisions specific to AI and ADMT into California's regulations regarding employment

discrimination – as their charge is to implement and enforce laws and regulations dealing with discrimination in employment. NAPEO was actively engaged in providing public comments to help improve and fine-tune CRD’s proposed regulations, which are set to take effect later this year.

Moreover, many of the same provisions of the CPPA’s proposed ADMT regulations (advance notice, impact assessments, opt-out rights) were considered by the legislature last year in AB 2930 (Bauer-Kahan) and are being considered this year in a reintroduced measure, AB 1018 (Bauer-Kahan). Other pending legislative measures seek to regulate the use of ADMT in the employment context, including SB 7 (McNerney).

Contributing to potential confusion for the employer community is the inclusion of employees and applicants for employment in a consumer protection scheme such as the CCPA/CPRA. Attempting to graft employment concepts into what at its core is a consumer protection law creates confusion and uncertainty for both employees and the regulated employer community. It also potentially doubles enforcement costs and burdens for employers as they attempt to comply with multiple regulatory schemes that all seek to address the same issue. For these reasons, we strongly supported the previous exemption in the CCPA/CPRA for employment and employees.

For these reasons, we believe that any proper regulation of AI and ADMT in the employment context is the purview of the legislature or the CRD. To the extent that CPPA’s proposed regulation will apply to the employment context, the result will be competing, inconsistent and conflicting regulation of ADMT that will be nearly impossible for the business community to reconcile.

### **Ongoing Concerns Regarding “Opt-Out” Provisions (Section 7221)**

The proposed regulations provide that a business must provide a consumer (employee/applicant) with the right to opt-out of the uses of ADMT. In the employment and hiring context, this could result in dynamics that are completely unworkable and costly and would compel businesses to forgo the use of ADMT altogether. For example, a business may use a resume screening tool to provide a first analysis of applications to determine which candidates meet the minimum job requirements and which do not, before hiring managers begin the process of human decisionmaking. Enabling an applicant to “opt-out” of this technology and require a human to perform this initial review of resumes would defeat any efficiencies provided by such ADMT in the first place.

The purported exception set forth in Section 7221(b)(1) to the “opt-out” requirement if the business provides a consumer with a method to appeal the decision to a “qualified human reviewer.” However, this is really no exception at all. Requiring a business to allow an applicant/employee to appeal to a “qualified human reviewer” is the same as requiring them to opt-out completely from the use of ADMT in the first place.

We appreciate the exception set forth in Section 7221(b)(2), which allows certain decisions to be exempt from the opt-out provisions where the business demonstrates that the ADMT is used solely for the business’s assessment, works for the business’s purposes and does not unlawfully discriminate based on protected characteristics. However, we feel that this exemption remains too narrow and will be a source of protracted litigation. The exemption only applies where the use of ADMT is used “solely for” specified purposes. In the employment context, the exemption also only applies for decisions related to the applicant’s ability to perform at work and whether to hire them. In order for such an exemption to be useful in the employment

context, it needs apply to all employment-related decisions and not be limited by terms that will result in needless litigation.

### **Miscellaneous Concerns**

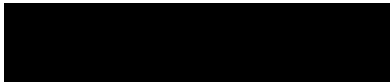
We also have concerns with some of the other specific provisions of the proposed regulations and therefore bring the following issues to your attention:

- **Risk Assessments for ADMT, AI, and Sensitive Personal Information (Section 7150(b)(1))** – “Significant risk” should be limited to the selling or sharing of “sensitive” personal information rather than all personal information. Without such a limitation, under the CCPA the use of tracking technologies such as cookies could be considered a significant risk to consumers for which businesses would need to conduct a risk assessment. We believe this is overbroad and unnecessary.
- **Risk Assessments for ADMT, AI, and Sensitive Personal Information (Section 7150(b)(2)(a))** – In the exception for employment purposes, we would recommend adding a catch-all for all employment-related purposes or language stating that such purposes “include, but are not limited to” the enumerated types of purposes. Limiting the list of employment-related purposes is too narrow and may exclude other legitimate employment-related purposes.
- **Pre-Use Notice Requirements and Responses to Requests for Access to ADMT (Sections 7220(d) and 7222(c))** – Both of these sections provide exceptions for information that is not required to be provided, either in the pre-use notification or the response to a request to access ADMT. We would suggest that these exceptions be expanded to include any confidential information or any other information that a business would not generally make available to the public.

### **Conclusion**

Once more, we appreciate your consideration of our comments on the proposed regulations related to ADMT and other issues. Should you have any questions with respect to the issues discussed herein, please do not hesitate to contact me at [hwalker@napeo.org](mailto:hwalker@napeo.org).

Respectfully,



Hannah Walker  
Senior Director, State Government Affairs  
NAPEO  
[hwalker@napeo.org](mailto:hwalker@napeo.org)



**Grenda, Rianna@CPPA**

---

**From:** dan.lewis@nprc-inc.org  
**Sent:** Monday, June 2, 2025 1:56 PM  
**To:** Regulations@CPPA  
**Subject:** National Payroll Reporting Consortium - Public comment on CCPA updates, cyber, risk, ADMT, and insurance regulations  
**Attachments:** NPRC Comments on CA CCPA Proposed Rules 06 02 2025.docx.pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

To Whom it May Concern, On behalf of NPRC please see the attached letter with our comments regarding CCPA updates. Please do not hesitate to contact me should you wish to discuss our comments further. Thank you for providing the opportunity to provide our feedback during this comment period.

Best regards,

Dan Lewis

President, NPRC



*National Payroll Reporting Consortium*

---

PO Box 850 ★ Henrietta, NY 14467-0850 ★ [www.NPRC-Inc.org](http://www.NPRC-Inc.org)

June 2, 2025

California Privacy Protection Agency  
2101 Arena Blvd.  
Sacramento, CA 95834

**Re: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations**

Dear Board Members,

On behalf of the National Payroll Reporting Consortium (NPRC), we appreciate the opportunity to comment on the proposed draft regulations updating the California Consumer Privacy Act (CCPA) and addressing cybersecurity audits.

NPRC is a non-profit trade association which represents payroll processing service providers that serve roughly 48% of the U.S. workforce. NPRC members provide human capital management (HCM) solutions, including payroll services and software systems that enable clients to manage their workforces. HCM software/platforms typically offer a wide range of functions, allowing clients to manage payroll, approve time-off requests, facilitate recruitment and hiring, conduct performance reviews, administer benefits, and offboard employees when they resign or are terminated. As HCM providers, our companies provide services involving the processing of personal data that would be impacted by the proposed regulations.

NPRC appreciates that the agency incorporated some of our recommendations in the revised proposed regulations; however, we continue to have concerns with the provisions addressing cybersecurity audits. More specifically, we are concerned as follows:

1. The proposed mandatory Cybersecurity Audit Requirement:
  - a. would impose an unnecessary financial and time burden on service providers without providing demonstrable benefit to California businesses.
  - b. fails to define the scope of the audit or to allow any objections, other than, "relevant information," which doesn't preclude requests for confidential or proprietary information of the service provider or third parties, or which might compromise the service provider's security practices.
  - c. fails to allow service providers to use prepared cybersecurity audit materials as the first step in responding to an annual audit, which saves everyone time and money and keeps service providers resources focused on cybersecurity issues and not document preparation, while not preclude California Businesses or their auditors from seeking additional information.

*ADP ★ AllianceHCM ★ ApexHCM ★ Asure Software ★ Check ★ CheckWriters ★ Dayforce  
Gusto ★ Heartland Payroll Solutions ★ Intuit ★ isolved ★ Netchex ★ Paychex ★ Paycom ★ Paycor  
Paylocity ★ PPI Business Services ★ PrimePay ★ Rippling ★ Symmetry Software ★ TriNet ★ UKG*



### **Proposed CCPA Mandatory Audit Requirement**

The regulations would require certain companies doing business in California ("California Business(es)") to perform a mandatory annual cybersecurity audit on their service providers (hereafter, "Proposed CCPA Mandatory Audit Requirement"). This requirement applies to service providers, such as NPRC members, if they process personal information of California consumers (including employees) and if such processing presents a "significant risk to consumers' security."

Under the Proposed CCPA Mandatory Audit Requirement, an annual audit of NPRC members would be mandatory so long as the auditor seeks relevant information. If adopted, NPRC members and other service providers should expect annual audit requests from either the California Businesses internal auditors or an engaged external audit firm. Either may lack incentives to appropriately cabin the scope of the audit as an in-house auditor typically would. The Proposed CCPA Mandatory Audit Requirement poses issues for NPRC members, or indeed any significant service provider that operates at scale, for the following reasons.

- 1. Volume of Audit Responses Unsustainable.** NPRC members are "one-to-many" providers of Human Capital Management (HCM) services with large numbers of customers. Companies with large client bases commonly provide standardized offerings. As part of this one-to-many model, NPRC members create, update, and provide cybersecurity collateral prepared in advance to customers to inform them of their cybersecurity programs. This collateral also includes information about the cybersecurity frameworks under which they operate; these may include, for example, SOC-2, ISO27001 and ISO27701 information.

The process of making this collateral available to clients helps substantially minimize the volume, time, and expense that NPRC members would otherwise face responding to individual client cybersecurity audits. Also, it avoids any risk related to breach of confidentiality, as well as information which could potentially compromise the security of the service providers system itself. For example, an auditor coming on site to audit on behalf of one client might see data of another, depending upon how systems are structured. That obviously creates a privacy risk; one that is avoided by provided vetted security-related collateral. Permitting a service provider to use prepared audit materials as a first line substitute does not preclude additional questions. Rather, it provides substantial relevant materials and saves time and money for both businesses and service providers.

The Proposed CCPA Mandatory Audit Requirement as currently drafted will impose substantial cost, effort, and expense on NPRC members without additional benefit to California Businesses or cybersecurity protection. What California Businesses need is information sufficient for them to have confidence in the cybersecurity practices of their service providers. As noted above, this can be provided via a standard set of written materials. Rather than require service providers to respond to specific bespoke audit requests from each customer's auditors, the CPPA should either (i) define a set of required information that service providers much provide to California Businesses regarding their cybersecurity practices or (ii) specifically allow service providers to provide prepared cybersecurity materials applicable to the California Businesses



scope of services, at least as the initial response, allowing the California Business to ask additional questions once they're reviewed the materials.

2. **Resource Burden; Diverts Resources Away from Other Cybersecurity Work.** In addition to the cost and volume discussed in Point 1, the predictable large volume of mandatory audits from California Businesses will unnecessarily shift the focus of valuable security resources at service providers away from their day-to-day cybersecurity work and turn them into document production experts. As noted above, NPRC members already provide customers with substantial cybersecurity collateral, consistent with our one-to-many approach in providing services. Requiring service providers to respond to individualized audit requests from clients would entail a shift in focus from day-to-day cybersecurity work to document production, without any corresponding benefit in transparency or protection.
3. **No Exceptions for Confidential/Proprietary Information.** The Proposed CCPA Mandatory Audit Requirement lacks an exception which allows a service provider to object to the disclosure of confidential, proprietary, or similar information in the audit. This could compromise the cybersecurity posture of companies such as NPRC members or disclose materials that are confidential or proprietary to them, and which provide them with a competitive advantage, including even trade secrets. At best, as drafted, the proposal will not encourage openness and cooperation. At worst, an unbridled disclosure requirement without guardrails for confidential and proprietary information could have a paradoxical effect on companies which continue to drive toward best-in-class security practices. If it is mandatory to disclose all cybersecurity methods, they may be less inclined to invest in competitive technologies if they must disclose their innovations without any carve-outs to every California Business which asks in a mandatory annual audit.

## Conclusion

Again, NPRC appreciates the opportunity to provide input on the proposed regulations and acknowledges the agency's thoughtful work in addressing these important issues.

We request that the CPPA reconsider the Proposed CCPA Mandatory Audit Requirement. Instead of requiring individualized annual audits, we recommend defining a standardized set of cybersecurity information that service providers must supply to California Businesses. This approach would balance the need for transparency and cybersecurity confidence with the practical realities faced by service providers. By reducing duplicative compliance burdens, this framework would allow service providers to focus resources on enhancing security practices rather than excessive administrative tasks. This will allow those one-to-many service providers with already-responsive cybersecurity audit materials to successfully satisfy their California Businesses without starting from scratch each time, causing the unnecessary economic harm described above. In doing so, it will be important to ensure that these information requirements appropriately protect the confidentiality of vendor information, per the point above.


Adopting these recommendations allows the CPPA to create a regulatory framework which advances its objectives of consumer protection and cybersecurity while avoiding unnecessary burdens on service providers. This balanced approach will provide the desired transparency to



California businesses, while maximizing resource availability for cybersecurity issues, and continued innovation and availability of workforce management tools which benefit California businesses and their employees.

If we can provide any additional information, please do not hesitate to contact me at 973.974.5273.

Sincerely,

 DocuSigned by:

  
Daniel Lewis  
President  
National Payroll Reporting Consortium

**Grenda, Rianna@CPPA**

---

**From:** Amit Elazari <amit@openpolicy.co>  
**Sent:** Monday, June 2, 2025 4:49 PM  
**To:** Regulations@CPPA; Panych, Vitaliy@CIO  
**Subject:** Public Comment on CPPA Updates, Cyber, Risk, ADMT, and Insurance Regulations  
**Attachments:** CPPA second revision comments (cyber) - OpenPolicy.pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Dear CPPA regulatory team,

OpenPolicy is thrilled to provide the attached comments as a follow-up on our previous comments, we would be delighted to discuss these at your earliest convenience.

Thanks, Amit

--



**Dr. Amit Elazari, J.S.D**  
**Co-Founder and CEO**

+1 (510) 813-9523  
[amit@openpolicy.co](mailto:amit@openpolicy.co)  
[openpolicy.co](http://openpolicy.co)

**May 28, 2025**

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
Via: [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

**OpenPolicy's Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations**

OpenPolicy appreciates the opportunity to submit these comments on the California Privacy Protection Agency's May 2025 revisions to the proposed CCPA regulations. OpenPolicy is a technology policy organization dedicated to democratizing access to policymaking for innovators and startups. We leverage data-driven insights to help companies engage with the government on critical cybersecurity and privacy issues. We are deeply committed to collaborative policymaking that strikes a balance between robust security and continued innovation. In this spirit, we commend the CPPA's diligent work on these regulations and the thoughtful incorporation of public feedback to refine the rules.

We applaud the CPPA for retaining a strong overall framework for consumer privacy and security in the revised regulations. Notably, the May 2025 draft preserves important **security measures such as multi-factor authentication (MFA) requirements and third-party identity verification services** within its provisions. By maintaining mechanisms such as phishing-resistant MFA and independent identity verification, the CPPA demonstrates a commitment to protecting consumer data through verified access controls and advanced authentication, which are critical defenses against fraud and unauthorized access.

At the same time, we note with concern that **certain key cybersecurity provisions were removed or narrowed** in the latest draft, presumably to reduce compliance burdens. In particular, the explicit reference to "zero trust architecture" was eliminated from the cybersecurity audit criteria. Zero Trust – the principle of granting the minimum necessary access and continually verifying identity and context – is widely recognized as a cornerstone of modern cybersecurity (indeed, U.S. federal agencies are required to meet specific Zero Trust objectives by FY 2024). While we understand the desire to streamline the rules, we believe the **underlying goals** of these removed provisions can still be achieved within the current regulatory text. Our comments, therefore, focus on **building upon what is still present**, recommending pragmatic enhancements and clarifications that reintroduce robust security practices in a manner compatible with the revised draft.



In the sections below, we provide feedback on **Article 5 (Verification of Requests)**, **Article 9 (Cybersecurity Audits)**, and **Article 10 (Risk Assessments)**. For each, we highlight retained elements that merit support and suggest improvements to reinforce cybersecurity safeguards without rehashing now-deleted language. Our tone is collaborative and forward-looking; we recognize the CPPA's efforts and offer constructive ideas to strengthen the regulations' security posture. We conclude by emphasizing OpenPolicy's readiness to assist in developing risk-based, future-proof solutions and by inviting continued engagement with the CPPA on these important issues.

## Article 5 – Verification of Consumer Requests

We are pleased to see that Article 5 continues to prioritize robust identity verification for consumer rights requests. The revised regulations maintain requirements for businesses to verify that a person making a request to delete, correct, or know personal information is the consumer about whom the information was collected (Section 7060(a)), and explicitly permit the use of third-party identity verification services as a means to accomplish this (Section 7060(c)(1)). Allowing reputable third-party verification services, so long as they meet CCPA standards, gives businesses flexibility to employ sophisticated tools for confirming identity, which can improve accuracy and reduce fraud. We also commend the rule that verification processes must scale in stringency with the sensitivity of the data in question (Section 7060(c)(3)(A)–(D)); this risk-based approach is essential to prevent unauthorized deletions or disclosures of highly sensitive personal information.

Moreover, we appreciate the ban on consumer-paid verification fees and onerous procedures. The regulations rightly prohibit businesses from charging consumers or forcing notarization as a condition of verification (Section 7060(e)), except in cases where reimbursement is required. This protects consumers from unnecessary barriers when exercising their rights. The rules also direct businesses to implement reasonable security measures to detect fraudulent verification activity (Section 7060(f)), a critical safeguard against bad actors attempting to exploit the privacy request process.

To further strengthen Article 5, OpenPolicy suggests the CPPA encourage or **clarify the use of multi-factor authentication (MFA) and modern cryptographic verification methods** in the verification process. While the regulations appropriately stop short of mandating any particular method, they define “multi-factor authentication” in Section 7001 and implicitly recognize its value. We encourage the adoption of advanced identity-proofing technologies that enhance security without increasing consumer burden. The regulations already allow the use of third-party services; the CPPA might consider clarifying that such services may employ innovative techniques like **cryptographic proofs or zero-knowledge proofs to verify identity attributes**. For instance, a service could cryptographically confirm that a

consumer's government ID is valid and matches their selfie, without retaining the ID image or exposing unnecessary data, thereby preserving privacy while authenticating identity. By validating credentials or attributes in a privacy-preserving manner (e.g., confirming "age over 18" or residence in California via zero-knowledge proof), businesses can reduce the collection of sensitive data during verification, aligning with the mandate in Section 7060(c)(2) to avoid collecting sensitive personal information unless needed. We believe the CPPA could highlight these emerging solutions in commentary or future guidance, signaling that the use of privacy-enhancing verification methods is encouraged so long as they meet the regulation's standards.

Additionally, we recommend explicitly addressing identity verification challenges associated with **AI agents and Non-Human Identities (NHIs)**, which include automated bots, service accounts, and API keys increasingly used to manage or process consumer information requests. Machine identities, particularly those embedded in automated AI workflows, often maintain persistent and elevated privileges, making them prime targets for attackers. These identities, if compromised, can significantly undermine identity verification processes. To mitigate these risks, we encourage the CPPA to clarify that identity verification requirements apply equally to both machine identities and human identities. Specifically, businesses should adopt **continuous, dynamic re-authorization methods that verify each API interaction or automated request in real-time**. Such an approach aligns well with the existing principle of scaling verification stringency based on risk, ensuring that AI-driven or automated identity interactions are continuously authenticated, and reducing the window of opportunity for unauthorized or fraudulent activity.

Further, we suggest reinforcing that fraud detection measures (Section 7060(f)) should be **dynamic and adaptive**. This recommendation is especially pertinent given the increasing sophistication of AI-driven attacks, where adversaries use AI to mimic legitimate consumer behavior, manipulate verification processes, or automate reconnaissance of verification vulnerabilities. Businesses should employ **dynamic risk scoring techniques** to assess contextual factors, such as geographic anomalies, behavioral patterns, or unusual request volumes, and automatically escalate verification stringency when risks are detected. Encouraging a **proactive risk-based stance** will ensure the verification framework remains resilient to evolving threats, including sophisticated AI-driven attacks.

Article 5's verification provisions are well-crafted to balance accessibility for consumers with strong security against imposters, including automated threats. OpenPolicy supports these measures and urges the CPPA to further emphasize advanced identity verification techniques, including MFA, cryptographic methods, privacy-preserving identity proofs, and dynamic re-authorization of machine identities, as best practices under the rule. By integrating these forward-looking, adaptive security strategies, the CPPA will future-proof

the regulations, enhancing trust and robustness in consumer rights requests while proactively addressing emerging risks associated with AI and machine identity exploitation.

## Article 9 – Cybersecurity Audits

OpenPolicy commends CPPA for retaining critical cybersecurity practices within Article 9, notably Multi-Factor Authentication (MFA), encryption of personal information at rest and in transit (Section 7123(b)(2)(B)), rigorous account management and access controls (Section 7123(b)(2)(D)), and mandatory security training and awareness (Section 7123(b)(2)(M)). These foundational practices set a strong baseline for organizational cybersecurity accountability. However, to further enhance resilience against increasingly sophisticated cyber threats, particularly those amplified by AI integration, we recommend embedding advanced cybersecurity principles and practices into Article 9.

Our primary concern in Article 9 is the removal of the explicit **“zero trust architecture”** provision from the list of security program components. In the initial draft, Section 7123(b)(2)(C) had called for businesses to implement a zero trust architecture (described as ensuring internal connections are encrypted and authenticated). The May 2025 modified text deletes this item. We understand that this change was intended to ease prescriptive burdens; however, we believe the *principles* of Zero Trust are too important to be lost. As noted, Zero Trust has become a foundational strategy in cybersecurity, moving beyond perimeter-based defenses to **assume no implicit trust** and constantly enforce least-privilege access. The White House’s federal Zero Trust strategy emphasizes that incremental improvements are not enough against modern threats and mandates a “dramatic paradigm shift” toward continuous verification of each user, device, and transaction<sup>1</sup>.

Rather than reinsert the exact “Zero Trust” language, we recommend that the CPPA incorporate the *spirit* of zero trust into the remaining provisions on access control. For example, Section 7123(b)(2)(D) already requires granular account privilege restrictions; this could be augmented with a comment that businesses should **continuously verify user access** and network integrity, and not rely solely on network location or single authentication events. In practice, this means encouraging measures like: **dynamic risk-based authentication** (re-authenticating or challenging users when context changes or anomalies are detected), **attribute-based access control (ABAC)** policies that evaluate a user’s role, device security, location, and other attributes before granting access, and network segmentation such that being “inside” the network grants no blanket trust.

---

<sup>1</sup> See Office of Management and Budget’s (OMB) Memorandum M-22-09 <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>

Additionally, businesses utilizing **hardened virtual appliances with tiered component positioning, assume-breach architecture, and internal service isolation**—where each service treats communications from other services as untrusted and communicates through cryptographically secure channels—should be explicitly recognized as meeting **zero-trust architecture standards**. Implementations that incorporate embedded security controls, sandboxed open-source libraries, and customer-owned encryption keys inherently satisfy zero-trust requirements through a comprehensive architectural design.

We suggest clarifying that **"restricting access to what is necessary"** includes ongoing monitoring of access sessions and automatic blocking of unauthorized lateral movement. By embedding these concepts, the regulation would still promote a Zero Trust mindset (continuous verification, least privilege by default) without necessarily using that exact term. This approach imposes minimal new burden—it clarifies how to implement existing listed controls rather than adding new ones—but importantly signals to businesses that simply having perimeter defenses is insufficient; they must actively reinforce internal defenses as well.

Likewise, in Section 7123(b)(2)(I) on network monitoring and defenses, we support the requirement for intrusion detection/prevention systems and would encourage the inclusion of **"real-time, continuous monitoring"** as an objective. Businesses should utilize modern security information and event management (SIEM) tools or extended detection and response (XDR) systems to audit their network and system logs for suspicious activity continuously. In today's threat environment, real-time visibility is crucial – waiting for a periodic check could miss fast-moving breaches. NIST's various guidelines on information security continuous monitoring highlight the value of automated tools that can audit system configurations and controls on an ongoing basis. We recommend that the CPPA emphasize that **continuous security monitoring** is a best practice that complements the annual audit. For instance, an **audit report could note how the company uses automated monitoring to maintain compliance between audits**, which would demonstrate proactive risk management. By encouraging continuous audit automation, the regulations can drive organizations toward more resilient, always-on security oversight, thereby catching issues early and reducing the likelihood of large breaches.

Recognizing the growing reliance on AI agents and automated systems, we recommend that Article 9 mandate governance of non-human identities, such as AI agents, API keys, automated bots, and service accounts. Each non-human identity should undergo continuous re-validation and context-aware risk assessments.

In modern IT environments, not only human users but also machines, applications, and AI agents often have credentials and access to data. These **non-human identities** (such as AI

agents, API keys, service accounts, robotic process automation bots, and AI algorithms operating autonomously) can be targets for attackers if not properly managed. We suggest that the CPPA clarify, under Section 7123(b)(2)(D) (Account Management), that businesses should include governance of **machine and service accounts** in their access controls. Each such account should have an identified owner, minimal privileges, and be rotated or revoked when no longer needed, similar to employee accounts. Additionally, as AI agents (such as autonomous software using personal data to make decisions) become more prevalent, companies should ensure that these agents are subject to the same access restrictions and monitoring as human users. For example, if an AI process is retrieving consumer data from a database, its access should be strictly scoped to the necessary fields and logged for audit purposes. We believe explicitly acknowledging **NHI security** in the audit criteria will future-proof the regulations, encouraging businesses to extend their identity and access management practices to all entities that can interact with personal information, whether human or not.

Further, Section 7123(b)(2)(B) appropriately requires encryption of personal information. We recommend that the CPPA encourage businesses to assess their cryptographic algorithms and **prepare for emerging threats such as quantum computing**. Quantum computers in the near future could potentially break widely used encryption (like RSA/ECDSA). Leading experts at NSA, NIST, and CISA have warned that actors might harvest encrypted data now to decrypt later when quantum capabilities arise, and they urge organizations to start planning for **post-quantum cryptography** transitions today<sup>2</sup>. In the context of CCPA audits, this means companies should inventory where they use long-lived encryption and follow NIST's work on quantum-resistant cryptographic standards.<sup>3</sup> We suggest adding to the encryption requirement that businesses **use strong, modern encryption algorithms and have a migration plan for quantum-resistant encryption**, aligning with already existing best practices in the field.

Additionally, recognizing businesses that employ file and disk **double encryption**—encrypting personal information at the application level with separate file-level keys and again at the operating system level for disk storage—should satisfy enhanced encryption standards. Similarly, businesses using TLS 1.3, AES-256 encryption, and FIPS 140-3 validated encryption standards should **meet advanced encryption-in-transit requirements**. These recommendations would modify CCPA regulations to acknowledge that comprehensive security platforms with **integrated encryption approaches provide superior consumer protection**, as opposed to requiring

---

<sup>2</sup> See Post-Quantum Cryptography: CISA, NIST, and NSA Recommend How to Prepare Now <https://shorturl.at/YFa9C>

<sup>3</sup> See NIST Post-Quantum Encryption Standards <https://shorturl.at/Y9CNt>



multiple separate and potentially less secure encryption implementations. Adopting these forward-looking measures ensures the long-term security of Californians' personal data, aligning with global best practices and reducing the risk and expense associated with future urgent encryption updates.

Regarding vendor and AI supply chain risk management, we are pleased to see the regulations (in the prior draft's Section 7123(b)(2)(O)) emphasize oversight of service providers, contractors, and third parties for CCPA compliance. We recommend extending this concept to explicitly include **security assessments of vendors**, particularly those handling personal information or providing critical technologies, such as AI systems. Many businesses rely on third-party software or AI models (for example, a fraud detection algorithm or a cloud analytics tool) that process consumer data. These supply chain elements can introduce vulnerabilities, as seen in incidents where compromised software updates or AI biases caused harm. The audit rule should encourage companies to **inventory their critical vendors and evaluate each vendor's security practices and reliability**. This could involve requiring vendors to complete security questionnaires, adhere to the business's cybersecurity standards, or obtain certifications. In particular, if a company uses third-party **AI or automated decision systems**, it should ensure that those systems are secure (free of malware, properly handling data) and that the vendor has controls in place to prevent unauthorized access to the shared data. By incorporating vendor risk management into the audit scope, the CPPA will help close a potential blind spot and ensure that outsourcing does not become a weak link in the protection of privacy.

Also, continuous monitoring should become a requirement to complement annual audits, particularly emphasized in Section 7123(b)(2)(I). Businesses must employ modern Security Information and Event Management (SIEM) systems or Extended Detection and Response (XDR) platforms to audit and monitor network and system logs continuously. Automated control testing, centralized log management, and proactive risk management strategies significantly enhance an organization's ability to detect, respond to, and mitigate fast-moving cyber threats.

## Article 10 – Risk Assessments

Conducting risk assessments is a proactive approach that compels businesses to **consider the potential harms to consumers** before and during high-risk processing. We commend the CPPA for retaining this requirement in the revised regulations, albeit with a narrowed scope and reduced procedural burden. By focusing risk assessments on truly significant decisions or sensitive profiling (as refined in the latest draft), the Agency ensures that effort is directed where it matters most – on processing that could seriously impact consumers' rights and freedoms.

Within the current structure, we recommend several steps to enhance the risk assessment process. Privacy and security risks are often intertwined. We suggest that businesses, when conducting a CCPA risk assessment, be explicitly encouraged to consider **cybersecurity risks posed by the processing activity** in addition to privacy impacts. For example, if a company is assessing a new system that uses sensitive personal information (like biometric data) to make automated decisions, the assessment should cover not only potential bias or fairness issues (privacy/ethics concerns) but also the security dimension e.g., could a breach of this system expose biometric identifiers, and what safeguards are in place to prevent that? The CCPA might clarify in Article 10 that a “risk assessment” should evaluate **the likelihood and severity of potential security incidents** associated with the processing, as well as misuse or unauthorized access. **Many modern privacy harms actually originate from security failures** (data breaches, malware, identity theft), so folding **security risk into the assessment will give a more holistic view of consumer risk**. We believe that this is entirely in line with the intent of the law, and it complements the cybersecurity audits (which look broadly at enterprise security) by focusing on the security of specific high-risk processing operations.

Building on our Article 9 comments, if a high-risk processing activity relies on third-party technology or data (for instance, using a third-party AI platform to analyze consumer data), the risk assessment should contemplate risks arising from that dependency. We recommend highlighting that **businesses should evaluate risks from their supply chain** in each relevant assessment – e.g., could the third-party fail to protect the data, or might the third-party’s model have hidden biases or security vulnerabilities? Including a section on vendor risk in the risk assessment template will prompt companies to ensure that their partners and service providers do not undermine consumer protection. The CCPA could even reference known standards or frameworks for such evaluations (like requiring that AI systems be subjected to a vendor security review, or checking if vendors adhere to industry security certifications). Thus, we suggest that **if a service provider plays a role in the high-risk processing, its controls must be factored into the risk analysis**.

Furthermore, the CCPA may consider encouraging businesses to utilize **automated or continuous risk assessment tools** as part of their compliance toolkit. Just as continuous monitoring helps in audits, continuous risk scanning can help flag issues between formal assessment cycles. Some organizations are adopting dynamic risk scoring systems that automatically update risk levels when conditions change (for example, if a dataset grows significantly or new threat intelligence emerges about a vulnerability in an AI algorithm). While not every business will have such tools, the CCPA could promote them in guidance, encouraging **real-time detection of changes in processing or in the threat landscape, which can trigger ad-hoc risk assessments** in addition to the required periodic ones. This ensures that risk management is **not a one-time checkbox but an ongoing practice**. It is



heartening that NIST and others have been developing catalogues of AI risks and suggesting continuous risk mitigation processes. Aligning California's approach with these evolving best practices will keep the regulations forward-compatible.

In closing, OpenPolicy **applauds the CPPA** for its leadership in crafting these regulations. This revision demonstrates a responsive approach – maintaining robust consumer protections and cybersecurity expectations, while streamlining areas that posed undue burden or legal uncertainty. **Thank you for your consideration of our comments.** We appreciate the CPPA's hard work and openness to feedback in this rulemaking process. Please do not hesitate to contact us for any clarification or further information. OpenPolicy looks forward to the successful finalization and implementation of the CCPA regulations, and to working with the Agency on promoting a secure, innovative, and privacy-respectful digital ecosystem.

**Sincerely,**

/s/ Dr. Amit Elazari

Dr. Amit Elazari  
CEO and Co-Founder of  
OpenPolicy

**From:** Pegah K Parsi <[REDACTED]>  
**Sent:** Monday, June 2, 2025 12:50 PM  
**To:** Regulations@CPPA  
**Subject:** Public Comment re: CPPA rules on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies  
**Attachments:** CPPA comment.pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Dear CPPA,

Please see the attached public comment for your consideration. The text is also pasted below for your convenience.

Thank you.

Best,  
Pegah Parsi  
-----

To the California Privacy Protection Agency Board:

My name is Pegah Parsi, and I serve as the Chief Privacy Officer at UC San Diego. While the University of California system does not fall directly under the CCPA/CPRA, I work closely with industry partners who are subject to it, and I spend much of my time evaluating how personal data is handled in both academic and commercial contexts. In addition to my professional role, I am a long-standing advocate for privacy rights and a committed member of the broader privacy community. I appreciate the opportunity to provide public comment on the CPPA's proposed rules regarding automated decisionmaking technologies (ADMTs) and AI.

As someone deeply invested in the responsible use of personal data, I urge the Board to continue prioritizing strong privacy protections for Californians, regardless of whether those protections affect conventional technologies or emerging AI systems. The CPPA is well within its mandate to regulate the use of personal data in any form, and it is both appropriate and necessary for the agency to address the unique risks associated with AI when it processes personal information.

Some critics suggest that addressing AI risks exceeds the agency's authority. However, regulating personal data—no matter the technology used—is firmly within the CPPA's purview. AI isn't exempt from this responsibility just because it's complex or politically sensitive. The focus should remain on the *processing* of personal data, not the buzzword status of the tool performing it.

We've also heard claims that regulation will stifle innovation. On the contrary, history shows that thoughtful, principled regulation creates the kind of public trust and accountability that innovation needs to thrive. California has long been a global leader not only in technology, but also in ethics and policy. The CPPA has an opportunity

to continue this leadership by establishing rules that reflect both technological awareness and a deep commitment to individual rights.

Below are several specific points I hope the Board will consider as you move toward finalizing these rules:

1. **Definition of ADMT:** The revised language creates unnecessary distinctions between tools that "replace" and those that "substantially replace" human decision-making. This could allow many influential systems to escape oversight simply because they involve minimal human involvement. The definition should be broadened to cover systems where human users heavily rely on ADMT outputs—even when they technically remain part of the loop.
2. **Behavioral Advertising:** Please retain a clear definition of "behavioral advertising" in the final rules. This is a critical and widely used application of personal data that should not be left ambiguous.
3. **Deepfakes:** Definitions matter. A clear definition of "deepfake" should remain in the rule to help identify this growing area of risk.
4. **Periodic Notices:** Long-term services often rely on a single consent point, which may not be remembered or remain meaningful over time. For high-impact data uses, periodic notices—like those used in financial or educational contexts—should be required.
5. **Section 7022:** The rule should ensure that deleted or de-identified data remains that way and is not quietly reintroduced through subsequent data pulls. This is critical, especially in light of data broker practices.
6. **Sections 7022 & 7023:** Consumers should continue to be informed of their right to file complaints with the CPPA, unless a request has been determined to be fraudulent.
7. **Privacy Audits:** The CPPA should encourage the inclusion of privacy assessments in standard audits, such as SOC 2 reports. A principle-based approach (e.g., the Privacy Trust Principle) would support consistency and accountability.
8. **Behavioral Advertising & Deepfakes:** These activities should be identified as presenting negative privacy impacts. This helps clarify the harms and guide appropriate risk mitigation strategies.
9. **Section 7153(b):** This section should be restored. When ADMTs are trained and made available to others, it is only reasonable that developers disclose key information about their data use and system limitations.
10. **Section 7157:** Businesses should be required to provide full, unredacted risk assessments to the CPPA or Attorney General when requested. Transparency here supports both enforcement and accountability.

Thank you for your thoughtful work on these regulations and for the opportunity to comment. I urge the Board to remain steadfast in your mission to protect Californians' privacy—especially in a time of rapid technological change.

Sincerely,  
Pegah Parsi, JD, MBA

June 2, 2025

California Privacy Protection Agency  
2101 Arena Boulevard  
Sacramento, CA 95834

To the California Privacy Protection Agency Board:

My name is Pegah Parsi, and I serve as the Chief Privacy Officer at UC San Diego. While the University of California system does not fall directly under the CCPA/CPRA, I work closely with industry partners who are subject to it, and I spend much of my time evaluating how personal data is handled in both academic and commercial contexts. In addition to my professional role, I am a long-standing advocate for privacy rights and a committed member of the broader privacy community. I appreciate the opportunity to provide public comment on the CPPA's proposed rules regarding automated decisionmaking technologies (ADMTs) and AI.

As someone deeply invested in the responsible use of personal data, I urge the Board to continue prioritizing strong privacy protections for Californians, regardless of whether those protections affect conventional technologies or emerging AI systems. The CPPA is well within its mandate to regulate the use of personal data in any form, and it is both appropriate and necessary for the agency to address the unique risks associated with AI when it processes personal information.

Some critics suggest that addressing AI risks exceeds the agency's authority. However, regulating personal data—no matter the technology used—is firmly within the CPPA's purview. AI isn't exempt from this responsibility just because it's complex or politically sensitive. The focus should remain on the *processing* of personal data, not the buzzword status of the tool performing it.

We've also heard claims that regulation will stifle innovation. On the contrary, history shows that thoughtful, principled regulation creates the kind of public trust and accountability that innovation needs to thrive. California has long been a global leader not only in technology, but also in ethics and policy. The CPPA has an opportunity to continue this leadership by establishing rules that reflect both technological awareness and a deep commitment to individual rights.

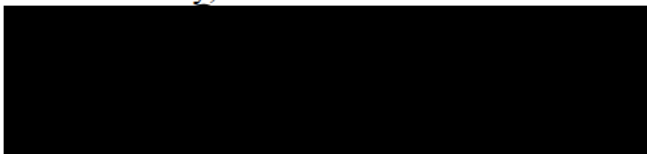
Below are several specific points I hope the Board will consider as you move toward finalizing these rules:

1. **Definition of ADMT:** The revised language creates unnecessary distinctions between tools that "replace" and those that "substantially replace" human decision-making. This could allow many influential systems to escape oversight simply because they involve minimal human involvement. The definition should be broadened to cover systems where human users heavily rely on ADMT outputs—even when they technically remain part of the loop.
2. **Behavioral Advertising:** Please retain a clear definition of "behavioral advertising" in the final rules. This is a critical and widely used application of personal data that should not be left ambiguous.

3. **Deepfakes:** Definitions matter. A clear definition of "deepfake" should remain in the rule to help identify this growing area of risk.
4. **Periodic Notices:** Long-term services often rely on a single consent point, which may not be remembered or remain meaningful over time. For high-impact data uses, periodic notices—like those used in financial or educational contexts—should be required.
5. **Section 7022:** The rule should ensure that deleted or de-identified data remains that way and is not quietly reintroduced through subsequent data pulls. This is critical, especially in light of data broker practices.
6. **Sections 7022 & 7023:** Consumers should continue to be informed of their right to file complaints with the CPPA, unless a request has been determined to be fraudulent.
7. **Privacy Audits:** The CPPA should encourage the inclusion of privacy assessments in standard audits, such as SOC 2 reports. A principle-based approach (*e.g.*, the Privacy Trust Principle) would support consistency and accountability.
8. **Behavioral Advertising & Deepfakes:** These activities should be identified as presenting negative privacy impacts. This helps clarify the harms and guide appropriate risk mitigation strategies.
9. **Section 7153(b):** This section should be restored. When ADMTs are trained and made available to others, it is only reasonable that developers disclose key information about their data use and system limitations.
10. **Section 7157:** Businesses should be required to provide full, unredacted risk assessments to the CPPA or Attorney General when requested. Transparency here supports both enforcement and accountability.

Thank you for your thoughtful work on these regulations and for the opportunity to comment. I urge the Board to remain steadfast in your mission to protect Californians' privacy—especially in a time of rapid technological change.

Sincerely,



Pegah Parsi, JD, MBA  
AIGP, CIPP/US/EU, CIPM  
Chief Privacy Officer, UC San Diego  
Of Counsel, XL Law Consulting

(organizations listed for identification purposes only)

## Grenda, Rianna@CPPA

---

**From:** Melissa O'Toole <motoole@pifc.org>  
**Sent:** Monday, June 2, 2025 2:10 PM  
**To:** Regulations@CPPA  
**Cc:** AAdey@pifc.org  
**Subject:** Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance  
**Attachments:** CPPA\_PIFC Comments on Updated Regulatory Package June 2025.pdf

### This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Good afternoon,

Attached, please find comments from the Personal Insurance Federation of CA (PIFC) and the National Association of Mutual Insurance Companies (NAMIC) regarding CCPA Updates, Cyber, Risk, ADMT and Insurance.

Thank you,

Melissa O'Toole  
Legislative and Communications Manager  
Personal Insurance Federation of CA  
motoole@pifc.org  
O: (916) 442-6646



Date: June 2, 2025

To: Members, California Privacy Protection Agency

Re: COMMENTS RELATED TO UPDATED PROPOSED REGULATIONS FOR CCPA REGULATORY PACKAGE.

Dear Members of the Board,

The Personal Insurance Federation of California (PIFC) is a statewide trade association that represents twelve of the nation's largest property and casualty insurance companies. These companies include State Farm, Farmers, Liberty Mutual Insurance, Progressive, Mercury, Nationwide, Allstate, CONNECT by American Family Insurance, Kemper, CSAA Insurance Group, Interinsurance Exchange of the Automobile Club (Automobile Club of Southern California), and GEICO, as well as associate members NAMIC and CHUBB. Collectively, these insurance companies write the majority of personal lines auto and home insurance in California.

We appreciate the movement made by the Consumer Privacy Protection Agency (the Agency) from the prior version of the regulatory package to the version updated for the May 1, 2025 meeting. While we believe that there is forward progress based on the new language, some concerns remain.

#### **Insurance Regulation**

With the Department of Insurance's sponsored bill, SB 354 (Limon) in process this year, we encourage the Agency to hold on further action for this regulation until clear delineation of authority on this space is settled. The insurance industry is subject to substantial oversight and the confusion that could be created by competing regulations would create an undue burden on an already struggling industry.

#### **ADMT**

We agree with Governor Newsom's April 23, 2025 letter to the Agency that the ADMT regulations are likely out of scope as they deal more with technology and innovation than privacy issues. As such we argue that these regulations should be substantially narrowed.

That being said, there are technical concerns with the ADMT regulations in that the limiting of the ADMT definition to decisions to technologies that "substantially replace[s]" human decision-making is an improvement, but still overly broad. As drafted, the language creates potential confusion with 7001(e), and more specifically the 7001(e)(3) carve out of what is excluded from ADMT, specifically tools like calculators and spreadsheets. Concern regarding tools of this nature has been raised from the beginning of discussion on the ADMT regulations.




This new drafting undermines the progress that has been made in this area prior to the May 1, 2025 version. We would encourage the Agency to consider using language more consistent with legislative proposals and the Colorado law passed in 2024 that addresses AI used to make “consequential decisions”: *“any technology that processes personal information and uses computation to replace or substantially replace human decisionmaking, where such decisionmaking results in a significant decision.”*

Finally, Section 7221 states that businesses must provide consumers with the ability to opt out of ADMT. This is overly restrictive and in some cases may be operationally infeasible, depending on how the business is using ADMT, especially given the breadth of the ADMT definition. The ability to opt-out should be tied to feasibility and the risk level of the ADMT use.


#### Other

The other concerns we share in this area apply broadly to the larger business community in the state, and as such will align ourselves with the comments of the California Chamber of Commerce. There continue to be substantial issues with the scope of the regulations as it related to the impact of the “profiling” definition at Section 7001(iii), the information an entity would be required to share under the “right to know” at Section 7024(e). We hope that the Agency will take the time to carefully tailor these areas to ensure workability and reasonability.

Sincerely,



Allison Adey  
Legislative Advocate  
Personal Insurance Federation of California



Christian John Rataj, Esq.  
Senior Regional Vice President  
National Association of Mutual Insurance Companies

**Grenda, Rianna@CPPA**

---

**From:** Julie Jensen <jujensen@proofpoint.com>  
**Sent:** Monday, June 2, 2025 4:45 PM  
**To:** Regulations@CPPA  
**Cc:** Jeff Reed  
**Subject:** Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations - Proofpoint  
**Attachments:** Public Comment on CCPA Updates Cyber Risk ADMT and Insurance Regulations\_20250602 Proofpoint.pdf

**This Message Is From an External Sender**

WARNING: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Dear California Privacy Protection Agency Board,

Please receive the attached Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations from Proofpoint, Inc. Thank you for your consideration.

Sincerely,

**Julie Jensen**

Director, Technology & Products Group - Legal

Mobile: [REDACTED]

This email is confidential and was prepared by a member of Proofpoint's legal department. It contains advice of counsel and may constitute privileged communication and/or attorney work product. If you are not the intended recipient, please delete immediately and contact the sender.

**proofpoint.**

June 2, 2025

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
400 R Street, Suite 350  
Sacramento, CA 95811  
[regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

Re: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations

Dear California Privacy Protection Agency Board,

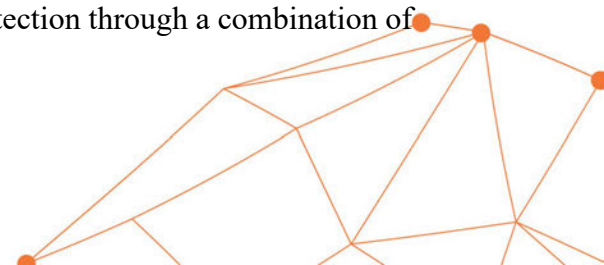
Proofpoint is a leading cybersecurity company that specializes in helping organizations protect against advanced cybersecurity threats and compliance risks such as identity theft, phishing, ransomware and business email compromise. As part of its cybersecurity and compliance services, Proofpoint provides and uses a global intelligence platform that gives businesses the critical visibility they need to maintain the security of their email, cloud applications, and other IT systems, and to respond to threats against the business and its employees.

Strong cybersecurity is essential for consumer privacy protection. Cybersecurity activities must be permitted to make proportionate use of personal information to manage security risks and incidents. We commend the Agency's efforts to craft regulations that effectively safeguard sensitive data and personal information from cyber threats. Our proposed additions to the draft regulations support these objectives by clarifying that the regulations should not be interpreted as discouraging businesses from using technologies designed to combat cybersecurity risks. To that end, our comments are limited to the following proposed modifications to the draft text:

- We recommend that **section 7001(ddd)(6)** clarify that a “significant decision” does not include detecting and preventing cyber security incidents or resisting malicious, deceptive, fraudulent, or illegal activity.
- We recommend that **section 7123(c)(8)(A)** clarify that network monitoring and defense components include the deployment of phishing, email fraud, and other business email compromise technologies.
- We recommend that **section 7123** clarify that the Cybersecurity Audit does not require a regulated business to disclose its trade secrets.

### **Sound Cybersecurity Practices are a Crucial Component of Information Privacy and Data Security**

Cybersecurity is a crucial component of information privacy and data security. To promote the important objective of consumer data protection, the regulations encourage businesses that process consumer's personal information to deploy effective security measures. Proofpoint's email threat detection and data security governance services provide such protection through a combination of



advanced threat detection, policy enforcement, and data loss prevention to protect its customers and their end users from malicious cyber threats. This includes threats that originate from outside (e.g., phishing, malicious attachments and URLs, business email compromise) and inside (e.g., negligent or malicious misuse of company data, including personal data) an organization.

Our comments aim to support these goals by clarifying that certain cybersecurity technologies are effective because of their use of automated decision-making and artificial intelligence. Such technologies are not the enemy of consumer data privacy and security but one of their most important allies.

**Section 7001(ddd)(6): Clarify that “Significant Decision” Excludes Detecting and Preventing Security Incidents, and Resisting Malicious, Deceptive, Fraudulent, or Illegal Activity**

Section 7001(ddd) defines “significant decision” and section 70001(ddd)(6) states that significant decisions “do[] not include advertising to a consumer.” We propose clarifying that a significant decision also does not include using technologies that combat cybersecurity threats by drafting section 7001(ddd)(6) to state the following:

Significant decision does not include advertising to a consumer, [detecting and preventing security incidents, and/or resisting malicious, deceptive, fraudulent, or illegal activity](#).

We propose this clarifying language to ensure that regulated businesses are not discouraged from using critical cybersecurity technologies to safeguard the personal and sensitive data they possess. Cybersecurity technology is advancing at a remarkable pace. Many of the platforms and services, including those offered by Proofpoint, employ powerful tools and technology that safeguard data, which often include artificial intelligence. The proposed regulations should clarify that making a “significant decision” does not include the use of these tools to combat cyber threats.

Furthermore, we propose this language to advance the core objectives of the privacy regulations — safeguarding California consumer privacy and security. Achieving this requires strong cybersecurity practices, which privacy regulations should actively support rather than hinder.

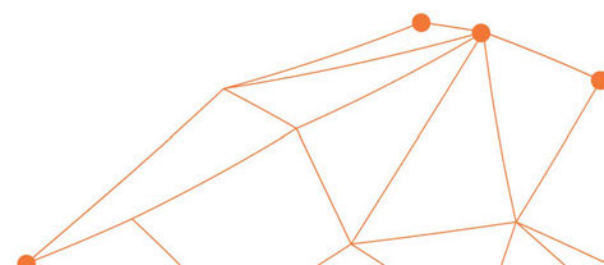
Finally, we recommend this language because the regulation already uses similar language elsewhere to describe technologies that combat cybersecurity threats and safeguard data.<sup>1</sup>

**Section 7123: Clarifying How the Cybersecurity Audit Requirements Promote Sound Cybersecurity Practices**

Section 7123 of the proposed regulations would define the scope of cybersecurity audits and identify the material required to be included in audit reports. We recognize the Agency’s careful attention to these important provisions. Our proposals reinforce that sound cybersecurity practices

---

<sup>1</sup> See e.g., §§ 7027(m)(2) and (3), 7050(a)(4), 7220(c)(2)(B).



are necessary for businesses to achieve the fundamental purpose of the privacy regulations, protecting sensitive and personal data.

### **1. The Cybersecurity Audits Should Encourage the Use of Tools that Combat Business Email Compromise and Email Fraud**

Some of the most common cyber threats (e.g., business email compromise and phishing) exploit human vulnerabilities. However, these threats are not explicitly addressed in the proposed regulations' cybersecurity audit scope. Including them in the audit criteria would encourage broader adoption of services and platforms designed to protect organizations and their employees from falling victim to targeted attacks.

To this end, we recommend that businesses be encouraged to use email threat security services by explicitly including them in the cybersecurity audit assessment requirement. Thus, we propose that Section 7123(c)(8)(A) be amended as follows:

- (A) Technologies, such as bot-detection, intrusion-detection, ~~and~~ intrusion-prevention, exfiltration detection, exfiltration prevention, and email fraud, phishing and other business email compromise prevention, which a business may use to detect unsuccessful login attempts, monitor the activity of authorized users, detect and prevent malicious email, protect a business's cloud applications, social media accounts and mobile devices, and detect and prevent unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information;

### **2. The Cybersecurity Audits Should Not Cause Businesses to Expose their Trade Secrets**

The proposed regulations recognize that modern cybersecurity technologies often include formulas, patterns, compilations, programs, devices, methods, techniques, or processes that, to protect their status as trade secrets, cannot be disclosed. For example, section 7220(d)(1) states that a business is not required to include trade secrets in its pre-use notice, and section 7222(c) states that a business is not required to include trade secrets in its response to a consumer's request to access ADMT.

A business's trade secrets are often its most important and valuable assets. Unauthorized disclosure of these trade secrets could disrupt business operations and undermine a cybersecurity provider's ability to successfully protect its customers and their end users from cyberattacks, ultimately harming the very people the regulations seek to protect.

We therefore recommend that Section 7123 add a clarifying section (g) to provide as follows:

§ 7123(g) In creating the cybersecurity audit and report required by this Section 7123, neither a business nor a service provider is required to disclose



information relating to Trade Secrets, as defined in Civil Section 3426.1, subdivision (d).

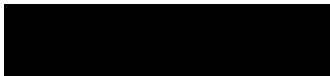
## **Conclusion**

As a cybersecurity company dedicated to helping organizations protect against advanced cybersecurity threats and compliance risks, we believe that strong cybersecurity is essential for consumer protection, and it is critical to ensure cybersecurity activities are permitted to make proportionate use of personal information to manage security risks and incidents. By incorporating our proposed language, the Agency can help ensure California companies and their consumers remain adequately protected against malicious cyber-attacks and security risks while simultaneously working to ensure consumer privacy protections.

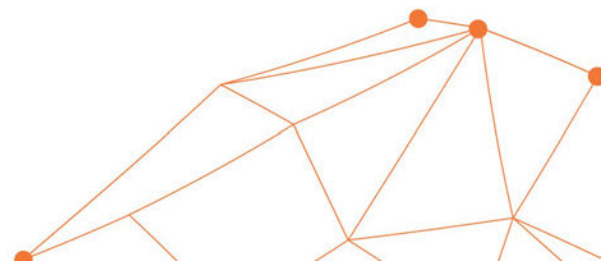
To help ensure that cybersecurity companies such as Proofpoint continue protecting the businesses and consumers of California, we request an in-person or virtual meeting to further discuss our proposed clarifications and additions to the draft regulations.

We thank you for your consideration and look forward to discussing these matters with you directly.

Sincerely,



Jeff Reed  
VP, Associate General Counsel  
Proofpoint, Inc.





**Grenda, Rianna@CPPA**

---

**From:** Jay Bajwa <JSingh@rmaintl.org>  
**Sent:** Monday, June 2, 2025 4:28 PM  
**To:** Regulations@CPPA  
**Cc:** David Reid  
**Subject:** Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations  
**Attachments:** RMAI Comments to CPPA Modifications to Proposed Regulations.docx

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

California Privacy Protection Agency:

Attn: Legal Division - Regulations Public Comment.

The Receivables Management Association International (“RMAI”) appreciates this opportunity to submit the following comments on the proposed rules updating the California Consumer Privacy Act (“CCPA”), and regarding cybersecurity audits, risk assessments, and automated decisionmaking technology (“ADMT”).

Best,  
Jay



**Jay Bajwa** | Legislative & Public Relations Specialist  
Receivables Management Association International

**Direct:** 916-719-9237 | **Office:** 916-482-2462

**Email:** [jsingh@rmaintl.org](mailto:jsingh@rmaintl.org) | **Web:** [www.rmaintl.org](http://www.rmaintl.org)

1050 Fulton Avenue, Suite 120, Sacramento, CA 95825





June 2, 2025

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
400 R Street, Suite 350  
Sacramento, CA 95811

Submitted via email: [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

**Re: CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations**

California Privacy Protection Agency:

The Receivables Management Association International (“RMAI”) appreciates this opportunity to submit the following comments on the proposed rules updating the California Consumer Privacy Act (“CCPA”), and regarding cybersecurity audits, risk assessments, and automated decisionmaking technology (“ADMT”).

## **I. BACKGROUND**

RMAI is a nonprofit trade association that represents over 600 companies that purchase or support the purchase of performing and nonperforming receivables on the secondary market. RMAI member companies include banks, credit unions, non-bank lenders, debt buying companies, collection agencies, law firms, brokers, and industry-related product and service providers.

Since 2013, RMAI’s Receivables Management Certification Program (“Certification Program”)<sup>1</sup> has set rigorous industry standards that are designed to meet or exceed the requirements of state and federal law for the protection of consumers. While the program was first designed to certify debt buying companies, it has expanded to include certifications for law firms, collection agencies, and vendors. Currently, over 500 businesses and individuals hold these internationally respected certifications. Additionally, all the largest debt buying companies in the United States are RMAI certified, and it is estimated that approximately 80 to 90 percent of all charged-off receivables that have been sold on the secondary market are owned by an RMAI certified company. RMAI’s Certification Program and its Code of Ethics<sup>2</sup> are the “gold standard” within the receivables management industry.

Notably, the Certification Program includes, among other things, the following requirements:

- Cyberinsurance Coverage;<sup>3</sup>

---

<sup>1</sup> Receivables Management Association International, *Receivables Management Certification Program*, Ver. 10 (Mar. 1, 2023), available at <https://perma.cc/7D8Q-KGVC>.

<sup>2</sup> Receivables Management Association International, *Code of Ethics* (August 13, 2015), available at <https://perma.cc/BM6J-USG>.

<sup>3</sup> Certification Standard A2.

- Data security policies and procedures compliant with state and federal law to ensure the safe and secure storage of consumer data;<sup>4</sup>
- Data breach policies and procedures;<sup>5</sup>
- Disaster recovery plans;<sup>6</sup>
- Secure and timely disposal of consumer data compliant with applicable laws;<sup>7</sup>
- Restrictions on the use of social media consistent with Regulation F; 12 CFR § 1006.22(f)(4);<sup>8</sup>
- Remote work policies and procedures to ensure the security and confidentiality of consumer data and requiring in-person training for remote employees covering, in part, privacy, confidentiality, monitoring, and security;<sup>9</sup>
- Policies and procedures designed to prevent discriminatory practices, including through the use of computer algorithms and artificial intelligence;<sup>10</sup>
- The exercise of due diligence prior to the transmission or receipt of consumer data, including examination of the recipient’s data security measures.<sup>11</sup>

## II. RMAI COMMENTS

### ARTICLE 1. GENERAL PROVISIONS

#### § 7001. Definitions

**Subsection (t):** This subsection provides a proposed definition for “information system.” Conceptually, this is similar to the definition of “information system” contained in the Federal Trade Commission’s (“FTC’s”) Gramm-Leach-Bliley Act (“GLBA”) Safeguards Rule:

Information system means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information containing customer information or connected to a system containing customer information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems that contains customer information or that is connected to a system that contains customer information.<sup>12</sup>

Similarly, in its cybersecurity regulations, the New York State Department of Financial Services (“NY DFS”) defines “information system” as:

---

<sup>4</sup> Certification Standard A7.

<sup>5</sup> Certification Standard A7(g).

<sup>6</sup> Certification Standard A7(h).

<sup>7</sup> Certification Standard A7(i).

<sup>8</sup> Certification Standard A19.

<sup>9</sup> Certification Standard A21.

<sup>10</sup> Certification Standard A22.

<sup>11</sup> Certification Standard B3.

<sup>12</sup> 16 C.F.R. § 314.2(j).

Information system means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.<sup>13</sup>

However, the CPPA's proposed text's definition deviates from the GLBA Safeguards and NY DFS' definitions by failing to specify electronic information. The following revisions would add clarity to the proposed text's definition and promote consistency among relevant definitions:

(v) "Information system" means ~~the~~ a discrete set of electronic information resources (e.g., network, hardware, and software) organized for the processing of personal information or that can provide access to personal information. The business's information system includes the resources organized for the business's processing of personal information, regardless of whether the business owns those resources.

**Subsection (ddd):** This subsection provides a proposed definition for "significant decision," which 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."

RMAI respectfully suggests that the application of this definition should be limited to businesses that are offering, or from which a consumer is seeking, such services. For example, a business to which a consumer owes an obligation may choose to furnish information regarding the obligation to credit reporting agencies. As currently drafted, the business could be considered to be making a significant decision if the furnishing positively or negatively affects the consumer's credit score and the provision or denial of financial or lending services by *other* businesses. The business furnishing the information cannot, however, reasonably anticipate the effect or outcome.

Therefore, RMAI recommends the following modification:

(ddd) "Significant decision" means a decision by a business that results in the business's provision or denial of financial or lending services, housing, education enrollment or opportunities, employment or independent contracting opportunities or compensation, or healthcare services.

## **ARTICLE 9. CYBERSECURITY AUDITS**

### **§ 7121. Timing Requirements for Cybersecurity Audits and Audit Reports.**

---

<sup>13</sup> 23 NYCRR 500.1(i).

RMAI appreciates the CPPA's recognition that businesses will need sufficient time to establish processes and implement procedures to conduct the cybersecurity audits contemplated by the proposed regulations. Likewise, RMAI appreciates the CPPA's recognition that smaller organizations may face higher obstacles in preparing for compliance and therefore more time is appropriate. However, in contrast to the prior draft, the proposed revisions introduce complexity and potential confusion as to when a business is required to comply and when the first audit must be conducted and for what time period.

To the extent that the CPPA retains the thresholds set forth in the revised § 7121, RMAI recommends that CPPA revise § 7121 to avoid potential conflict with § 7120, particularly for proposed § 7121(a)(3), and clarify that the business must first meet the criteria of § 7120, *i.e.*, for Section 7121(a)(3), the business meets the threshold set forth in Civil Code § 1798.140(d)(1)(A) and the business' annual gross revenue for 2028 was less than fifty million dollars.

### **§ 7122. Thoroughness and Independence of Cybersecurity Audits.**

**Subsection (a):** This subsection, in part, describes the procedures and standards that must be used by an auditor and specifically four organizations that have adopted acceptable standards. RMAI believes this is too limited as other organizations may also have relevant standards and suggests the following modification:

Every business required to complete a cybersecurity audit pursuant to this Article must do so using a qualified, objective, independent professional ("auditor") using procedures and standards accepted in the profession of auditing, such as procedures and standards provided or adopted by the American Institute of Certified Public Accountants, the Public Company Accountability Oversight Board, the Information Systems Audit and Control Association, ~~or~~ the International Organization for Standardization, [or similar organizations](#).

### **§7123. Scope of Cybersecurity Audit and Audit Report.**

Subsection (c)(1)(A): This subsection describes the components a cybersecurity audit must assess. Authentication must include "[m]ulti-factor authentication (including multi-factor authentication that is resistant to phishing attacks for employees, independent contractors, and any other personnel, service providers, and contractors)."

The requirement is conceptually similar to GLBA Safeguards Rule which requires financial institutions, as defined, to "[i]mplement multi-factor authentication for any individual accessing any information system, unless [the] Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls."<sup>14</sup>

The proposed text provided by the CPPA, however, introduces uncertainty as it does not specify when multi-factor authentication is required, *i.e.*, when accessing any information system as

---

<sup>14</sup> 16 C.F.R. § 314.4(c)(5).

defined in § 7001(t)). Accordingly, the proposed revisions below would avoid this confusion and promote clarity:

(A) Multi-factor authentication (including multi-factor authentication that is resistant to phishing attacks for employees, independent contractors, and any other personnel, service providers, and contractors) [for any individual accessing an information system](#);

## **ARTICLE 11. AUTOMATED DECISIONMAKING TECHNOLOGY**

RMAI supports throughout Article 11 the removal of training uses of ADMT.

### **§ 7200. Uses of Automated Decisionmaking Technology.**

**Subsection (b):** This subsection states any business that uses ADMT for a significant decision prior to January 1, 2027, must be in compliance with the requirements of this Article no later than January 1, 2027. A business that uses ADMT on or after January 1, 2027, must be in compliance with the requirements of this Article any time it is using ADMT for a significant decision.

RMAI believes that this provision should apply only to businesses that use ADMT as the sole basis to make a significant decision concerning a consumer. Additionally, RMAI believes an effective date of April 1, 2030, similar to the requirement under § 7121, would help ensure businesses are able to meet the requirements. Accordingly, RMAI suggests the following language:

(b) A business that uses ADMT [as the sole basis](#) for a significant decision prior to ~~January 1, 2027~~ [April 1, 2030](#), must be in compliance with the requirements of this Article no later than ~~January 1, 2027~~ [April 1, 2030](#). A business that uses ADMT on or after ~~January 1, 2027~~ [April 1, 2030](#), must be in compliance with the requirements of this Article any time it is using ADMT for a significant decision.

### **§ 7220. Pre-use Notice Requirements.**

**Subsection (a):** This subsection requires notice to consumers of the use automated decisionmaking technology (“ADMT”) if a business is using it as set forth in § 7200.

RMAI suggests that the pre-use notice requirements should not apply to a business that only uses ADMT with respect to personal data that is exempt from the CCPA pursuant to § 1798.145, e.g., GLBA, HIPAA, FCRA, etc. Placing this requirement on such businesses will likely lead to consumer confusion while imposing additional compliance burdens on businesses without any countervailing benefits for consumers.

**Subsection (c)(3):** This subsection specifies the information that must be included with respect to the consumer's right to access ADMT and how the consumer can submit their request to access ADMT.

RMAI believes as outlined below in its comments to §7222, that access to ADMT would prove to be very problematic and harmful to both businesses and consumers.

**Subsection (c)(5):** This subsection provides additional information on how the ADMT works to make a significant decision about consumers, and how significant decisions would be made if a consumer opts out, in a plain language explanation.

RMAI believes this provision should be deleted, as it will require a business to distill complex AI Models into a plain language explanation which will likely result in the meaning of the explanation losing value. Additionally, even with the fraud prevention language found in §§ 7222(d), 7221, and 7222, this could provide a roadmap for fraudsters to target.

**Subsection (d):** This subsection provides exceptions to what must be included in the Pre-use Notice.

RMAI is largely in support with this section though it believes that the expansiveness of (c)(5) will make it difficult for businesses to accurately assess what information falls into these enumerated categories.

## **§ 7222. Requests to Access ADMT.**

**Subsection (b):** This subsection specifies the information that must be included in a response to a consumer's request to access ADMT.

RMAI believes the potential costs to businesses of fulfilling these requests are likely to be significant and will impose substantial burdens on businesses to develop responses that meet the level of individualized explanation required by the regulation.

Receiving a large volume of requests could be crippling to a business' operations. In many cases, even the threat of a large volume of such requests could deter companies from investing the time and resources necessary to adopt ADMTs and prevent them from realizing the benefits in terms of quality and efficiency that ADMTs can offer both to businesses and consumers.

## **III. CONCLUSION**

RMAI appreciates the opportunity to submit its comments concerning the modifications to the proposed regulations. Please do not hesitate to contact RMAI's General Counsel, David Reid, at [dreid@rmaintl.org](mailto:dreid@rmaintl.org) or (916) 482-2462 for clarification on RMAI's comments or if RMAI can be of further assistance.

Sincerely,



---

David Reid  
General Counsel & Senior Director of Government Affairs  
Receivables Management Association International



**Grenda, Rianna@CPPA**

---

**From:** Justine Murray <jmurray@sdchamber.org>  
**Sent:** Monday, June 2, 2025 12:48 PM  
**To:** Regulations@CPPA  
**Subject:** SDRCC Comments on Proposed Rulemaking  
**Attachments:** SDRCC CPPA Proposed Rule Making 6.2.25.pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Please see the attached comment letter from the San Diego Regional Chamber of Commerce regarding CPPA's proposed rulemaking

**Justine Murray**

Executive Director of Public Affairs

**San Diego Regional  
Chamber of Commerce**

c: [REDACTED]  
[SDChamber.org](https://www.senchamber.org)





402 West Broadway, Suite 1000  
San Diego, CA 92101-3585  
p: 619.544.1300

[www.sdchamber.org](http://www.sdchamber.org)

June 2, 2025

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
2101 Arena Blvd.  
Sacramento, CA 95834

**RE: Public Comment on CCPA Proposed Rulemaking**

Dear California Privacy Protection Agency Board:

On behalf of the San Diego Regional Chamber of Commerce, I am writing to address our concerns regarding the proposed regulations for Automated Decisionmaking Technology (ADMT) and Risk Assessment Regulations. The Chamber represents over 2,000 member businesses and over 300,000 jobs, with a mission to make the San Diego region the best place to live and work. San Diego is home to some of the state and country's top tech companies, and we have significant concerns regarding the proposed draft rulemaking actions because California is a global leader in AI research, development, and deployment. Additionally, our region is poised to become a hub for AI technology, given its position as a leader in the state's innovation economy.

While the new draft includes some helpful changes, the proposed rules remain overly broad, costly, and misaligned with the agency's core consumer privacy mission. If adopted in their current form, these regulations would impose sweeping and unnecessary burdens on businesses across the state, while doing little to meaningfully improve consumer privacy.

Even under this revised version, the agency's estimate shows that California businesses would face more than \$1.2 billion in compliance costs during the first year alone. This staggering figure underscores the breadth and burden of the regulations that remain. Companies of all sizes would be forced to conduct extensive audits of internal software and systems, overhaul existing processes to offer consumers and workers new opt-out rights, and produce detailed public-facing disclosures about business operations, regardless of whether any real privacy risk exists. These costs are especially difficult to justify given the minimal privacy gains they appear to achieve.

The regulations also continue to define "automated decisionmaking" so broadly that they would apply to common, decades-old tools that are in no way autonomous or invasive. Even with changes to the definition, the current draft would still capture basic software systems used for everyday functions like analyzing employee performance, tracking safety metrics, or determining eligibility for routine bonuses. In such cases, the software functions solely as a decision-support tool for human managers, rather than as an autonomous decision-maker. Yet, these tools would still fall under the agency's regulatory authority, triggering extensive new requirements simply because they assist human judgment. That is not what voters intended when they approved Proposition 24 to safeguard consumer privacy.

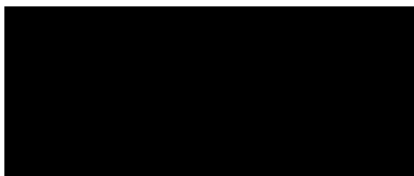
In addition, while the regulations purport to target cutting-edge technologies with real privacy implications, such as facial recognition or emotion detection tools, they instead sweep in a vast range of routine, low-risk business activities. For example, even automated systems that calculate small performance-based incentives or attendance-based bonuses could be subject to regulation. There is no identified privacy harm posed by such systems, yet they would be treated as if they represent the same kind of risk as unregulated AI tools with no human oversight. This disconnect reveals the underlying flaw in the agency's approach: rather than targeting high-risk, high-impact use cases, the rules cast an unnecessarily wide net over ordinary business practices.

We are particularly concerned that the revised draft removes the common-sense exemption for fraud prevention systems. Businesses depend on automated tools to detect and stop fraudulent or malicious activity—tools that are essential to consumer protection and system security. Under the current proposal, even these systems could be subject to opt-out rights, undermining their very purpose. The prior version of the regulations wisely exempted anti-fraud technologies from opt-out requirements, and we urge the agency to restore that exemption to avoid jeopardizing vital security measures.

While we recognize the agency's efforts to respond to feedback, the current proposal remains far too expansive. These regulations still risk pulling in virtually any system that processes data, regardless of whether it poses real privacy concerns. By trying to regulate everything from bonus calculations to employee attendance tracking, the agency is overstepping its consumer privacy mandate and veering into territory traditionally left to employment and business operations policy. We echo calls from Governor Newsom and bipartisan legislators to narrow the scope of these regulations and refocus on true privacy harms.

California's businesses remain committed to protecting the privacy of their customers and employees. We urge the agency to adopt a more targeted, risk-based approach that protects consumers without stifling innovation or burdening routine operations. As currently written, these regulations would cause significant economic disruption without delivering commensurate benefits to privacy. The Chamber respectfully requests that the agency significantly revise the proposed rules to better align with the voter-approved mission of the California Privacy Protection Agency.

Sincerely,



Justine Murray  
Executive Director of Public Affairs  
San Diego Regional Chamber of Commerce

CC: Ashkan Soltani, Executive Director, CPPA

**Grenda, Rianna@CPPA**

---

**From:** Jake Parker <jparker@securityindustry.org>  
**Sent:** Monday, June 2, 2025 4:57 PM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance  
**Attachments:** SIA Comment on CCPA Modifications to Proposed Cyber, Risk, ADMT, and Insurance Regulations.pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Please see attached SIA's comments on the Modified Proposed Rules, published May 9, 2025.

Thank you!

**Jake Parker**

Senior Director, Government Relations  
Security Industry Association (SIA)  
202-365-5249  
[jparker@securityindustry.org](mailto:jparker@securityindustry.org)

Confidentiality Note: This message and any attachments may contain legally privileged and/or confidential information. Any unauthorized disclosure, use or dissemination of this e-mail message or its contents, either in whole or in part, is prohibited. The contents of this email are for the intended recipient and are not meant to be relied upon by anyone else. If you are not the intended recipient of this e-mail message, kindly notify the sender and then destroy it.



June 2, 2024

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
2101 Arena Blvd.  
Sacramento, CA 95834

**Re: May 9 Notice of Modifications to Proposed Cyber, Risk, ADMT, and Insurance Regulations**

The Security Industry Association (SIA) appreciates the opportunity to submit comments on modifications to the text of proposed rules to implement the statutory provisions of the California Consumer Privacy Act (CCPA) regarding cybersecurity audits, risk assessments and automated decision-making.

SIA represents over 200 companies headquartered in California that provide products essential to protecting the physical safety of people property, businesses, schools, and critical infrastructure in the state and throughout the nation. This includes access control, alarm systems, security camera systems, screening and detection equipment, and many other applications. Our member companies are deeply committed to safeguarding personal information and protecting people through their own business practices as well as the design of the products and services they provide that collect and process information.

**SUMMARY**

The California Privacy Protection Agency (“CPPA” or “Agency”) is seeking comments<sup>1</sup> on modifications to the text of its proposed rules addressing automated decision-making technology (“ADMT”), cybersecurity audits and risk assessments, among other things, (collectively, “Modified Proposed Rules”).<sup>2</sup>

The Agency has made significant improvements in its modifications to the proposal to establish a more risk-based approach that is also more harmonized with other AMDT frameworks. Yet, there are still important edits that are needed to ensure that Californians are not cut off from important technology use cases that can protect them, and to ensure that the new rules are drafted in a consistent, targeted manner that is not overly broad.

Accordingly, building on the positive updates in the Modified Proposed Rules, and before finalizing the new rules, the Agency should:

- (1) Restore the security, fraud prevention and safety exception to ADMT opt-out requirements,<sup>3</sup> and appropriately extend this exemption to risk assessment requirements.
- (2) Modify risk assessment requirements to ensure they are targeted to high-risk circumstances.
- (3) Remove requirements creating individual liability for attestation and certifications regarding businesses’ Cybersecurity Audits and Risk Assessments.

Taking these steps will allow the regulations to appropriately manage risk, while best promoting critical security and safety use cases.

---

<sup>1</sup> [https://cppa.ca.gov/regulations/pdf/ccpa\\_updates\\_cyber\\_risk\\_admt\\_notice.pdf](https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_notice.pdf).

<sup>2</sup> Cal. Civ. Code § 1798.185(a)(15)-(16).

<sup>3</sup> As detailed below, the new rules should be limited in scope to ADMT and should not sweep in other forms of “automated processing.” However, to the extent the Agency retains its use of the term “automated processing,” the safety and security exemption should apply equally to that term.

## RECOMMENDATIONS

**Recommendation 1: The “security, fraud prevention, and safety” exemption should be expanded to apply to all portions of the Modified Proposed Rules related to ADMT and automated processing.**

The Modified Proposed Rules remove the exemption for “security, fraud prevention, and safety” from the opt-out requirement, so the current draft only contemplates a security and safety exemption in the limited contexts of pre-use notices<sup>4</sup> and access requests.<sup>5</sup>

The removal would be contrary to the purpose of a similar exemption in section 7027(m) with respect to opt-out rights. A consistent exemption when it comes to these purposes is critical, as opt-out mechanisms are sure to invite misuse by fraudsters and other bad actors and make data analysis needed to prevent future fraud or address security risks impossible. Businesses must be able to take appropriate steps to protect their employees and patrons, as well as safeguard the personal data of consumers they may process or retain.

Such an exemption is critical both to ensure that the new rules do not impede safety and security uses of AI, and to be consistent with other state regimes.

**Facilitating Safety and Security Use Cases.** Consistent applicability of the the security and safety exemption throughout the regulation is sound policy. Businesses and consumers clearly and directly benefit when AI is used to enhance security and safety. As SIA has explained in previous rounds of comments, AI enables its users to respond to and analyze potential safety and security risks in a substantially quicker and more accurate manner than traditional, manual methods. Examples include transcribing incident reports and efficiently analyzing video feeds for high-risk safety and security situations. Additionally, widely used biometric identity verification capabilities support a tremendous volume of online commerce on a daily basis. These capabilities are also used for physical security such as access control and facility security screening and even support rapid contactless travel experiences such as clearing customs and aviation security screening.

Absent a broadly applicable security and safety exemption, the rules risk be construed as restricting products and services related to security and safety, which will impede services that substantially benefit California consumers and businesses. Exemptions with narrow or only partial applicability would potentially render security and safety use cases like these impracticable and undermine the use of technology to protect the public. In particular, a piecemeal exemption—as is currently contemplated in the Modified Proposed Rules—would be confusing to consumers and companies trying to act in good faith to comply with the regulations while bringing innovative technologies to the marketplace.

**Harmonization.** In every state outside of California that has adopted a comprehensive privacy law—Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia—the privacy laws offer broader exemptions for security and safety activities, specifying that the rules are not to be construed to limit entities’ ability to engage in various activities to protect and promote security and safety.<sup>6</sup>

Thorough applicability of the security and safety exemption would align California’s approach with these other states, promoting greater consistency and reducing the burden on businesses that comply with various state privacy laws. This would ultimately benefit both businesses and consumers.

---

<sup>4</sup> *Id.* § 7220(d)(2).

<sup>5</sup> *Id.* § 7222(c)(2).

<sup>6</sup> See, e.g., C.G.S.A. § 42-524(a) (Connecticut’s law exempting actions to “prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity, preserve the integrity or security of systems or investigate, report or prosecute those responsible for any such action”).

## **Text Recommendations**

Accordingly, the Agency should make the following two updates:

- Restore the “security, fraud prevention, and safety exception” language that is currently proposed for deletion in Section 7221(b) of the Modified Proposed Rules, and update the language for consistency with the revised security and safety exemptions in Sections 7220(d)(2) and 7222(c)(2) of the Modified Proposed Rules, so that the exemption applies to the requirements governing requests to opt-out of ADMT.

The restored and updated language should read: ***“A business is not required to provide consumers with the ability to opt-out of a business’s use of ADMT to make a significant decision in the following circumstances: (1) The business’s use of that ADMT is to achieve the security, fraud prevention, or safety purposes listed below (“security, fraud prevention, and safety exception”): (A) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information; (B) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business or at consumers, or to prosecute those responsible for those actions; or (C) To ensure the physical safety of natural persons or property.”***

- Include the same “security, fraud prevention, and safety exception” in Section 7150 as a new subsection (d), so that the full exemption applies to the requirements governing risk assessments.

The updated language should read: ***“A business is not required to conduct a risk assessment in the following circumstances: The business’s use of ADMT or automated processing is to achieve the security, fraud prevention, or safety purposes listed below (“security, fraud prevention, and safety exception”): (A) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information; (B) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business or at consumers, or to prosecute those responsible for those actions; or (C) To ensure the physical safety of natural persons or property.”***

Without a consistent exemption for security and safety for the regulations that govern ADMT and automated processing, the rules, once finalized, could be interpreted as limiting important safety and security services, which may have a direct negative impact on California consumers. The benefits of exempting practices and technologies related to providing security and safety clearly outweigh other considerations and thus should be extended to all relevant provisions of the regulations.

<b>Recommendation 2: The Risk Assessment requirement should only target high-risk uses of ADMT.</b>
---

The Modified Proposed Rules have made significant improvements to establish rules that are more risk-based by focusing on using ADMT for a significant decision concerning a consumer. However, there are some inconsistencies in the Modified Proposed Rules that should be addressed to ensure a more harmonized, risk-based approach to the scope of the Agency’s new rules.

Specifically:

Sections 7150(b)(4) and 7150(b)(5) are overly broad because they reference “automated processing” instead of ADMT. We note that “Automated processing” is not a defined term within the proposal.

Inclusion of “automated processing” together with the other references to “ADMT”—a term that has been carefully contemplated and defined—will introduce uncertainty and risk an overbroad interpretation of these sections.



It is not clear that Sections 7150(b)(4) and 7150(b)(5) are focused on ADMT used for significant decisions, which is inconsistent with the other Modified Proposed Rules. Section 7150(b)(4)'s reference to "systematic observation" raises First Amendment concerns to the extent that it sweeps in technology based on publicly available or publicly observable information.

### **Text Recommendations**

To address these issues and inconsistencies, the term "automated processing" should be omitted, and those sections should be amended as follows:

- **Section 7150(b)(4) should be struck entirely.** When updated to be focused on ADMT used for a significant decision, this section would be duplicative of Section 7150(b)(3), which already covers ADMT used for significant decisions concerning consumers acting in their capacity as an educational program applicant, job applicant, student, employee, or independent contractor for the business.
- Section 7150(b)(5) should be amended as follows: *"Using ~~automated processing to infer or extrapolate a consumer's intelligence, ability, aptitude, performance at work, economic situation, health (including mental health), personal preferences, interests, reliability, predispositions, behavior, or movements,~~ ADMT to make a significant decision concerning a consumer based upon that consumer's presence in a sensitive location. ~~"Infer or extrapolate" does not include a business using a consumer's personal information solely to deliver goods to, or provide transportation for, that consumer at a sensitive location."~~*

<b>Recommendation 3: Cybersecurity Audit and Risk Assessment certifications should not create individual liability for company leadership.</b>
--

Under the Modified Proposed Rules, Section 7124 (c) would still require that cybersecurity audits must be signed by a member of the business's executive management team. Section 7157 (b) similarly requires the written certification for a risk assessment to include an "attestation" by the employee that it is "true and correct." As we noted in our February comments, there is no precedent anywhere in the world for a government authority requiring such risk assessments or an annual cybersecurity audit signoff by an individual, requiring them to put their name on the line for the organization.

Again, current legal precedents reflect the reverse. *FTC v. Wyndham Worldwide Corp.* (2012)<sup>7</sup> highlights the FTC's authority to enforce data security practices and emphasizes that compliance is a shared responsibility across various organizational functions, not solely placed on a single individual. And the case *In re: Target Corporation Customer Data Security Breach Litigation* (2014),<sup>8</sup> demonstrates that organizations can be held liable for data breaches regardless of a specific role assigned to an individual in security compliance. This reinforces the common understanding that compliance should involve multiple stakeholders, including IT, legal, and compliance officers, and the responsibility does not rest with a sole individual.

### **Recommendation:**

These sections should be amended so that third party auditors can work with internal audit and cybersecurity teams to conduct the cybersecurity audit for their objective expertise and ultimate collective sign-off.

---

<sup>7</sup> *FTC v. Wyndham Worldwide Corp.*, Case. No. 13-cv-01887, which was in the U.S. District Court for the District of New Jersey. The complaint alleged that Wyndham's lax cybersecurity policies constituted unfair business practices and that the company's privacy policy was deceptive in violation of the FTC's prohibition on "unfair or deceptive acts or practices in or affecting commerce" as codified in 15 U.S.C. § 45(a). For more information see <https://natlawreview.com/article/third-circuit-holds-ftc-has-authority-to-regulate-cybersecurity-under-unfairness>.

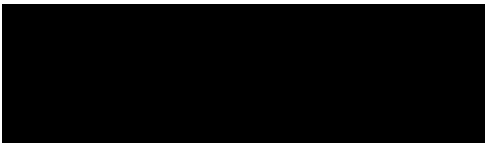
<sup>8</sup> [https://www.mnd.uscourts.gov/sites/mnd/files/2017-0517-14mdl2522\\_M%26O.pdf](https://www.mnd.uscourts.gov/sites/mnd/files/2017-0517-14mdl2522_M%26O.pdf).

## **CONCLUSION**

While the Modified Proposed Rules take steps in the right direction with respect to establishing a more risk-based and harmonized approach, their current scope—without changes to consistently apply the security and safety exemption and to update the scope of the risk assessment requirements to make them more focused on high-risk use cases—still poses a significant risk of impeding essential security operations and critical safety functions and sweeping too broadly.

SIA appreciates the opportunity to provide input to the Agency on these matters. SIA and our members stand ready to provide any additional information you may need as these important issues are considered. Please let us know if you have any questions or if we can provide any additional information that would be helpful.

Respectfully Submitted,



Don Erickson  
Chief Executive Officer  
Security Industry Association  
Silver Spring, MD  
[www.securityindustry.org](http://www.securityindustry.org)  
Staff Contact: Jake Parker, [jparker@securityindustry.org](mailto:jparker@securityindustry.org)

**Grenda, Rianna@CPPA**

---

**From:** MacGregor, Melissa <mmacgregor@sifma.org>  
**Sent:** Monday, June 2, 2025 10:59 AM  
**To:** Regulations@CPPA  
**Cc:** Chamberlain, Kim  
**Subject:** Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance  
**Attachments:** California Cyber and Automated Decision Making Regulation Letter - June 2 2025.pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Please see the attached comments on the CCPA proposed regulations. Thank you!



June 2, 2025

Submitted via email: [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
2101 Arena Blvd.  
Sacramento, CA 95834

**Re: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations**

Dear CPPA Board Members,

The Securities Industry and Financial Markets Association (“SIFMA”)<sup>1</sup> appreciates the opportunity to respond to the modifications to the *Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology, and Insurance Companies* published by the California Privacy Protection Agency (“CPPA”) on May 9, 2025 (the “Proposed Regulations”). SIFMA appreciates many of the modifications the CPPA has made to the original proposal and urges the CPPA to make additional changes to the Proposed Regulations as outlined below to ensure better harmonization with overlapping federal, state, and non-US laws and regulations applicable to SIFMA members.

SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets, including a significant presence in California. SIFMA has 20 broker-dealer members headquartered in California. There are approximately 358 broker-dealer main offices, nearly 40,000 financial advisers, and over 100,000 securities industry jobs in California.<sup>2</sup>

---

<sup>1</sup> The Securities Industry and Financial Markets Association (SIFMA) is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's one million employees, we advocate on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit <http://www.sifma.org>.

<sup>2</sup> See SIFMA California Data here <https://states.sifma.org/#state/ca>

**1. The Proposed Regulations should expressly exempt federally regulated financial institutions from the requirements.**

As a threshold matter, SIFMA continues to recommend that the CCPA expressly exempt federally regulated financial institutions including broker-dealers, registered investment advisers, and banking organizations, as well as their holding companies and affiliates, from the cybersecurity audit, risk assessment, and automated decisionmaking technology (“ADMT”) requirements in the Proposed Regulations. As federally regulated financial institutions, SIFMA members are subject to, and have built robust programs adhering to, federal regulatory regimes which cover cybersecurity, risk management, and the use of (“ADMT”). SIFMA members are governed by the Gramm-Leach-Bliley Act (“GLBA”) and its regulations that cover cybersecurity, privacy and data protection. SIFMA members are further subject to a plethora of federal financial regulatory frameworks and guidance that govern cybersecurity risk for registrants as well as non-U.S. regulators.<sup>3</sup> Federal regulators require extensive policies and procedures, risk management, reporting and testing under their various regulatory regimes including Reg S-P and the Safeguards Rule. Further, SIFMA members are subject to robust oversight including examinations and enforcement by federal regulators.

Without a clear exemption, financial institutions will be forced to divert resources away from proactively guarding against emergent threats to meet the duplicative and unnecessarily prescriptive regulatory obligations, while also still complying with rigorous federal requirements specifically targeted at the financial services industry.

**2. The Proposed Regulations do not exempt activities that are essential for financial institutions to combat malicious activity.**

SIFMA appreciates the narrowing of the scope of the ADMT requirements in the Proposed Regulations which will help to minimize the risk that the Proposed Regulations would cover longstanding compliance and business use cases. Although most data SIFMA members process is covered by GLBA and therefore exempt from the CCPA and the Proposed Regulations, additional clarification is necessary to ensure that our members’ fraud prevention capabilities are not limited by the Proposed Rules. In fact, the Proposed Rules impose more limitations on a covered institution’s ability to use ADMT for fraud detection purposes than the previous version despite broad support for such usage in many comment letters.

The Proposed Rules should be further revised to include an explicit exception for fraud detection activities including but not limited to technology used to detect money-laundering, exploitation of seniors, violations of the Foreign Corrupt Practices Act, Ponzi schemes, insider trading, pump and dump schemes and more. Such uses clearly benefit customers and the

---

<sup>3</sup> Financial regulatory regimes which include data, privacy, and or cybersecurity requirements include those under the Securities and Exchange Commission (“SEC”), Financial Industry Regulatory Authority (“FINRA”), the Office of the Comptroller of the Currency (“OCC”), the Board of Governors of the Federal Reserve System, the Commodity Futures Trading Commission (“CFTC”), the Consumer Financial Protection Bureau (“CFPB”), the Federal Deposit Insurance Corporation (“FDIC”), the National Credit Union Administration (“NCUA”), the U.S. Department of the Treasury,

financial system. As currently drafted, such detection technology is covered thus creating limitations which may not be as beneficial for efficient detection.

Additionally, if an individual decides to opt-out, it can have significant impact on the overall algorithm and models used to detect fraud and provide fraudsters with an additional way to engage in bad activity by opting-out to remain off the radar. The exemption should also specifically allow the use of fraudsters' data for training ADMT models which will help to prevent and catch future frauds. There is no compelling justification for protecting malicious activities or actors, and such data is necessary for training models over time and maintaining the most current defense mechanisms as scams evolve.

Further, there should be a clear exemption for any legal and compliance-related activities which protect customers, investors, the firm, or the financial markets more broadly. Excluding such uses severely impedes the evolution of more efficient compliance systems which runs counter to the goals of the CCPA.

**3. The required risk assessments are triggered at an unnecessarily low threshold and are overly prescriptive.**

The modified Proposed Regulations do not adequately address the unnecessarily low threshold and the prescriptive nature of the required risk assessments which provide limited benefit to consumers. The threshold does not align with other existing risk assessment frameworks, nor does it align with the other sections of the Proposed Regulations. SIFMA urges the CPPA to adopt a standard that would require a risk assessment for activities that are "likely to result in a high risk to the rights and freedoms of natural persons" as is similarly required under the EU General Data Protection Regulation. Such a standard would more directly benefit consumers as it is directly related to higher risk activities. This would also align with the CPPA's changes to the scope of the ADMT requirements in this version which now apply to "significant decisions." The CPPA should similarly align the risk assessment threshold.

**4. The cybersecurity audits are not aligned with existing well-established cybersecurity frameworks and are overly prescriptive.**

SIFMA appreciates the significant changes made to the cybersecurity audit requirements in the Proposed Regulations. Aligning the requirements to existing standards is critical for ensuring that work is not duplicated unnecessarily. Unfortunately, the Proposed Regulations do not adequately incorporate those requirements and even contradict existing standards. For example, the Proposed Regulations require a single annual information security audit. The goal of the proposal would be better achieved if the standard were to align with risk assessments based on broader risk assessment standards which may require audit resources to be deployed in higher risk areas as necessary. If warranted, multiple periodic audits should satisfy the requirements of the Proposed Regulations.

The cybersecurity audit requirements also remain overly prescriptive without any clear reason or consumer benefit. For example, the reporting requirements for the internal auditor are unnecessarily restrictive and do not match how many federally regulated financial institutions are organized. The previous version of the Proposed Rules requiring the senior auditor to report to

the company's board more accurately reflected how financial institutions are structured but also may not work for other industries. This is a clear example of how unnecessarily prescriptive requirements impose burdens which contradict the purpose of the rulemaking and the CCPA. The Proposed Regulations should be revised to provide more flexibility for firms to meet the cybersecurity audit requirements or clearly exempt federally regulated financial institutions from these provisions.

\* \* \* \* \*

SIFMA and its members appreciate the opportunity to provide these comments and welcome further discussion. Please reach out to Melissa MacGregor at [mmacgregor@sifma.org](mailto:mmacgregor@sifma.org) with any questions or to schedule a meeting.

Sincerely,



Melissa MacGregor  
Managing Director & Associate General Counsel

cc: Kim Chamberlain, Managing Director, State Government Affairs, SIFMA



## Grenda, Rianna@CPPA

---

**From:** Anton Van Seventer <avanseventer@SIIA.net>  
**Sent:** Monday, June 2, 2025 12:08 PM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations  
**Attachments:** SIIA CPPA ADMT Comment 6.2.25.pdf

### This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

California Privacy Protection Agency,

Please see attached SIIA's comment regarding the CPPA's revised draft ADMT and cyber regulations. Thank you very much in advance for your consideration.

All the best,

**Anton van Seventer**

Counsel, Privacy and Data Policy

SIIA - Accelerating Innovation in Technology, Data & Media

PO Box 34340, Washington, DC 20043

[avanseventer@siia.net](mailto:avanseventer@siia.net)

Telephone: +1-202-789-4471

Mobile: [REDACTED]

LinkedIn: <https://www.linkedin.com/in/antonvanseventer>



## **Comments of the Software & Information Industry Association**

### **California Privacy Protection Agency**

Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies

*June 2, 2025*

The Software & Information Industry Association (SIIA) appreciates the opportunity to provide comments on the California Privacy Protection Agency's (CPPA's) revised proposed regulations. SIIA is the principal trade association for those in the business of information, including its aggregation, dissemination, and productive use. Our members include roughly 380 companies reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used worldwide, and companies specializing in data analytics and information services.

SIIA supports privacy as a fundamental value to individual autonomy and a functioning democracy. Data privacy standards that harmonize meaningful consumer safeguards with appropriate business compliance will ensure smooth implementation of data privacy practices. We have previously provided stakeholder input on the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), since these laws set an important milestone for companies engaging in interstate commerce both inside and outside of California.

We appreciate the goals of the regulations and the Agency's attention to concerns we have previously articulated regarding both the efficacy and potential unintended consequences of overly prescriptive requirements. Furthermore, SIIA recognizes that the Agency has made significant improvements in both clarity and workability since past drafts, especially around striking first party advertising restrictions as permitted under the CCPA, and prudently avoiding the incorporation of the entire artificial intelligence (AI) stack into the proposed regulations around ADMT. In this submission, we focus on provisions in the draft regulations that would either benefit from additional clarity, or remain likely to have unintended consequences.

## **Definitions**

### ***Comments on Definition of ADMT***

We appreciate the improvements made to the definition of ADMT, particularly the clarification that ADMT refers to technology that uses computation to “execute a decision” or “substantially facilitate human decisionmaking.” This vague scope from previous drafts is now restricted to technology that “replaces” or “substantially replaces” human decisionmaking. This is a positive change and lends much-needed clarity to the definition.

To improve clarity and workability, we recommend three additional changes. First, we recommend clarifying in section 7001(e)(1)(B) that human reviewers consider information that is “necessary” to make a decision, instead of “relevant” to make a decision. Relevance is a subjective determination that will be implemented inconsistently by businesses. In addition, if interpreted expansively, requiring review of any and all “relevant” information may prove impossible for a human reviewer.

Second, in section 7001(e)(3), we recommend striking “provided that they do not replace human decisionmaking.” This language contradicts the purpose of the exemption, which is to allow for the use of ADMT to replace human decisionmaking in certain administrative tasks.

Third, we recommend adding “search term software” to the exemption in section 7001(e)(3). Employers and recruiters frequently use software to assist manual searches to narrow the scope of a recruitment pool, and covering this step in the evaluation process will ensure that this activity is not brought in scope and subject to risk assessments and the suite of consumer rights that are ill-tailored to this employment context.

Fourth, section 7001(e)(2) states that ADMT “includes profiling,” which creates confusion because the “profiling” definition goes beyond profiling for “significant decisions.” Thus, it would be helpful to clarify that “profiling” in the ADMT context only extends to “significant decisions.” Otherwise, it will be unclear to businesses whether, for example, personalized content using first party data remains ADMT activity, in line with the intent of the revised draft.

### ***Comments on Definition of “Sensitive Location”***

We recommend revising the definition of “sensitive location,” newly added in this version of the draft regulations, to comport with the CCPA and avoid unintentionally capturing a



range of low-risk locations. The definition at 7001(aaa) remains overbroad, constitutionally problematic, and most of all unnecessary.

First, the CCPA explicitly exempts “publicly available information,” defined as information made available from the consumer to the general public or from widely distributed media, or if the consumer has not restricted the information to a specific audience. This decision was made very deliberately during drafting to avoid clear-cut constitutional infirmities that would otherwise run afoul of the First Amendment.

Second, it is notable that truly sensitive data, such as any and all consumer precise geolocation data, is already covered under the CPRA. This includes the requirement to conduct risk assessments around this data. In addition to alleviating concerns around collection and processing of this truly sensitive data without risk assessments, the provision even aligns with the draft regulations’ definition of “systematic observation.”

Third, we suggest clarifying that the trigger for a “sensitive location” is a business identifying a consumer visiting such a location and using this data about the sensitive visit for profiling purposes. Without this clarification, consumer visits to nonsensitive locations in the proximity of sensitive locations could come in scope. It would also be helpful to clarify that consumer driven geolocation processing that does not present a risk of harm (*i.e.*, self-trackers, maps) is outside the scope of the “sensitive location” definition.

### **Substantive Provisions**

While we appreciate the care taken by the Agency to streamline the proposed regulations, we continue to have concerns about certain substantive provisions that would needlessly increase the burden on businesses, create uncertainty for both companies and consumers, and not add materially to consumer protection.

#### ***Comments on 7150 (When a Business Must Conduct a Risk Assessment)***

To the extent the definition of “sensitive location” does not change, we recommend striking section 7150(b)(5). This provision would require risk assessments based on “profiling a consumer based upon their presence in a sensitive location.” If left unchanged, this will require businesses to conduct risk assessments based on nonsensitive, low-risk, and publicly available information, such as a consumer’s presence on a college campus or at a grocery store. The regulations would even likely cover very low-risk activities, such as providing discounts for



prescriptions at pharmacies based on a consumer's prior use, or college merchandise based on student residency at that college.

We also recommend further revisions to section 7150(b)(6) concerning the use of personal information to train an ADMT. As a preliminary matter, it is not clear what risk to privacy is posed by the training of ADMT. ADMT "training" encompasses a broad swath of activities, including, for example, adjusting the parameters of an algorithm used for automated decisionmaking technology or artificial intelligence, improving the algorithm that determines how a machine-learning model learns, and iterating the datasets fed into automated decisionmaking technology or artificial intelligence. The ability of ADMT to deliver faster, fairer and more inclusive outcomes to consumers depends on developers' ability to alter algorithms to incorporate both new information and wider datasets representative of all consumers. Restricting developers from tweaking algorithms at scale would be incredibly burdensome; it would have a disproportionate impact on smaller California firms, and also, inevitably, harm consumers' use of and experience with AI tools.

In addition, the proposed definition of "intends to use" contained in this provision should be removed. The language about "plans" to use or permit others to use conflicts with the intentionality component of the revised text, and will bring in scope general use models that are primarily used for other low-risk purposes.

Further, imposing risk assessment and consumer rights obligations to the *training* of ADMT is likely beyond the scope of the statute itself. Imposing heightened obligations on the processing of personal information to train ADMT is not reasonably necessary to effectuate the purpose of the underlying statute, creating potential legal challenges in the future. ADMT training does not involve decisions that concern a specific consumer. It therefore is not automated "decisionmaking," which is what the statute addresses. The scope of the CPPA's rulemaking authority is limited to "access and opt-out rights" with respect to "automated decision-making." It is the right to access, correct, or delete consumer data that provides consumers with mechanisms to acquire information about, or avoid, the processing of their personal information to train ADMT models.

Finally, section 7001(ee) includes an overly broad definition of "physical or biological identification or profiling." The definition would arguably cover emotional detection technologies even when they are not used to make a significant decision or identify a specific data subject. It would be helpful for the Agency to clarify that when not used for these purposes, it is not necessary to conduct risk assessments for these technologies.



***Comments on Section 7200 (When a Business’s Use of ADMT is Subject to the Requirements of This Article)***

The definition of “significant decision” in section 7001(ddd)(4) covers almost all activity within the scope of the employment lifecycle, including hiring, promotion, and suspension and termination – as well as assignment of work and setting of base and incentive compensation over the course of the employment itself. We would prefer this be limited to hiring and firing practices, as the scope of the full panoply of employment-related processes risks restricting productive activities necessary for operating a business that present few privacy risks to consumers yet could hamstring routine operations.

Furthermore, we recommend striking the first sentence of Section 7200(b) requiring businesses that use ADMT for a significant decision prior to the effective date to be in compliance with the requirements of the article by the implementation date. It makes little sense to require a business to provide a risk assessment when the ADMT was used only prior to the effective date.

***Comments on Sections 7220 (Pre-use Notice Requirements), 7221 (Requests to Opt-Out of ADMT), and 7222 (Requests to Access ADMT)***

The text of the draft regulations compels a pre-use notice, an access right and an opt-out right in multiple ways that are at odds with best practices on consumer protection. For example, U.S. state privacy regimes have repeatedly rejected the type of in-your-face notice described in section 7220(c)(5) even for more privacy-invasive practices than ADMT training — such as selling sensitive information — out of concern over consumer notice fatigue. Moreover, the content requirements within the pre-use notice requirement around the “type of output” and “how the output is used” attempt to regulate expressive content and compel protected speech on the part of California businesses to explain their intent and judgments about their processes. The California legislature likely recognized this infirmity, which is why it limited the rulemaking provision regarding “notice” to rules related to how notice is provided and not what notices should contain.

It is also virtually impossible to provide access rights to ADMT training data on an individual level, as required by section 7222(b), because of how training data is combined. Further, explaining to the consumer specifically how one specific piece of data is used to train often complex ADMT – where this data is used in several training processes, while other data is used to train the same processes – in “plain language,” as mandated by the draft regulations, is potentially challenging for businesses, and is also of comparatively little privacy value to consumers.



Further, imposing a backward-facing opt-out is not workable in cases where data is previously integrated into a technology in a manner that does not permit reidentification, such as where data is integrated into a model. This is because it would be prohibitively costly to delete and rebuild a model each time deletion is requested. Like the provisions around actual sales of data, we believe this provision should be solely forward looking.

Lastly, the opt out right would also restrict California businesses when developing their own productive ADMT applications internally by working off larger models from tech companies. In addition to reducing innovation in the state, it would also complicate and perhaps render impossible efforts on the part of ADMT developers to combat discriminatory outcomes resulting from automated tools. The opt-outs would inevitably result in unrepresentative data sets, and this skew would adversely impact those subject to automated decisions simply due to representative bias. Unfortunately, biased outcomes under such a regime are all-but inevitable. This is even the case where the consumers who are themselves subject to automated decisions do not opt out.

#### ***Comments on Section 7123 (Scope of Cybersecurity Audit and Audit Report)***

The proposed audit requirements under section 7123(f) would require businesses to conduct unique audits for California even if they are already complying with best practices. This creates unnecessary duplication and expenses that will impede the objectives. We recommend instead that the Agency permit companies to use common cybersecurity audit frameworks — such as ISO 27001, ISO 27018, SOC 2 Type 2.

In addition to avoiding compliance burden and costs, relying on industry best practices will also avoid a situation in which the CPPA audit requirements become obsolete as technology advances. Existing cybersecurity audit standards anticipate this. For example, NIST recommends as a security control that “the confidentiality, integrity, and availability of data-at-rest are protected.” The Agency’s proposal, however, requires *specific* security controls to achieve certain outcomes (e.g., requiring assessment of encryption of personal information at rest, assuming the use of multi-factor authentication and passwords when businesses are increasingly moving to passkeys). We believe this is out of step with the core purpose of audits — to identify and remediate risks — rather than mandate detailed papering exercises.





## Process

### ***The cost estimate underestimates implementation costs.***

The CPPA's Standardized Regulatory Impact Assessment (SRIA) estimates that compliance will cost California businesses \$3.4 billion. We believe this is likely well below the true cost that will be incurred. This is because the analysis underestimates the number of businesses affected and does not consider the regulations' continuing effects on California businesses' operating costs and productivity.

First, the estimate only includes businesses with employees in California, eschewing the many out-of-state companies that sell into California and its markets. The SRIA actually acknowledges the proposed regulations' effects on out-of-state companies, yet opts to leave out these costs because they do not impact California businesses themselves. However, the SRIA also requires recognition of effects on jobs and investment in the state. Because the proposed requirements would compel out-of-state businesses to face the same audits, ADMT opt-out provisions, and risk assessment requirements, small entities especially will be incentivized to withdraw from California markets to avoid these costs. The cost of the reduction in choices, reduced competition, and higher prices is likely to raise first-year costs by potentially several billion dollars above the estimate.<sup>1</sup>

Second, the SRIA addresses only the costs of programming, cybersecurity audits and risk assessments, and ignores the effects of the proposed regulations on ongoing business operations, including negatives to cost and productivity. This underestimates the expense, especially of the proposed regulations around ADMT, whose broad scope and first-in-the-nation impact will dramatically increase California business's ongoing costs.

These include costs associated with:

- 1) intake and response to ADMT opt-out requests from consumers,
- 2) administering a non-automated process for each ADMT-covered decision,
- 3) responding to consumer inquiries about the purpose for which the business is using ADMT and outputs regarding that consumer, and
- 4) the inevitably negative impact of consumer and employee opt-outs on the reliability of ADMT or the reliability of behavioral advertising (as previously discussed).

---

<sup>1</sup> [Comments on August 2024 CPPA SRIA for California Chamber of Commerce.](#)



Policies that stifle a significant fraction of the total value of AI adoption and use would likely have impacts in excess of tens of billions per year – a cost that far exceeds any savings accrued from the proposed regulations.<sup>2</sup>

\* \* \*

Thank you for considering our feedback to the proposed regulations. We are happy to discuss any of these comments in further detail. SIIA's point of contact for this submission is Anton van Seventer, Counsel for Privacy and Data Policy ([avanseventer@siia.net](mailto:avanseventer@siia.net)).

---

<sup>2</sup> Goldman Sachs, "Generative AI Could Raise Global GDP by 7%." April 5, 2023.  
<https://www.goldmansachs.com/insights/articles/generative-ai-could-raise-global-gdp-by-7-percent>.



**Grenda, Rianna@CPPA**

---

**From:** Peter Leroe-Muñoz <pleroemunoz@svlg.org>  
**Sent:** Monday, June 2, 2025 4:21 PM  
**To:** Regulations@CPPA  
**Subject:** Re: Public Comments Regarding Proposed Regulations on CPPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT) and Insurance Companies  
**Attachments:** REVISED Comments\_Silicon Valley Leadership Group.pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Hello,

Please find attached REVISED comments from the Silicon Valley Leadership Group.

Please disregard the prior comments.

I am happy to address any questions.

Best,  
Peter

**Peter Leroe-Muñoz** (He/Him/His)

General Counsel  
SVP, Tech & Innovation

408.427.4697 | [svlg.org](https://svlg.org)

Connect with us: [Twitter](#) | [LinkedIn](#) | [Facebook](#)

On Fri, May 30, 2025 at 2:04 PM Peter Leroe-Muñoz <[pleroemunoz@svlg.org](mailto:pleroemunoz@svlg.org)> wrote:

Hello,

Please find attached public comments from the Silicon Valley Leadership Group.

Please advise of any questions.

Best,

Peter

**Peter Leroe-Muñoz** (He/Him/His)

General Counsel

SVP, Tech & Innovation

408.427.4697 | [svlg.org](https://svlg.org)

Connect with us: [Twitter](#) | [LinkedIn](#) | [Facebook](#)



**SILICON VALLEY**  
LEADERSHIP GROUP

▼ 2460 N First St., Suite 260  
San Jose, California 95131

☎ (408) 501-7864

🌐 [svlg.org](http://svlg.org)

California Privacy Protection Agency  
2101 Arena Blvd.  
Sacramento, CA 95834

**June 2, 2025**

**Ahmad Thomas, CEO**  
Silicon Valley Leadership Group

**Jed York, Chair**  
San Francisco 49ers

**Eric S. Yuan, Vice Chair**  
Zoom Video Communications

**James Gutierrez, Vice Chair**  
Luva

**Victoria Huff Eckert, Treasurer**  
Google

**Aart de Geus**  
Synopsis

**Vintage Foster**  
AMF Media Group

**Raquel Gonzalez**  
Bank of America

**Paul A. King**  
Stanford Children's Health

**Alan Lowe**  
Lumentum

**Rao Mulpuri**  
View

**Kim Polese**  
CrowdSmart

**Sharon Ryan**  
Bay Area News Group

**Siva Sivaram**  
Western Digital

**Tom Werner**  
SunPower

Dear California Privacy Protection Agency Board Members and Staff,

Thank you for the opportunity to provide public comment on the modifications to the text of the Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT) and Insurance Companies. These comments supplement those that we previously joined as part of a larger coalition of business associations.

The Silicon Valley Leadership Group (SVLG) is a business association representing innovation companies throughout California, including global-leading firms, visionary startups and premier research institutions.

Within Article 1, General Provisions, Section 7001, the scope of "significant decisions," specifically §7001(ddd)(4) "Employment or independent contracting opportunities or compensation" should be narrowed. In particular, section (B), "allocation or assignment of work" and compensation decisions should be removed.

This section covers decisions that are not high-risk from a privacy perspective. They do not involve the disclosure of sensitive data, or result in high-risk decisions, like termination, credit, or healthcare decisions.

Further, with the section as drafted, the Agency would be involving itself in day-to-day operational decisions of businesses, which are well beyond the Agency's scope as a privacy regulator.

The Board discussed making a similar change during its April meeting, but the change was not adopted in the amended version of the regulation. It should be made here.

In addition to the changes articulated above, we raise concerns around other elements of the proposed regulations. Regarding Article 10, our global posture is that we request that all references to "training AI" in this Risk Assessment section be removed. The California Consumer Privacy Act only authorizes the Agency to issue regulations on the "use" of ADMT.

More specific points on this and other sections are raised here. Regarding §7150(b)(5) – Profiling – Sensitive Location, we seek removal of this provision because the rules still regulate the use of ADMT to process publicly available information, such as a consumer's presence on a college campus or a grocery store with a pharmacy. None of this is private information. The California Privacy Rights Act (CPRA) otherwise regulates the use of data collected from geo-trackers that identify a consumer's precise geolocation, regardless of the location. As sensitive data, a controller must still conduct a risk assessment and provide an opt out.



## SILICON VALLEY LEADERSHIP GROUP

The overbreadth here would capture low risk activities such as providing discounts for prescriptions at specific pharmacies based on a consumer's prior use or college merchandise based on a student's residence at a specific college.

Regarding Section 7150(b)(6) – AI/ADMT Training, we support the revised scope to exclude language covering models that are “capable” of certain purposes and limit it to models where the business intends to use it for those purposes. However, as defined in revised text, the term “intends to use” also covers “permits others to use, plans to permit others to use” and advertising such uses. This language should be removed, as it conflicts with the “intent” language and will bring in scope a wide-range of general use models that are primarily used for other, low-risk purposes. The proposed rules otherwise cover if a deployer intends to use a model to make a significant decision or a deployer modifies a model with supplemental training that it then intends to use to make a significant decision.

Moreover, the rules should not extend risk assessments to processing for training a model that is used for emotion recognition, if it does not otherwise involve identifying a specific person (which is already covered). It should also not expressly call out training for models used for biological identification. Risk assessments already extend to processing of sensitive data, which includes biometric data as defined under CPRA. If a deployer is using such a model for biological identification, then assessments already apply. The same is true if a developer uses biometric data to train a model. But it should not extend to models that are not trained on biometric data; otherwise, the rules remove an incentive for developers to minimize the sensitive data that they use in training.

Regarding Section 7200(b), the first sentence should be removed. A business should not have to provide a risk assessment where ADMT was used prior to an effective date and is not used on or after the effective date.

For Section 7220(c)(5) – Explainability, the updated rules still require notices to include a significant amount of information. The most problematic are (A) and (B), which require disclosing the type of outputs generated and how the output is used to make a significant decision. The CPPA should consider whether this genuinely helps the consumer and whether risks are better mitigated through an assessment that requires rigorous testing.

Finally, regarding Section 7222(b) – Response to Access Request, the rules should be limited to where the ADMT use resulted in an adverse decision. Further, Subsection (2) language should be removed. Other regulatory regimes that require an adverse decision explanation do not require disclosing methodology. This does not relate to any privacy risk to the consumer but does create a risk of requiring the disclosure of sensitive business information.

Best,



Peter Leroe-Muñoz  
SVP of Tech + Innovation Policy | Silicon Valley Leadership Group

**Grenda, Rianna@CPPA**

---

**From:** Randi Morrison <[rmorrison@societycorpgov.org](mailto:rmorrison@societycorpgov.org)>  
**Sent:** Thursday, May 29, 2025 1:25 PM  
**To:** Regulations@CPPA  
**Cc:** Randi Morrison  
**Subject:** Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations  
**Attachments:** Society CCPA Comment Letter May 29, 2025.pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Dear Ladies and Gentlemen,

Attached for your consideration is a comment letter from the Society for Corporate Governance on the above-referenced draft regulations. Please let me know if you have any questions.

Thank you.

Kind regards,

Randi

Randi Val Morrison  
General Counsel & Chief Knowledge Officer  
Society for Corporate Governance  
52 Vanderbilt Avenue, Suite 510, New York, NY 10017  
(212) 681-2001  
[rmorrison@societycorpgov.org](mailto:rmorrison@societycorpgov.org)  
<https://www.societycorpgov.org>







May 29, 2025

Submitted via electronic mail: [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
400 R Street, Suite 350  
Sacramento, CA 95811

**Re: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations**

Dear Ladies and Gentlemen:

The Society for Corporate Governance appreciates the opportunity to submit comments to the California Privacy Protection Agency ("Agency") on its ongoing rulemaking under the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA").<sup>1</sup> In particular, as directed by the Agency's Notice of Modifications to Text of Proposed Regulations and Additional Materials Relied Upon,<sup>2</sup> the Society's comments are limited to modifications to the text of the proposed regulations after the initial comment period, specifically the text concerning addressing the internal audit reporting structure under **§7122 – Thoroughness and Independence of Cybersecurity Audits**.

**Background**

Founded in 1946, the Society is a professional membership association of more than 3,700 corporate and assistant secretaries, in-house counsel, outside counsel, and other governance professionals who serve approximately 1,600 entities, including 1,000 public, private, and nonprofit organizations of almost every size and industry. Our organization has more than 75 years of experience empowering professionals to shape and advance corporate governance within their organizations, in part through providing the knowledge and tools they need to advise their boards and executive management on corporate governance; regulatory and legal developments; and disclosure.

In this context, we are pleased to provide our perspective to the Agency with respect to the governance of the internal audit reporting structure in relation to the cybersecurity audit provisions proposed under §7122.

**Analysis**

The proposed regulations provide:

**§ 7122. Thoroughness and Independence of Cybersecurity Audits.**

(3) ~~(2)~~ If a business uses an internal auditor, to maintain the auditor's independence, the highest-ranking auditor must report ~~regarding cybersecurity audit issues~~ directly to ~~the business's board of directors or governing body, not to business management~~ ~~that has direct responsibility for the business's cybersecurity program. If no such~~

<sup>1</sup> "California Consumer Privacy Act (CCPA)," Office of the Attorney General, last modified March 13, 2024, <https://oag.ca.gov/privacy/ccpa>

<sup>2</sup> "Notice of Modifications to Proposed Text," California Privacy Protection Agency, May 9, 2025, [https://coppa.ca.gov/regulations/pdf/ccpa\\_updates\\_cyber\\_risk\\_admt\\_notice.pdf](https://coppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_notice.pdf)

~~board or equivalent body exists, the internal auditor must report to the business's highest-ranking~~ a member of the business's executive management team who ~~that~~ does not have direct responsibility for the business's cybersecurity program. ~~The business's board of directors, governing body, or highest-ranking executive that does not have~~ A member of the business's executive management team who does not have direct responsibility for the business's cybersecurity program must conduct the highest-ranking auditor's performance evaluation, if any, and determine the auditor's compensation.

While the Society appreciates the removal of the previously proposed provisions mandating, as opposed to permitting, that the internal auditor report directly to the board of directors (former §7122(a)(3)), and other proposed board-related provisions (e.g., former §7122(f), §7124(e)), the newly proposed text requiring that the highest-ranking auditor report to a member of executive management who does not have direct responsibility for the company's cybersecurity program (inclusive of evaluation of the auditor's performance and determination of compensation) is inconsistent with recommended best practices, which provides for direct or functional reporting<sup>3</sup> to the audit committee of the board of directors or another board body.

The Institute of Internal Auditors' Global Internal Audit Standards ("Standards"), most recently updated in 2024, provide as follows:

Internal auditing is most effective when the internal audit function is directly accountable to the board (also known as "functionally reporting to the board"), rather than directly accountable to management for the activities over which it provides assurance and advice. A direct reporting relationship between the board and the chief audit executive enables the internal audit function to perform internal audit services and communicate engagement results without interference or undue limitations. Examples of interference include management failing to provide requested information in a timely manner and restricting access to information, personnel, or physical properties. Limiting budgets or resources in a way that interferes with the internal audit function's ability to operate effectively is an example of undue limitation.<sup>4</sup>

The Standards also note the recommended and common practice of a bifurcated reporting structure, where the chief audit executive ("CAE") reports functionally to the board (typically, the audit committee) and administratively to a member of senior management.<sup>5</sup>

Consistent with the foregoing recommended practices, according to the IIA's "2025 North American Pulse of Internal Audit" based on its late 2024 survey of more than 400 CAEs and directors, 92% of public companies and 94% of financial services CAEs have a direct / functional reporting relationship with the board, most commonly, the audit committee. As noted above, functional reporting includes, among other things, evaluation and compensation of the CAE.<sup>6</sup> The report further provides that 83% of all respondents,

<sup>3</sup> "Functional reporting refers to oversight of the responsibilities of the internal audit function, including approval of the internal audit charter, the audit plan, evaluation of the chief audit executive, and compensation of the chief audit executive," as written in "2025 North American Pulse of Internal Audit," The Internal Audit Foundation, March 2025, pp. 10, <https://www.theiia.org/globalassets/site/resources/research-and-reports/pulse-of-internal-audit/2025-iaa-pulse-report.pdf>

<sup>4</sup> "Global Internal Audit Standards," The Institute of Internal Auditors, January 9, 2024, pp. 47, [https://www.theiia.org/globalassets/site/standards/globalinternalauditstandards\\_2024january9.pdf](https://www.theiia.org/globalassets/site/standards/globalinternalauditstandards_2024january9.pdf)

<sup>5</sup> "While the chief audit executive reports functionally to the board, the administrative reporting relationship is often to a member of management. This enables access to senior management and the authority to challenge management's perspectives. To achieve this authority, it is leading practice for the chief audit executive to report administratively to the chief executive officer or equivalent, although reporting to another senior officer may achieve the same objective if appropriate safeguards are implemented," as written in "Global Internal Audit Standards," pp. 47-48.

<sup>6</sup> "2025 North American Pulse of Internal Audit," pp.10.

including those associated with nonprofit, privately held, and public sector organizations, have a functional reporting relationship with the board, while 94% of such organizations have audit committees.<sup>7</sup>

Numerous other reputable sources advise a similar reporting structure.<sup>8</sup> As such the proposed revised text requires companies in scope of the cybersecurity audit requirements that wish to use their internal auditor rather than an external auditor to conduct the audit to have an organizational reporting structure that is inconsistent with common and recommended best practices.

## **Recommendation**

In view of the foregoing, we propose that the regulations afford companies the flexibility to choose the internal audit reporting structure that best suits their facts and circumstances, whether that be functional reporting to the audit committee or another board-level body (consistent with common and recommended best practices) or a member of senior management who does not have direct responsibility for the business's cybersecurity program as currently proposed.

Illustrative proposed text is as follows (with proposed new text underlined and proposed deleted text reflected as strikethrough):

If a business uses an internal auditor, to maintain the auditor's independence, the highest-ranking auditor must report directly either to the board of directors or a committee of the board of directors (such as the audit committee) or a member of the business's executive management team who does not have direct responsibility for the business's cybersecurity program. ~~A member of the business's executive management team who does not have direct responsibility for the business's cybersecurity program must~~ As used herein, direct reporting shall include conducting the highest-ranking auditor's performance evaluation, if any, and determining such auditor's compensation.

---

<sup>7</sup> Administrative reporting among publicly traded and privately held companies is most commonly to the Chief Financial Officer, as seen in "2025 North American Pulse of Internal Audit," pp. 10.

<sup>8</sup> See, e.g., "An effective relationship between the audit committee and internal auditors is fundamental to the success of the internal audit function. Internal audit should have direct access to the audit committee, optimally with the chief audit executive (CAE) reporting directly to the audit committee and administratively to senior management. In this reporting structure, internal auditors can remain structurally separate from management, enhancing independence and objectivity. This also encourages the free flow of communication on issues and promotes direct feedback from the audit committee on the performance of the CAE and the function," "Audit Committee Guide," Deloitte, 2025, pp. 32, <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-audit-committee-guide-2025.pdf>; "The need for internal audit to be independent from the activities it audits remains. This is typically achieved by having a direct reporting line to the audit committee and safeguards in place when the chief audit executive has additional responsibilities outside of internal audit. In addition, internal auditors must maintain an unbiased mindset and avoid conflicts of interest to ensure that their assessments are impartial and credible," "Governing a relevant, effective, and valued internal audit function," Deloitte, November 2024, pp. 2, [https://higherlogicdownload.s3.amazonaws.com/GOVERNANCEPROFESSIONALS/5d47927b-105a-4bc7-9aef-821536f3505b/UploadedImages/us-otaca-nov-2024-new\\_1.pdf](https://higherlogicdownload.s3.amazonaws.com/GOVERNANCEPROFESSIONALS/5d47927b-105a-4bc7-9aef-821536f3505b/UploadedImages/us-otaca-nov-2024-new_1.pdf); "Internal audit often reports to both the audit committee and management," "Getting the most out of internal audit," PwC, October 2024, pp. 4, <https://www.pwc.com/us/en/governance-insights-center/publications/assets/pwc-getting-the-most-out-of-internal-audit.pdf> at 4; "The Institute of Internal Auditors (IIA) and others suggest that internal audit report 'functionally' to the audit committee and 'administratively' to executive management, creating a direct line of communications between the chief audit executive (CAE) the CEO or other C-level executive—e.g., the CFO, general counsel, or other C-level—who can effectively serve as the 'internal audit champion.' What is the role of the audit committee versus management in this reporting relationship—e.g., reviewing and approving internal audit's plan, budget, and resources; hiring or firing the head of internal audit; conducting a performance review and determining compensation? Each organization will need to structure the head of internal audit's reporting relationships and oversight roles according to its unique needs and circumstances; however, in many cases it will make sense for both the audit committee and the internal audit champion to be jointly responsible for overseeing internal audit," Audit Committee Guide, KPMG, 2022, pp.16, <https://kpmg.com/us/en/board-leadership/articles/kpmg-audit-committee-guide.html>

## **Conclusion**

The foregoing proposed text allows in-scope companies the flexibility to maintain a reporting structure that best suits their particular facts and circumstances, which may reflect common and recommended best practices, in a manner that is also consistent with the auditor independence objectives of §7122.

Thank you for considering the Society's input.

Respectfully submitted,

A black rectangular box redacting the signature of Randi Val Morrison.

Randi Val Morrison  
General Counsel & Chief Knowledge Officer

**Grenda, Rianna@CPPA**

---

**From:** Willy Martinez <willy.martinez@marinerstrategies.com>  
**Sent:** Monday, June 2, 2025 8:11 AM  
**To:** Regulations@CPPA  
**Cc:** Andrew Kingman  
**Subject:** SPSC - Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations  
**Attachments:** SPSC - CPPA Regulations - Revised Comments 06.02.25.pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Good Morning,

On behalf of the State Privacy and Security Coalition (SPSC), please find attached our written comments regarding the California Privacy Protection Agency's proposed regulations on Cybersecurity Audits, Risk Assessments, and Automated Decision-Making Technology (ADMT).

With our best,

Willy & Andy

--

**Willy Chanes Martinez** (He/Him/His)  
FIP, AIGP, CIPP/US, CIPP/E, CIPM, CIPT  
*Associate*  
703.675.7315  
[www.marinerstrategies.com](http://www.marinerstrategies.com)

Co-Host of *The Spyglass* Podcast – Listen [Here!](#)



# STATE PRIVACY & SECURITY COALITION

June 2, 2025

California Privacy Protection Agency  
2101 Arena Blvd  
Sacramento, CA 95834  
[regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

## RE: Comments on Revised CCPA Regulations

Dear Members of the California Privacy Protection Agency ("CPPA" or "Agency"):

The State Privacy & Security Coalition (SPSC), a coalition of over 30 companies and six trade associations in the retail, technology, telecommunications, automobile, health care, and payment card sectors, respectfully submit follow up comments to our February 2025 letter regarding the proposed California Consumer Privacy Act (CCPA) regulations.

As previously noted, our coalition works in all 50 states on data privacy, cybersecurity, and automated decision-making technology (ADMT) legislation and regulation. We come from a compliance orientation, ensuring that new proposals achieve the necessary balance of improving consumer privacy while retaining operational workability for businesses, and cybersecurity protections for all stakeholders. While we appreciate the work the Agency has done to scale down the proposed regulations, we are still concerned with the revised regulations' scope and resulting cost to businesses, without a corresponding privacy benefit to consumers.

### I. ARTICLE 9 - CYBERSECURITY AUDITS

We acknowledge the CPPA's changes to Article 9, including the removal of some of the overly prescriptive requirements such as mandatory Zero Trust Architecture and the addition of significantly improved governance provisions. However, the revised regulations continue to present operational challenges and lack sufficient alignment with industry standards, particularly in three critical areas: audit scope, audit cadence, and recognition of existing cybersecurity frameworks.

Simply put, we believe the cybersecurity audits need the following improvements in order to justify the cost and resource expenditures to businesses:

- ***Make clear that the audits are intended to evaluate risk-based approaches to cybersecurity programs;***
- ***Establish that the use and reasonable implementation of recognized international cybersecurity frameworks creates a presumption of compliance with this section of the regulations; and***
- ***Establish that compliance with this section constitutes "reasonable care" of consumer data such that the CCPA's private right of action does not apply.***

The scope of the cybersecurity audit remains overly broad and insufficiently risk based. Section 7123(b) requires auditors to assess a business's implementation of each component of its cybersecurity program listed in subsection (c), regardless of whether those components are material to the risks posed by the specific data processing activities, or the types of personal information involved. This departs from the risk-based approach reflected in widely accepted cybersecurity frameworks such as the National Institute for Standards and Technology Cybersecurity Framework 2.0 (NIST CSF), International Standards Organization 27001 framework, and CIS Critical Security Controls (CIS Controls). While the regulations note that auditors may explain why a particular control is inapplicable, it still requires documentation and justification for each excluded element. This approach risks diverting security resources toward compliance paperwork rather than substantive risk mitigation.

Second, the regulations should recognize that annual audits are not feasible for many businesses and are also inconsistent with global norms. For example, ISO 27001 and NIST frameworks support a three-year full audit cycle with interim risk-based assessments. Article 9 should allow a similar structure: a full audit every three years supplemented by targeted, risk-based reviews during interim years. This adjustment would preserve the CPPA's goal of accountability while aligning with



international standards and significantly reducing unnecessary costs. The CPPA is empowered to define the scope of the audit. By limiting the scope in intervening years of a three-year cycle to only materially updated or new conditions, the cost and compliance burden of these regulations will be substantially reduced for businesses without sacrificing security considerations. This could be accomplished by the requiring that the business, in the intervening years of the three-year cycle, complete an intervening audit or assessment to account for materially updated or new conditions.

Third, although Section 7123 now suggests that businesses may rely on a prior cybersecurity audit conducted under another framework, it still could be read as requiring a detailed mapping to all regulatory requirements—even when the external audit was conducted using comprehensive and rigorous standards such as NIST CSF. The CPPA should clarify that businesses may satisfy audit obligations by using such frameworks, provided they are implemented in good faith and reasonably address the regulation’s core requirements. Without this clarification, businesses face duplicative audit efforts and confusion over whether their compliance posture meets California’s expectations.

Finally, the CPPA should consider incorporating a limited affirmative defense for companies that have completed a cybersecurity audit in good faith and implemented remediation plans for any identified gaps. The CCPA allows for private rights of action in cases where a business did not meet the standard of “reasonable security procedures and practices.” The CPPA should make clear that compliance with the cybersecurity audit provisions of these regulations satisfy the CCPA’s standard for reasonable care. This would provide important incentives for compliance and mitigate the litigation risk associated with data breach cases involving personal information.

We encourage the CPPA to adopt a more risk-based, interoperable, and incentive-aligned approach to cybersecurity auditing that preserves consumer protection while enabling businesses to focus on practical security outcomes.

## II. ARTICLE 10 – RISK ASSESSMENTS

Similarly, we appreciate the Agency’s decision to make several improvements to the risk assessment framework, including the attempt to eliminate the constitutional issues associated with the prohibition on processing when risks outweigh benefits, clarifying submission requirements, and limiting certain obligations to more narrowly defined use cases. These are important steps that reflect a more workable understanding of how privacy risk assessments function in practice. However, the revised draft regulations continue to present several legal, operational, and interoperability challenges that require further modification to avoid undermining their stated purpose.

### a. Interoperability with Other Frameworks is Critically Underdeveloped

The revised text in § 7156 attempts to permit use of assessments conducted for other laws, but it imposes restrictive conditions that severely undercut any practical benefit. While a business may reuse another assessment if it contains the information that must be included in a CPPA-compliant risk assessment, that is functionally equivalent to requiring a standalone California-specific analysis. This approach is inconsistent with how interoperability is handled under other comprehensive privacy laws. For example:

- Colorado’s Privacy Act explicitly allows businesses to rely on “data protection assessments prepared pursuant to comparable laws or regulations” (Colo. Rev. Stat. § 6-1-1311).
- The EU General Data Protection Regulation (GDPR) similarly recognizes that data protection impact assessments (DPIAs) should not be redundant and can be reused across comparable processing contexts (Art. 35(10), GDPR).

Requiring parity or supplementation without recognizing functional equivalency burdens businesses operating across jurisdictions, especially when risk assessments already cover similar data flows, processing purposes, and mitigation strategies. Instead, the CPPA should revise § 7156 to permit businesses to rely on assessments prepared under other laws that are “reasonably similar in scope and effect,” mirroring language used in the Colorado regulations.

## **b. Confidentiality and Legal Privilege Must Be Explicitly Protected**

While we welcome the CPPA's clarification that businesses are not required to submit full risk assessments as part of the routine attestation process in § 7157, concerns remain about the confidentiality of assessments submitted in response to targeted agency requests.

Risk assessments often involve privileged legal analysis, internal audit findings, and candid evaluations of organizational vulnerabilities. Without an express provision preserving attorney-client privilege and work product protections, compelled submission may chill the candor of future assessments or inadvertently waive protections in litigation. We recommend the regulations include the same protections that all other state privacy laws include with their risk assessment provisions, such as: *"Submission of a risk assessment to the Agency shall not be deemed a waiver of any applicable legal privilege, including attorney-client privilege or attorney work product protections, nor shall it constitute public disclosure under state law."*

## **c. Overly Prescriptive Elements Undermine Risk-Based Flexibility**

The enumeration of operational elements under § 7152(a)(3), particularly subsections (D), (F) and (G), creates an excessively formulaic structure that diverts focus from substantive risk analysis. Privacy risk assessments are inherently contextual. Requiring a rigid mapping of data sharing to third-party categories or a disclosure of the "logic" behind ADMT models ignores ongoing research challenges and the varied nature of processing environments. In particular:

- Subsection (D) requires businesses to approximate the number of consumers it plans to process. Particularly for a new product or service, making this assessment pre-launch is not feasible.
- Subsection (F) requires businesses to match data recipients to purposes in a way that may duplicate information already covered in privacy notices or service provider agreements.
- Subsection (G)(1) obliges disclosure of "assumptions or limitations of the logic" used by ADMT. Not only is this vague, but such logic may be proprietary, underdeveloped, or too complex to meaningfully articulate in plain terms. The risk to individuals often lies not in understanding a model's architecture but in its impacts—which are already addressed under separate obligations.

This type of prescriptiveness encourages rote compliance over meaningful evaluation and is inconsistent with frameworks like the GDPR, which emphasize proportionality, context, and accountability.

## **d. Additional Requirements for Businesses that Process Personal Information to Train Automated Decision-making Technology Should Be Refined**

The Agency should remove references to the training of ADMT from the draft regulations. The CCPA authorizes rulemaking related to a business's *use* of ADMT in processing personal information—not the development or training of such technologies. Training refers to the internal development phase of ADMT and does not result in individualized decisions or outcomes affecting any specific consumer. As such, it falls outside the statutory scope contemplated by the CCPA. Numerous stakeholders, including Governor Newsom, have emphasized that extending these rules to cover training exceeds the boundaries of the enabling legislation. The Agency should, therefore, eliminate all provisions referencing the training of ADMT from the regulatory text.

Additionally, Section 7153(a) should be revised to safeguard confidential, proprietary, and security-sensitive information. As currently drafted, the regulation requires a business to provide "all facts available" to support a recipient-business's risk assessment when making ADMT available for use. This broad language may be interpreted to compel disclosure of trade secrets, proprietary model architecture, training datasets, algorithmic logic, or sensitive information about system vulnerabilities. To strike the appropriate balance between transparency and security, the regulation should clarify that businesses are required to provide only non-confidential, material information reasonably necessary for the recipient-business to conduct a compliant risk assessment.



## **e. Annual Submission Requirements Should Be Calibrated to Risk**

Under § 7157, businesses are required to submit attestation forms annually detailing how many risk assessments were conducted and whether they involved specific categories of personal information. However, this requirement applies regardless of the level of privacy risk involved. Submitting metrics tied to low-risk processing (e.g., short-term cookie usage or internal employee training tools) imposes a high compliance cost without commensurate privacy benefit.

The Agency should consider limiting this obligation to a subset of high-risk activities—such as:

- Processing involving sensitive personal information (as defined in Cal. Civ. Code § 1798.140(ae)); and
- ADMT used to make legally or similarly significant decisions.

Additionally, the Agency should clarify that metrics submitted under § 7157 may be aggregated and need not include consumer-specific information or granular processing disclosures. This change would be more aligned with data minimization principles and would ease concerns about how the Agency plans to store and protect the information it receives.

## **f. Definition of Systematic Observation Should be Narrowed**

The current definition of “systematic observation” in § 7001 is overbroad and risks capturing low-risk or incidental activities. As drafted, it could encompass anything from video recordings of a training seminar to badge scans at office entrances. To preserve the intent of focusing on high-risk surveillance practices, the Agency should clarify that: *“‘Systematic observation’ means methodical and regular or continuous observation, which includes methodical and regular or continuous observation using Wi-Fi or Bluetooth tracking, radio frequency identification, drones, video or audio surveillance (such a closed-circuit television) or live-streaming, technologies that enable physical or biological identification or profiling; and geofencing, location trackers, or license-plate recognition.”*

Without refinement, this definition risks triggering heightened obligations for a wide range of benign, operational tools that pose limited or no privacy risk.

## **g. Timing of Risk Assessments**

The proposed rules create confusion regarding the timing of risk assessments. Section 7155(b) states that risk assessments for processing activities initiated before the effective date and continuing thereafter must be completed by December 31, 2027. However, Section 7155(a)(1) requires a risk assessment prior to initiating any new processing activity, and Section 7155(a)(3) requires that risk assessments be updated within 45 calendar days of a material change to a processing activity.

These provisions are difficult to reconcile. For example, §7155(a)(1) appears to prohibit new processing from beginning without a prior risk assessment—even though §7155(b) allows risk assessments for pre-existing activities to be completed as late as December 31, 2027. Similarly, §7155(a)(3) requires updates within 45 days of a material change, but that presumes the existence of an initial assessment, which may not yet be required under §7155(b).

To resolve these inconsistencies, we recommend revising the rule language to clarify that:

- For any processing activity requiring a risk assessment that is underway before December 31, 2027, the assessment must be completed by December 31, 2027;
- For any new processing activity initiated after December 31, 2027, the risk assessment must be conducted prior to initiation; and
- For any material change occurring after December 31, 2027, an existing risk assessment must be updated within 45 calendar days.

## III. ARTICLE 11 – AUTOMATED DECISION-MAKING TECHNOLOGY

### a. Sec. 7001(e): Automated decision-making Technology (ADMT)

#### *i. The ADMT Definition Exceeds Statutory Authority and Should Be Deferred*

We appreciate the Agency's efforts to refine the definition of "automated decision-making technology" (ADMT) in the revised draft. By removing references to tools that merely "execute" or "substantially facilitate" human decision-making—and instead focusing on technologies that "replace" or "substantially replace" human decision-making—the Agency has taken a meaningful step toward better aligning the definition with higher-risk use cases.

Nevertheless, the revised definition still reaches into areas that are the subject of active legislative consideration and executive policy development. As Governor Newsom stated in his April 23, 2025, letter, the Agency's rulemaking authority—while significant—is not without limits. The Governor warned that extending beyond the boundaries of Proposition 24 risks unintended consequences, and he reaffirmed that the Agency "can fulfill its obligations to issue the regulations called for by Proposition 24 without venturing into areas beyond its mandate." Deferring final action on ADMT would allow for coordination with broader policymaking efforts and ensure alignment with the Governor's stated priorities and the statutory framework of the CCPA.

Moreover, multiple stakeholders have emphasized that the statute permits regulation only of fully automated decision-making. Although the revised text now refers to tools that "replace" or "substantially replace" human involvement, the change does not resolve the core statutory issue. The CCPA authorizes regulation of the **"use of automated decision-making technology"**—language that plainly refers to processing conducted without human input. Where a human remains involved in the decision, the tool is not "automated" and falls outside the Agency's jurisdiction. To remain faithful to the statutory text, the definition should be limited to processing of personal information for decisions made solely through automated means.

For both legal and policy reasons, we urge the Agency to reconsider the inclusion of ADMT regulations at this time. Postponing final action would allow for further alignment with legislative developments and reduce the risk of regulatory overreach.

#### *ii. The ADMT Definition Requires Further Refinement to Ensure Clarity, Feasibility, and Alignment with Risk-Based Approaches*

If the Agency nonetheless chooses to proceed, several elements of the revised definition still require clarification to ensure the regulation remains targeted, operationally feasible, and consistent with risk-based frameworks adopted in other jurisdictions. First, the standard used to determine when a technology "substantially replaces" human decision-making should be refined. The three-pronged test in subsection (1) provides a helpful structure, but subsection (1)(b)—which requires the reviewer to consider "any other information that is relevant"—is overly vague and difficult to implement. In practice, it may be infeasible for a human reviewer to assess all information that could be deemed "relevant," especially in systems that involve complex or high-volume inputs. We recommend replacing "relevant" with "necessary" to better reflect actual decision-making protocols. Where a business has identified and documented the specific information required for a reviewer to validate or override an output, that should be sufficient under the rule.

In addition, the current formulation appears to require reviewers to analyze every output in real time, imposing a level of human involvement that could negate the efficiency and scalability benefits ADMT is intended to deliver. A more workable approach would focus on whether the reviewer is equipped with the knowledge to analyze outputs when appropriate rather than mandating review of each individual result. We therefore recommend revising subsection (1)(b) to read: *"Know how to review and analyze the output of the technology, and any other information that is necessary to make or change the decision."* The proposed alternative preserves meaningful oversight without overburdening systems that already incorporate structured review mechanisms.

Second, the exceptions listed in subsection (3) are critical but are significantly weakened by the inclusion of the qualifier "provided that they do not replace human decision-making." This caveat

undermines the purpose of enumerating common tools—such as spellcheckers, spreadsheets, and antivirus software—as excluded from the definition of ADMT. If, for example, a business relies on a calculator to support a decision, that alone should not trigger the full scope of ADMT compliance obligations. We recommend removing this qualifier entirely to maintain the clarity and utility of the exclusion.

We also recommend expanding the list of excluded tools to include other low-risk, operationally essential technologies, such as search term software, keyword filters, code debugging tools, and systems used to monitor or maintain system performance. These technologies are widely used across industries and do not present the type of privacy or autonomy risks that warrant regulation under an ADMT framework. In addition, there should be a clear carveout for tools specifically designed to detect security incidents, resist malicious, deceptive, fraudulent, or illegal activity, and assist in prosecuting those responsible. These tools are foundational to organizational compliance and consumer protection and should not fall within the scope of a rule intended to govern consequential decision-making technologies.

Finally, the inclusion of profiling within the definition of ADMT remains problematic and warrants clear limitation. As currently drafted, the regulation does not specify whether only profiling activities that replace or substantially replace human decision-making are covered, or whether all profiling—regardless of consequence—is in scope. We strongly urge the Agency to clarify that profiling qualifies as ADMT only when it is used to make decisions about individuals without meaningful human involvement.

Without this clarification, the rule risks sweeping in a wide range of tools that support—but do not independently make—decisions. As noted in our February letter, the existing definition of “profiling” under § 7001(ii) is already broad and captures technologies commonly used for employee development, such as systems that generate performance feedback, recommend training opportunities, or facilitate self-assessment. These tools are supportive in nature and are not determinative of employment or legal outcomes. Subjecting them to ADMT requirements—such as access rights, opt-outs, and explainability—would impose significant compliance burdens without advancing consumer privacy goals. This is especially concerning in employment settings, where such tools are used to enhance transparency and promote employee growth. Requiring opt-outs could force employers to revert to less efficient manual alternatives or abandon beneficial programs altogether, ultimately discouraging innovation in workforce management.

## **b. Sec. 7001(ii): Profiling**

The definition of “profiling” remains unchanged from prior drafts and continues to raise significant implementation concerns due to its breadth and lack of limiting principles. It broadly encompasses “any form of automated processing of personal information” used to evaluate or predict a range of personal attributes—such as intelligence, aptitude, preferences, behavior, location, and movements. Such a broad formulation captures a wide variety of technologies, including low-risk, non-decision-making, or protective systems, and applies regulatory obligations without regard to context, impact, or purpose.

In addition, the definition imposes regulatory requirements on all automated analysis, regardless of whether it results in meaningful consequences for individuals. Technologies that analyze behavioral patterns to improve operational efficiency or recommend content based on user preferences are grouped together with systems used to determine access to housing, employment, or credit. A more practical approach, consistent with frameworks in Colorado and Virginia, would establish a two-step process to determine regulatory applicability. First, it would ask whether data is being processed for profiling. Second, it would assess whether the profiling is used to make legally or otherwise significant decisions about individuals, such as those impacting employment eligibility, access to credit, or legal rights. Profiling that supports operational decisions, enhances public safety, or improves service delivery without producing legal consequences should not be treated the same as profiling used to make eligibility determinations.

To avoid overreach and preserve the integrity of protective technologies, the definition of profiling should be narrowed to exclude systems used for public safety, physical security, and fraud prevention. At the same time, the overall framework should focus regulatory obligations on the subset of profiling activities that result in legally or materially significant effects for individuals.

These changes would bring California’s approach into alignment with other leading state frameworks and ensure that the regulation targets high-impact scenarios without imposing unnecessary burdens on routine or safety-driven data uses.

**c. Sec. 7001(ee): Physical or Biological Identification or Profiling**

To ensure clarity and avoid duplication with existing statutory provisions, we respectfully recommend removing the proposed definition of “physical or biological identification or profiling,” and all references thereto in the proposed draft regulations. The CCPA already defines biometric information as data derived from physiological, biological, or behavioral characteristics used to establish individual identity. This definition substantially overlaps with the proposed new category, which focuses on identifying or profiling a consumer based on physical or biological traits. As a result, businesses processing biometric information would already be required to conduct risk assessments under the current framework. Layering on a separate requirement for “physical or biological identification or profiling” would create duplicative obligations without yielding additional consumer protections.

In practice, the overlap could lead to confusion over when multiple assessments are required for a single activity and introduce unnecessary operational burdens. For example, a business using biometric data to train or deploy ADMT could be subject to risk assessments both under the sensitive data provisions and again under this new category—even where the risks and use cases are functionally identical.

To the extent the Agency seeks to address concerns related to the training or use of ADMT that processes physical or biological characteristics for profiling purposes, those activities are already likely to fall under existing obligations for sensitive personal information. Introducing a separate category for similar conduct is unnecessary to advance consumer privacy and may instead complicate compliance for businesses and enforcement for the Agency. Accordingly, we recommend omitting the proposed definition to maintain coherence with the statute and avoid redundant requirements that increase costs without improving consumer privacy protections.

**d. Sec. 7001(aaa): Sensitive Location**

The introduction of “sensitive location” as a defined term and regulatory trigger in the proposed draft regulations is not authorized by the CCPA. While the law provides the Agency with authority to require risk assessments in connection with certain types of processing, that authority is expressly limited to situations where the processing of personal information—particularly sensitive personal information—presents a significant risk to consumers’ privacy or security.

The enabling statute, Section 1798.185(a)(14)(B), empowers the Agency to require a risk assessment “with respect to [a business’s] processing of personal information, including whether the processing involves sensitive personal information.” The scope of this provision is clear: it contemplates risk assessments where there is elevated risk associated with the type of personal information or manner of processing. It does not authorize the Agency to create entirely new categories of data—such as location-based designations—that are not grounded in the statute.

The proposed draft regulations’ introduction of “sensitive location” as a distinct concept—defined to include a wide array of physical spaces such as churches, schools, shelters, and political offices—imposes new risk assessment obligations based not on the nature of the personal information, but on the location where a person happens to be. Section 7150(b)(5) would require risk assessments for the use of automated processing to infer consumer traits based on their presence at such locations. This expands the scope of regulated conduct far beyond what the statute permits and introduces substantial compliance burdens without clear statutory justification.

Importantly, the statute already includes tools to address concerns related to data collected in sensitive contexts. If a business processes sensitive personal information (such as precise geolocation or health data) derived from a consumer’s presence in a particular place, that processing may already require a risk assessment. Creating an entirely new trigger based solely on the nature of the location—without statutory basis—undermines the statutory structure and creates legal uncertainty for regulated businesses.

Accordingly, we respectfully urge the Agency to remove all references to “sensitive location.” The regulation of high-risk processing must remain tethered to the categories and triggers expressly authorized in statute: personal information, sensitive personal information, and the nature and scope of processing activities.

**e. Sec. 7001(ddd): Significant Decision**

We appreciate that the revised regulations relocate the definition of “significant decision” to the general definitions section and narrow its scope by removing coverage of decisions related to advertising, insurance, criminal justice, or access to “essential goods and services.” However, we remain concerned that the definition remains overly broad and continues to capture routine or low-risk business activities that are already regulated under other legal frameworks. Further refinement is needed to ensure that the regulation targets truly impactful decisions while avoiding operational overreach and regulatory duplication.

With respect to “financial or lending services,” the inclusion of decisions related to the extension of credit is more clearly tied to consumer impact, but the remainder of the category sweeps in activities that are routine, already regulated, and not appropriately treated as “significant decisions.” The definition currently includes services such as “transmitting or exchanging funds,” “provision of deposit or checking accounts,” “check cashing,” and “installment payment plans”—activities that fall squarely within the scope of existing financial services laws, including the Gramm-Leach-Bliley Act (GLBA). We therefore recommend deleting the reference to “transmitting or exchanging funds” and refining the language around accounts to refer only to the “opening of deposit or checking accounts,” rather than the broader and less precise term “provision.” Additionally, the definition should include a clarifying express exclusion for decisions made to prevent, detect, or respond to fraud or other malicious activity, which are protective in nature and should not be subject to the same requirements as determinations that bear directly on consumer rights or access to services.

The inclusion of employment-related decisions that extend beyond hiring and termination also raises significant issues. While determinations such as hiring, promotion, or dismissal may carry legal and economic consequences for individuals, the addition of categories like “allocation or assignment of work” and “salary, hourly or per-assignment compensation, incentive compensation such as a bonus, or another benefit” risks capturing a wide range of internal HR processes and administrative functions that are neither novel nor high-risk. For instance, assigning projects or administering payroll—especially when aided by automated tools—should not be subject to the same obligations as systems making determinative employment decisions. The breadth and ambiguity of this provision may create unnecessary compliance complexity and expand the regulation beyond its intended scope. To address this, we recommend deleting subsection (4)(B). In the alternative, the language should be narrowed to focus on consequential employment decisions—such as hiring, promotion, or termination—while clearly excluding routine functions like work allocation and compensation administration.

**f. Sec. 7200: When a Business’s Use of ADMT is Subject to Article 11**

Section 7200(b) should be revised to remove the first sentence, which implies that compliance is required for any use of ADMT occurring prior to January 1, 2027. As drafted, the language could be interpreted to impose retroactive obligations, even where ADMT was no longer in use as of the effective date. Imposing requirements on discontinued systems offers no privacy benefit and would create unnecessary compliance burdens.

**g. Sec. 7220: Pre-use Notice Requirements**

***i. Scope of Requirement***

The regulation in Section 7220 imposes a pre-use notice obligation that goes beyond the statutory authority granted under the CCPA and should be revised to reflect the limits set by Cal. Civ. Code § 1798.185. The statute authorizes the Agency to adopt regulations concerning access and opt-out rights related to the use of ADMT, but it **does not** authorize the imposition of a separate notice obligation in contexts where no such rights apply. As explained in our February letter, requiring pre-



use notices in addition to access disclosures results in overlapping obligations without a clear legal basis and risks confusing consumers.

The current formulation applies the pre-use notice requirement even where ADMT is used solely for exempt purposes which are not subject to consumer access or opt-out rights. Mandating disclosures in these cases not only imposes unnecessary compliance costs but could also reduce the effectiveness of safety tools by revealing details about sensitive processes. For example, disclosing the existence or purpose of security analytics in public-facing privacy notices could inadvertently compromise protective systems or open them to manipulation. To bring the regulation in line with the statutory framework and reflect practical deployment realities, the pre-use notice requirement should be limited to ADMT uses that trigger consumer access or opt-out rights. We therefore recommend the following revision to Section 7220(a): *“A business that uses automated decision-making technology as set forth in section 7200, subsection (a), and subject to the exceptions in section 7221(b) and section 7222(a)(1), must provide consumers with a Pre-use Notice.”*

## **ii. Content of the Pre-Use Notice**

We appreciate the Agency’s revisions to Section 7220(c)(5), which represent a meaningful improvement by shifting away from requiring disclosure of ADMT “logic” and “key parameters” and instead focusing on how personal information is processed to make significant decisions. The addition of subsection 7220(d) appropriately protects proprietary and security-sensitive information. However, subsections (A) and (B) still raise practical concerns. Requiring detailed descriptions of outputs and how they are used may result in technical disclosures that offer little value to consumers and risk causing confusion. A more effective approach to mitigating harm would prioritize robust internal testing under Section 7223 over granular pre-use disclosures.

Moreover, there is also ongoing ambiguity regarding the relationship between the disclosures required in subsection (A) and those under the access right in Section 7222(b)(2). Subsection (A) requires a plain-language explanation of how personal information is processed to make a decision, while the access provision requires disclosure of the ADMT logic. Without further clarification, the overlap between these requirements could create uncertainty about how much information must be disclosed in different contexts and increase the complexity of implementation. We recommend clarifying the interaction between these provisions to promote consistency and avoid duplicative or conflicting obligations.

## **iii. Clarifying Exemption Language**

The language Section 7220(d)(2)(B) and Section 7222(c)(2)(B)—“resist malicious, deceptive, fraudulent, or illegal actions”—does not fully reflect the range of protective activities businesses engage in to secure systems and safeguard consumers. Narrowly framing the provision around “resistance” may exclude other critical functions such as prevention, detection, and investigation, which are essential components of a comprehensive security posture.

To more accurately capture standard security practices and avoid disclosures that could undermine system defenses, we recommend revising both provisions to state: “Prevent, detect, investigate, and resist malicious, deceptive, fraudulent, or illegal actions directed at the business or at consumers, or to prosecute those responsible for those actions; or” This revision aligns with common cybersecurity frameworks and ensures the regulation protects the operational integrity of security systems without diminishing consumer transparency where appropriate.

## **h. Sec. 7221: Requests to Opt-Out of ADMT**

### **i. Method of Opt-Out**

Section 7221(i) permits businesses to offer consumers choices regarding specific uses of ADMT, provided a single, comprehensive opt-out is also presented. While offering granular options is beneficial, our previous concerns about the inflexibility of the overall opt-out framework remain unresolved. The current approach assumes that all uses of ADMT pose harm, overlooking the many ways these tools enhance efficiency, promote objectivity, and reduce human bias. A blanket opt-out requirement disregards the value ADMT can offer to consumers and businesses alike. In many cases, enabling automation reduces error, accelerates service delivery, and supports more

consistent outcomes. Imposing a one-size-fits-all opt-out undermines those benefits and forces organizations to maintain redundant manual systems—often at significant cost—without corresponding gains in consumer protection.

Moreover, requiring multiple designated opt-out methods, as required by Section 7221(c), adds operational burdens, particularly for digital-first businesses. Allowing companies to integrate ADMT opt-outs into their existing communication channels would preserve accessibility while avoiding duplicative or fragmented processes. Requiring overlapping disclosures, such as layering ADMT notices on top of cookie banners, risks overwhelming users and diluting the effectiveness of both.

Tailored opt-out notices that reflect specific use cases—such as fraud prevention, eligibility screening, or personalized experiences—would give consumers more meaningful context to assess tradeoffs and make informed choices. We encourage the Agency to revise this provision to permit greater flexibility in how opt-out mechanisms are designed and presented, particularly for low-risk or high-value use cases. Doing so would support a more nuanced and functional regulatory approach.

## ***ii. Opt-Out Exceptions***

We appreciate the Agency’s addition of exceptions in Section 7221(b)(2) and (3), which acknowledge that not all uses of ADMT in employment and education contexts necessitate consumer opt-out rights. These carveouts represent an important recognition that ADMT, when used appropriately, can enhance fairness, efficiency, and consistency in operational decisions. However, the current structure of the exceptions introduces limitations that could inadvertently restrict their application and increase compliance uncertainty.

First, each exception is currently limited to circumstances in which the ADMT is used “solely” for the specified purpose—either for assessing an individual’s ability to perform in an employment or educational context or for allocating work or compensation. As drafted, this could be read to exclude any ADMT system that serves additional, non-significant business functions, such as improving workflow or optimizing resource distribution, even if those functions do not independently constitute “significant decisions” as defined in § 7001(ddd). So long as ADMT is not being used to make other significant decisions, the exception should apply. We recommend removing the word “solely” from both subsections to avoid unduly narrowing the scope of these provisions.

Second, the current standard that a business “ensures” the ADMT works as intended and does not unlawfully discriminate sets an unreasonably high bar. A strict “ensures” requirement could be interpreted as creating a strict liability standard, which is both impractical and inconsistent with broader regulatory norms. Instead, the regulation should reflect a reasonableness standard that accounts for what is technically feasible and commercially reasonable under the circumstances. The language should also recognize that ADMT deployers may reasonably rely on documentation, assessments, or other assurances provided by the developer, particularly where the deployer lacks the access or expertise to independently assess the system. To reflect these changes, we recommend revising both subsections (2)(B) and (3)(B) as follows: *“(B) Takes reasonable measures to ensure that the automated decision-making technology works as intended for the business’s proposed use and does not unlawfully discriminate based upon protected characteristics, which may include reliance on a documented assessment or guidance provided by the developer.”*

Finally, consistent with the CCPA and other state privacy laws, the regulation should preserve robust exemptions for fraud prevention, detection, and enforcement activities. Section 7221(b)(1)(B) should be clarified to ensure that the opt-out right does not apply to processing conducted to prevent, detect, resist, or respond to malicious, deceptive, fraudulent, or illegal actions directed at the business, including efforts to identify and prosecute those responsible. Without this clarity, the provision could be misinterpreted in a way that hinders critical risk mitigation activities. We, therefore, recommend revising the language to explicitly confirm that processing carried out for fraud prevention and response purposes remains outside the scope of the opt-out right.

## i. Sec. 7222: Requests to Access ADMT

We acknowledge and appreciate the Agency's revision to Section 7222(a), which limits the access right to situations where a business uses ADMT to make a "significant decision." We also support the Agency's inclusion of language in Sections 7220(d) and 7222(c) clarifying that businesses are not required to disclose trade secrets or information that would compromise security, fraud detection, or proprietary models.

However, the current structure of Section 7222 continues to raise serious implementation concerns and deviates from the risk-based approach contemplated in Cal. Civ. Code § 1798.185(a)(16). That provision authorizes the Agency to issue regulations requiring disclosure of "meaningful information about the logic involved in [ADMT] and the likely outcome of the process with respect to the consumer," but it does not mandate individualized, consumer-specific responses. Consumers already have separate access rights under the CPRA that allow them to request their personal data, including inputs and outputs related to ADMT. Duplicating or expanding those rights to require explanation of the decision-making methodology itself is unnecessary, inconsistent with the statute, and likely to result in significant harm to innovation and security.

Nevertheless, we recommend the following clarifications and revisions to Section 7222:

- **Limit Access Obligations to Adverse Decisions:** A company should not be required to provide logic-based explanations where no harm or adverse outcome is involved—such as a pre-approval for credit, a job interview invitation, or an automatically awarded benefit. This approach is consistent with longstanding federal frameworks such as the Fair Credit Reporting Act (FCRA) and the Equal Credit Opportunity Act (ECOA), which require transparency only in the event of adverse action. No other U.S. privacy law mandates businesses to explain the internal mechanics of favorable decisions.
- **Avoid Consumer-Specific Disclosures of Logic or Use:** Section 7222(b)(2) requires businesses to explain how ADMT processed personal information to generate a specific output, and Section 7222(b)(3) requires explanation of how that output was used to make a decision. These provisions create an untenable compliance burden and risk disclosure of proprietary business logic. If retained, these obligations should be reframed to allow a general explanation of the range of potential outputs, not a consumer-specific output or its internal application, particularly where the output does not itself constitute personal information. Moreover, compelling businesses to disclose detailed explanations of how ADMT was used (or will be used) to make a decision risk enabling individuals to game or manipulate the system.
- **Harmonize with Existing Exceptions and Risk-Based Carveouts:** We strongly urge the Agency to integrate the same exceptions recognized in Section 7221(b) for employment-related ADMT use into this section. If the definitions of "significant decision" or "ADMT" are interpreted broadly, screening tools or interim hiring systems could trigger individualized access obligations—regardless of whether a final decision has been made. Such a framework would eliminate the very efficiencies ADMT is meant to provide in high-volume, rapid-response environments such as recruiting or workforce allocation.

## IV. ARTICLE 3 – BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS

The example in Section 7027(m)(2)(B) should better reflect the full range of legitimate purposes for scanning outgoing employee emails. Limiting the exception solely to the prevention of data leakage overlooks other critical functions, such as identifying policy violations involving illegal conduct, conflicts of interest, or unethical behavior. These activities are often necessary to uphold internal compliance standards and meet legal or regulatory obligations.

Accordingly, we recommend deleting the second sentence of this provision. In the alternative, to ensure appropriate flexibility while maintaining consumer protections, we recommend the following revision: "*A business may scan employees' outgoing emails to prevent employees from leaking sensitive personal information outside of the business **or violating company policy.** However, scanning the **employee's outgoing** emails for other purposes would not fall within this exception to the consumer's right to limit.*"



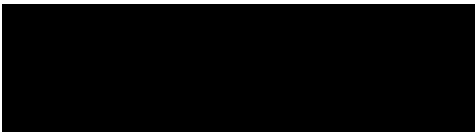
\* \* \*

Finally, we want to flag that the amendments to the existing regulations—many of which impose new requirements—do not specify a compliance timeline. Several changes include mandatory updates to Privacy Policy disclosures and the conversion of previously optional disclosures into mandatory ones. In addition, the regulations introduce a new process for handling “requests to know” and “requests to correct” regarding certain sensitive data elements. This process must enable consumers to verify specific pieces of information, including Social Security numbers—raising significant implementation and security considerations.

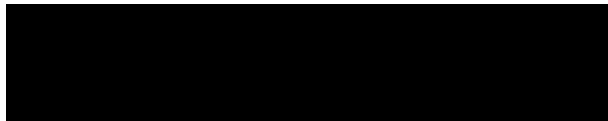
Businesses will need time to design and implement a secure and effective process that both protects sensitive data and meets consumer expectations. ***Accordingly, we strongly urge the Agency to set January 1, 2027, as the compliance date for all amendments to the existing regulations.***

While we appreciate the Agency’s efforts to scale back portions of the rulemaking, this latest draft still introduces new concepts and obligations that extend beyond the intended scope of the CCPA. These changes—however well-intended—create substantial compliance burdens with questionable benefits for consumers. We urge the Agency to reassess whether the current regulatory approach strikes the right balance between consumer protection and regulatory impact. A more measured and targeted rulemaking would better serve Californians while avoiding unnecessary economic harm.

Respectfully Submitted,



Counsel, State Privacy & Security Coalition



William C. Martinez  
Counsel, State Privacy & Security Coalition

**Grenda, Rianna@CPPA**

---

**From:** Steve Ball [REDACTED]  
**Sent:** Friday, May 9, 2025 8:31 PM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

AI is the scourge of society and used by technology companies to harness personal information for their own gain to the detriment of California citizens. I request you remove these alterations and restore the original draft.

**Grenda, Rianna@CPPA**

---

**From:** Andy Jung <ajung@techfreedom.org>  
**Sent:** Monday, June 2, 2025 1:44 PM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations 6.2.2025  
**Attachments:** TF Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations 6.2.2025.pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

I have attached TechFreedom's public comment, dated June 2, 2025, on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations.

--

Andy Jung  
Associate Counsel  
TechFreedom | @TechFreedom | @AndyJungTech  
<https://techfreedom.org/>



**Comments of**

**TechFreedom**

Andy Jung<sup>i</sup>

**In the Matter of**

*Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations*

**June 2, 2025**

---

<sup>i</sup> Andy Jung is Associate Counsel at TechFreedom, a nonprofit, nonpartisan technology policy think tank. He can be reached at [ajung@techfreedom.org](mailto:ajung@techfreedom.org).

## TABLE OF CONTENTS

Introduction .....	1
I. The CCPA Is a Privacy Statute, Not an Artificial Intelligence Regulation: Stretching Its Authority Risks Undermining the Agency.....	2
II. Conclusion .....	3

## INTRODUCTION

TechFreedom is a nonprofit, nonpartisan think tank based in Washington, D.C. It is dedicated to promoting technological progress that improves the human condition. It seeks to advance public policy that makes experimentation, entrepreneurship, and investment possible and thus unleashes the ultimate resource: human ingenuity. TechFreedom champions a light-touch approach to artificial intelligence regulation<sup>1</sup> that promotes open-source development,<sup>2</sup> protects consumers from concrete harms,<sup>3</sup> and upholds free speech under the First Amendment.<sup>4</sup> TechFreedom regularly engages on privacy issues ranging from data collection and security<sup>5</sup> to the Fourth Amendment<sup>6</sup> to children's online privacy.<sup>7</sup>

---

<sup>1</sup> Corbin Barthold, 397: *AI Policy Potpourri (Part One)*, Tech Policy Podcast (Feb. 17, 2025), <https://podcast.techfreedom.org/episodes/397-ai-policy-potpourri-part-one>; Andy Jung, *Don't California My Texas: Stargate Edition*, TECHFREEDOM (Jan. 24, 2025), <https://techfreedom.substack.com/p/dont-california-my-texas-stargate>; Andy Jung, *'Unregulated AI' is a myth*, THE ORANGE COUNTY REGISTER (Apr. 1, 2024), <https://www.ocregister.com/2024/04/01/unregulated-ai-is-a-myth/>.

<sup>2</sup> TechFreedom, Comment on Managing Misuse Risk for Dual-Use Foundation Models (Sept. 9, 2024), <https://techfreedom.org/wp-content/uploads/2024/09/TechFreedom-NIST-AI-800-1-Comments.pdf>; Andy Jung, *California's AI Bill Threatens To Derail Open-Source Innovation*, REASON (Aug. 8, 2024), <https://reason.com/2024/08/13/californias-ai-bill-threatens-to-derail-open-source-innovation/>; *TechFreedom Delivers Remarks at FTC's August Open Commission Meeting*, TECHFREEDOM (Aug. 1, 2024), <https://techfreedom.org/techfreedom-delivers-remarks-at-ftcs-august-open-commission-meeting/>.

<sup>3</sup> Andy Jung, *The FTC, AI, and Its Existing Authority*, STATE OF THE NET (Feb. 12, 2024), <https://sotn24.sched.com/event/1Z1C0/the-ftc-ai-and-its-existing-authority-how-the-commission-has-and-will-apply-its-authority-to-artificial-intelligence>; *TechFreedom Delivers Remarks at FTC Open Commission Meeting*, TECHFREEDOM (May 19, 2023), <https://techfreedom.org/techfreedom-delivers-remarks-at-ftc-open-commission-meeting-2/> (Remarks of Andy Jung).

<sup>4</sup> TechFreedom, Comment on Disclosure and Transparency of Artificial Intelligence-Generated Content in Political Advertisements (Sept. 19, 2024), <https://techfreedom.org/wp-content/uploads/2024/09/TechFreedom-FCC-AI-Comments.pdf>; Letter from TechFreedom to the Senate Committee on Rules and Administration Re: S. 2770, The Protect Elections from Deceptive AI Act (May 14, 2024), <https://techfreedom.org/wp-content/uploads/2024/05/Coalition-Letter-S.-2770-The-Protect-Elections-from-Deceptive-AI-Act.pdf>; Ari Cohn, *A.I. Panic is Causing First Amendment Hallucinations...in Humans*, TECHFREEDOM (Jan. 29, 2024), <https://aricohn.substack.com/p/ai-panic-is-causing-first-amendment>.

<sup>5</sup> *TechFreedom Delivers Remarks at FTC's Commercial Surveillance and Data Security Public Forum*, TECHFREEDOM (Sept. 8, 2022), <https://techfreedom.org/techfreedom-delivers-remarks-at-ftcs-commercial-surveillance-and-data-security-public-forum/>; TechFreedom, Comment on Trade Regulation Rule on Commercial Surveillance and Data Security (Nov. 21, 2022), <https://techfreedom.org/wp-content/uploads/2022/11/TechFreedom-Comments-Trade-Regulation-Rule-on-Commercial-Surveillance-and-Data-Security.pdf>.

<sup>6</sup> Corbin Barthold, 395: *The Digital Fourth Amendment — With Orin Kerr*, Tech Policy Podcast (Jan. 23, 2025), <https://podcast.techfreedom.org/episodes/395-the-digital-fourth-amendment-with-orin-kerr>.

<sup>7</sup> TechFreedom, Comment on Children's Online Privacy Protection Rule (Mar. 11, 2024), <https://techfreedom.org/wp-content/uploads/2024/03/TechFreedom-COPPA-Rule-Comments-3.11.2024.pdf>.

We write to commend the California Privacy Protection Agency (the Agency) for amending the Proposed Regulations on Automated Decisionmaking Technology (ADMT regulations) in response to comments from the public. In our initial comments, TechFreedom implored the Agency to narrow the proposed definition of “automated decisionmaking technology” to cover only automated technologies that directly implicate consumer privacy.<sup>8</sup> We warned the agency that the proposed ADMT regulations threatened to shoehorn misguided artificial intelligence rules into the California Consumer Privacy Act (CCPA)—which is a privacy law, not an artificial intelligence regulation.

The Agency responded by striking all references to “artificial intelligence” from the modified ADMT regulations.<sup>9</sup> Consequently, the Agency has addressed TechFreedom’s primary concerns in the ADMT rulemaking.

### **I. The CCPA Is a Privacy Statute, Not an Artificial Intelligence Regulation: Stretching Its Authority Risks Undermining the Agency.**

Throughout the ADMT rulemaking process, CCPA architect and Agency board member Alastair Mactaggart has highlighted the risk and disutility of stretching the statute to regulate artificial intelligence:<sup>10</sup>

*...[T]he ADMT language that’s in these regulations seeks to regulate much more than privacy. It seeks to basically regulate all use of AI with respect to humans much more stringently than any law that passed out of the legislature last year.*

In addition, since we’ve last met, the governor’s task force on AI regulation, which our fellow board member Ms. Nonnecke participated in, has issued guidelines for AI regulation. And the legislature is currently considering, I think it’s safe to say, dozens of bills aimed at AI regulation.

There’s a robust effort in California to regulate AI now. And yet here we are, trying to regulate AI through the back door of privacy. *Let me repeat again, this is a privacy statute, not an AI regulation statute.*

---

<sup>8</sup> TechFreedom, Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations § V (Feb. 19, 2025), <https://techfreedom.org/wp-content/uploads/2025/02/TF-Public-Comment-on-CCPA-Updates-Cyber-Risk-ADMT-and-Insurance.pdf#page=8>.

<sup>9</sup> Modified Text of Proposed ADMT Regulations (May 9, 2025), CALIFORNIA PRIVACY PROTECTION AGENCY, [https://cppa.ca.gov/regulations/pdf/ccpa\\_updates\\_cyber\\_risk\\_admt\\_mod\\_txt\\_pro\\_reg.pdf](https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_mod_txt_pro_reg.pdf). *See also* Explanation of Modified Text of Proposed Regulations at 1, CALIFORNIA PRIVACY PROTECTION AGENCY (May 1, 2025), [https://cppa.ca.gov/meetings/materials/20250501\\_item4\\_mod\\_text.pdf](https://cppa.ca.gov/meetings/materials/20250501_item4_mod_text.pdf) (“Deleted definition of ‘artificial intelligence’ as unnecessary and removed corresponding references.”).

<sup>10</sup> *See* TechFreedom, *supra* note 8, at 4-5 (quoting Mactaggart, who criticized the breadth of the proposed ADMT regulations and raised concerns that they would fail to protect consumer privacy).

If we enact these regulations, this will be a complete gift to those seeking federal preemption of our entire bill and agency. This action will play right into the hands of those seeking to get rid of our agency permanently and provide concrete evidence to the critics out there that we're off course and need to be reined in.<sup>11</sup>

Artificial intelligence is beyond the scope of the CCPA and the Agency's core competence. As artificial intelligence continues to proliferate, the Agency must resist the urge to stretch its authority to regulate the technology. Doing so would only serve to validate the concerns of the Agency's many critics.<sup>12</sup>

## **II. Conclusion**

If the Agency moves forward with the ADMT regulations, it should retain the amended text from May 9, 2025, which deleted all references to "artificial intelligence." Moving forward, the Agency must not attempt to regulate artificial intelligence as a technology. Instead, the Agency may only regulate artificial intelligence—and automated technologies more generally—to the extent they directly implicate consumer privacy.

Respectfully submitted,

\_\_\_\_\_/s/\_\_\_\_\_  
Andy Jung  
Association Counsel  
TechFreedom  
ajung@techfreedom.org  
1500 K Street NW, Floor 2  
Washington, DC 20005

June 2, 2025

---

<sup>11</sup> California Privacy Protection Agency Board, Transcription of Recorded Public Meeting at 34-35 (Apr. 4, 2025), [https://cppa.ca.gov/meetings/materials/20250404\\_audio\\_transcript.pdf#page=34](https://cppa.ca.gov/meetings/materials/20250404_audio_transcript.pdf#page=34) (emphasis added).

<sup>12</sup> See, e.g., Taylor Semakula, *Governor Newsom Urges Caution on CPPA's Proposed AI Regulations*, AMERICAN BAR ASSOCIATION (May 2, 2025), [https://www.americanbar.org/groups/health\\_law/news/2025/5/governor-newsom-urges-caution-cppas-proposed-ai-regulations/](https://www.americanbar.org/groups/health_law/news/2025/5/governor-newsom-urges-caution-cppas-proposed-ai-regulations/); *CalChamber Submits Comments on CPPA's Proposed Privacy and Security Rules; Raises Concerns and Calls for Extended Compliance Timeline*, CALIFORNIA CHAMBER OF COMMERCE (Feb. 19, 2025), <https://advocacy.calchamber.com/2025/02/19/calchamber-submits-comments-on-cppas-proposed-privacy-and-security-rules-raises-concerns-and-calls-for-extended-compliance-timeline-2/>.



**Grenda, Rianna@CPPA**

---

**From:** Robert Boykin <rboykin@technet.org>  
**Sent:** Monday, June 2, 2025 1:42 PM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations  
**Attachments:** TechNet ADMT Response Letter\_Final 6.2.2025.pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Resending on letterhead

--

Robert Boykin  
Executive Director | California & the Southwest  
TechNet | The Voice of the Innovation Economy  
(c) [REDACTED] | [rboykin@technet.org](mailto:rboykin@technet.org)  
Twitter: @TechNetSouthwest





**TECHNET**  
THE VOICE OF THE  
INNOVATION ECONOMY

TechNet Southwest | Telephone 408.898.7145  
915 L Street, Suite 1270, Sacramento, CA 95814  
[www.technet.org](http://www.technet.org) | @TechNetSW

June 2, 2025

California Privacy Protection Agency  
2101 Arena Blvd.  
Sacramento, CA 95834

**Re: PROPOSED REGULATIONS FOR CALIFORNIA CONSUMER PRIVACY ACT (CCPA) UPDATES, CYBERSECURITY AUDITS, RISK ASSESSMENTS, AUTOMATED DECISIONMAKING TECHNOLOGY (ADMT), AND INSURANCE COMPANIES**

Dear Board Members,

On behalf of TechNet and our member companies, I am writing to provide feedback on the latest draft regulations relating to the Proposed Rulemaking pertaining to Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking. TechNet appreciates the work the California Privacy Protection Agency ("CPPA/the Agency") has done so far and appreciates your continued public engagement throughout this rulemaking process to incorporate the concerns of all stakeholders.

In particular, we appreciate the board's emphasis on wanting to harmonize the CPPA's rules with other jurisdictions and evidence-based rulemaking. Given the pace of change in automated technology and the laws and regulations governing this technology, we want to ensure California's approach serves consumers for the long-term while also maximizing interoperability for businesses to defend California's standing as a global leader in innovation.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet. Together, they represent over 4.5 million employees and countless customers across information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

While we appreciate many of the changes made so far, we also recognize that by the agency's own estimates the compliance costs of these regulations are projected to reach over \$1.2 billion in the first year alone. Below are several concerns about the latest version of the rules and proposed fixes to harmonize the rules with other jurisdictions and reduce compliance costs while maintaining robust consumer privacy protections.

### **Key Definitions Remain Overly Broad and Would Include Tools and Decisions Beyond the Intended Scope**

While we appreciate the efforts to refine and narrow definitions from previous proposals, the current version would include tools that are beyond the agency's intended scope, don't have a meaningful connection to privacy, and create unnecessary compliance risks for businesses without reducing risks for consumers.

For example, while narrowing the definition of ADMTs to tools that "replace" or "substantially replace" human-decision making, this definition still risks capturing common business technologies. For example, the new language in § 7001(e)(1)(B) that requires human review of all information "relevant" to making the decision is ambiguous and sets an unreasonable standard of reviewing all information rather than just the information necessary for a significant decision. Plus, § 7001(e)(2) still considers all "profiling" to count as ADMT, which could capture common business technologies including, among other things, basic software or systems that "analyze" ordinary workplace conduct like "performance at work" or "reliability". This would sweep in tools designed to merely track and analyze worker behavior even if it does not involve any decisionmaking or present any privacy risks within the scope of this regulation.

Another concern is that the current definition could be read to cover emerging agentic AI systems that automate routine business functions, particularly under the current definition of "significant decision" as it relates to workplace decisions, which we detail further in the next section. Agentic tools are designed to autonomously solve problems, plan, and perform mundane tasks to replace human effort. These are not "decisions" of consequence in the sense intended by the CPPA and should not be subject to the same regulatory burdens as systems used for lending, hiring, or housing determinations.

We are also concerned about the addition of "provided that they do not replace human decisionmaking" to the end of the list of exemptions of common business

tools in § 7001(e)(3). This additional language undermines the purpose of the exemption in the first place.

Finally, we recommend explicitly excluding first-party advertising from the definition of “Request to opt-in to sale/sharing.” For example, the definition could be amended to include the following sentence: “The use of personal information for first-party advertising does not constitute a ‘request to opt-in to sale/sharing’ and does not require separate consent.”

**The New Definition of “Significant Decision” also Risks Incorporating Decisions Beyond the Statutory Scope of the Agency’s Rules.**

We appreciate the willingness to refine the definition of “significant decision” and focus on decisions that result in the provision or denial of services. However, we urge revisions such as striking references to “allocation or assignment of work.” Regarding employment, this definition continues to go beyond hiring and firing to also include the allocation or assignment of work and decisions about compensation for both employees and independent contractors. Decisions about allocations of work or individual tasks are often routine operational business guided by software tools that not only improve efficiency but often support compliance with labor regulations. Their inclusion within the ADMT framework will create compliance burdens without proportional consumer benefit as these decisions do not present a significant privacy risk, exactly the type of over-inclusion Governor Newsom identified in his April letter to this board. This category is extremely broad and, along with the definition of automated decisionmaking technology, will capture basic tools for assigning work hours, implementing schedules, or matching consumers to workers for the benefit of workers and consumers.

While we appreciate the effort to better define “financial or lending services” in this latest draft and support many of the changes, we urge revisions by either dropping “financial” or narrowing the scope of the new definition to align with other jurisdictions. Including financial services, as defined, would sweep in tools used for common, non-credit purposes. For example, including “transmitting or exchanging funds” could apply to every instance of lawful payment activity or money movement performed by the 90% of consumers who use digital payments. Automated technologies help consumers efficiently pay bills, helps small businesses collect payment and pay wages, and facilitate payments between friends and families. Without revision this new definition risks preventing individuals and small businesses from accessing the financial products they rely on. As written, this new definition could also impact the AI tools companies use to comply with financial

rules and regulations by efficiently screening transactions and identifying potential risks in real-time to reduce fraud and protect consumers. AI-enabled risk detection and monitoring streamlines compliance efforts and allow human oversight to focus on the highest-risk activities.

**Cybersecurity Audit Requirements Can be Further Aligned with Best Recognized Best Practice**

While improvements have been made to this section, the requirement for a comprehensive audit each year remains excessive. Burdensome, prescriptive compliance requirements divert resources away from protecting the enterprise and personal information. Instead, providing information to auditors has to take precedence. This undermines a business's security posture and misappropriates limited resources.

We propose the Agency only require a full audit as detailed in section 7123(b) "at least once every three years". In the intervening years of the three year cycle, a business should only have to complete an intervening audit or assessment to account for materially updated or new conditions. Depending on the assessment of risk, it is possible that certain components/domains could be audited more frequently than every three years to account for new conditions, but the regulation shouldn't prescribe the entire universe to be audited annually.

Additionally, while we appreciate the inclusion of the NIST Cybersecurity Framework as an example of industry best practice that could be used in lieu of the security requirements in this regulation, we also recommend including additional examples of acceptable frameworks such as NIST 800-53 and ISO 2701.

Another improvement could include explicitly recognizing that Service Organization Control 2 (SOC2) and/or Payment Card Industry Data Security Standard (PCI DSS) reviews satisfy the requirement. For example, the CPPA could amend § 7123(f) to say: "A business may utilize a cybersecurity audit, assessment, or evaluation that it has prepared for another purpose, provided that it sufficiently satisfies the requirements of this Article, either on its own or through supplementation. For example, a business may have engaged in an audit requirement that uses the National Institute of Standards and Technology Cybersecurity Framework 2.0 and meets all of the requirements of this Article, or a business may have completed a Service Organization



Control 2 (SOC2) or Payment Card Industry Data Security Standard (PCI DSS) review.”

**An Overly Prescriptive Risk Assessment Framework Risks Creating Burdensome Compliance Requirements**

As referenced by the Board during hearings, there is active legislation in California that could establish statutory requirements for algorithmic risk assessments. Finalizing regulatory language ahead of legislative outcomes risks confusion and inconsistency. We recommend deferring or minimizing prescriptive risk assessment language until the legislative landscape settles.

In addition, the new definitions of significant risk go beyond the underlying statutory text. For example, including profiling in a sensitive location in § 7150(b)(5) risks pulling in systems that perform innocuous location-based inferences, such as whether a user is located on a college campus, under the umbrella of high-risk profiling. The rule should make clear that only sensitive and consequential uses of location profiling, such as detecting protected characteristics, trigger obligations. Without this clarity, basic location-tagging or geofencing tools may fall under onerous ADMT provisions requiring opt-outs and risk assessments.

Another significant concern in the same subsection is including training an AI system or ADMT as a trigger for risk assessments, which would apply regardless of whether or not the resulting model is deployed. Additional requirements for training ADMTs are overly broad and redundant. ADMT requirements should only apply when an ADMT is used for a significant decision that will affect an individual, but the current definition of “intends to use” has created confusion whether research activities like fine-tuning models for other low-risk use cases would trigger a risk assessment. The explicit mention of specific types of sensitive data is also redundant given California’s existing strong protections of sensitive consumer data. We ask for clarification to ensure California’s approach aligns with risk-based proposals passed in Colorado focused on when ADMTs are put into actual use.

The prescriptive California-specific requirements in risk assessments also impose burdens on our state’s companies and will increase the cost of compliance. The laundry list of explicit requirements detailed in § 7152(a)(3)

will be difficult to compile and increase the risk of disclosing trade secrets through vague definitions such as explaining the logic of ADMTs. For example, this requires the approximate number of consumers whose personal information the business plans to process. If a business is planning a new product the number of consumers that will be using the product at that pre-launch phase will be impossible to calculate. It is also unclear exactly how these granular requirements will be used by the agency to improve consumer privacy when other jurisdictions and privacy laws require assessments tailored to the processing activity.

Additionally, Section 7151 unnecessarily specifies which employees should participate in the privacy risk assessment process. This could include many individuals who are not directly involved in the creation of products or have the necessary context to conduct an assessment. Every organization manages governance differently and the specificity in this draft rule may not be relevant to every business.

While clauses like § 7156(b) are premised on the importance of interoperability, requiring companies to submit every additional data requirement included by California undermines the benefit of using privacy assessments prepared in other jurisdictions. Requiring prescriptive, detailed disclosures, whether here or in sections like § 7157(b), will only increase compliance costs for companies and give consumers inconsistent experiences depending on their jurisdiction. We urge the Board to evaluate these lists of specific requirements to focus on functional data with clear utility for consumers and to harmonize these requirements with other jurisdictions to avoid creating an unhelpful box-checking exercise.

We request that the same information protection language used elsewhere throughout the proposed regulations be included in the Risk Assessment reporting requirements in § 7157 to create a consistent standard of information security across all interactions between companies and the agency.

We are also concerned about the difficulty in reconciling the various timing of risk assessment completions. The proposed rules require that risk assessments be completed by December 31, 2027 (§ 7155(b)), for any activity that a business initiated prior to the effective date and that continues following the effective date. But § 7155(a)(1) provides that any new processing activity will require a risk assessment prior to being initiated and

§ 7155(a)(3) provides that a risk assessment must be updated no later than 45 calendar days if there is a material change related to the processing activity. We recommend changes to make it clear that: (a) for all processing requiring a risk assessment that a company is engaged in prior to December 31, 2027, the risk assessment would be due on December 31, 2027; (b) for any new processing initiated after December 31, 2027 that requires a risk assessment, the risk assessment must be done prior to initiation; and (c) any material change after December 31, 2027 to processing requiring a risk assessment, such risk assessment must be updated within 45 calendar days.

### **Article 11 Sweeps Too Broadly and Would Burden Low-Risk Tools**

We also have concerns about the notices required for ADMTs. While we appreciate changes such as the inclusion of significant decision in § 7200(a), consolidation of the pre-use notice and notice of collection, the rules as currently written will still create unnecessary burdens for companies without clear privacy benefits to consumers.

For example, one concern is that § 7200(b) as written appears to require businesses to comply even if their tool was exclusively used before the effective date of these rules. If such use did not continue past January 1, 2027, a pre-use notice would not be necessary. Another narrow concern is ambiguity related to the requirement for pre-use notices in § 7220(a). As written, the rules would include companies using ADMTs for exempt purposes that do not grant consumers the right to access or opt out as defined in section 7221(b) and section 7222(a)(1). A pre-use notice should only be required when a business is required to offer an opt-out.

We appreciate the removal of the prohibition of justifying the use of decisions with terms like “to improve our services” in pre-use notices, as prohibiting that phrase is highly subjective and could preclude companies from using descriptions that are more easily understandable to consumers. However, the regulations still prohibit the use of this phrase in explaining risk assessments as well as in responding to consumers’ request to access ADMT. For consistency and to improve consumer communications, we ask the prohibition be removed throughout the regulations.

Another consideration would be to re-include the security and fraud prevention exception to the ADMT opt-out rights detailed in § 7221. Requiring opt-outs presents little privacy upside to consumers but will



weaken fraud-detection systems used to keep consumers safe and stop nefarious activity like account theft and payment fraud. This is also an opportunity to harmonize with the broader norm adopted in other privacy regulations exempting fraud prevention from opt-out rights.

There are also concerns about the amount of information required in the pre-use notices. While we appreciate the removal of requirements to explain the “logic” of an ADMT and an exemption for trade secrets, the new language in § 7220(c)(5) still mandates extensive disclosures such as the ADMTs output and how it is used to make decisions, which continue to go beyond the requirements of § 1798.185(a)(15) of the CCPA. Concerns about risks are better addressed through assessments or reviews rather than lengthy disclosures about the workings of an ADMT.

We are also concerned about maintaining the requirement for a single-user ADMT opt-out option. Given the broad definitions of ADMTs and their wide range of benefits for consumers, such a tool may cause consumers to unknowingly opt-out of a much broader set of tools than intended. This could be avoided by only requiring opt-outs narrowly targeted to specific use cases rather than a single general opt-out. We also disagree with the decision to remove former § 7221(b)(1), which provided that a business need not offer an opt-out from technology that’s used for security, fraud prevention, or safety purposes. That common-sense exception should be restored.

Regarding access requests outlined in § 7222, these requests should be limited to the specific adverse decision affecting the consumer making the request. Requiring access requests for all instances is out of step with other regulatory regimes like the Fair Credit Reporting Act, which only requires disclosures for adverse decisions. Also, the amount and type of information required in response to these access requests runs into similar over-disclosure issues listed earlier, particularly the requirement to explain details that go beyond the agency’s statutory mandate. The relevant part of the CCPA requires disclosure only of the overall “logic involved in the decisionmaking process” and the “outcome of the process,” not the specific “logic of the ADMT,” the output of the ADMT, “how the business used the output of the ADMT,” or potential future uses of the those outputs. At the very least, we encourage considering restricting disclosures to high-level information sufficient to facilitate a consumer’s understanding to make this requirement easier to operationalize.

**Changes to Existing Regulations**

In closing, we want to flag that changes that add new requirements to existing regulations don't provide a timeline by when businesses need to comply. Some of the changes include additional Privacy Policy disclosures, and changes from optional to mandatory disclosures. In addition, there is a new process businesses must develop in both "requests to know" and "requests to correct" with respect to certain pieces of sensitive data. This new process must allow consumers a way to confirm those pieces of information. This process will require time to safely build, particularly taking into account the security risks because social security numbers are included. Businesses need time to develop a thoughtful process that meets consumer needs but that also protects the information appropriately. We urge the agency to set January 1, 2027 as the compliance date for amendments to existing regulations.

We appreciate your consideration of these concerns we have raised. As privacy laws proliferate throughout the United States, it is even more critical to enhance the clarity and interoperability of laws and regulations that will allow companies to comply with differing requirements and allow California to maintain our status as a global leader in innovation.

Sincerely,

A solid black rectangular box used to redact the signature of Robert Boykin.

Robert Boykin

Executive Director for California and the Southwest

**Grenda, Rianna@CPPA**

---

**From:** Thomas Murphy [REDACTED]  
**Sent:** Saturday, May 10, 2025 5:25 AM  
**To:** Regulations@CPPA  
**Subject:** Watering down of privacy regs for Californians

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

I am a registered California voter, living in ZIP Code 90815 in Long Beach.

I'm writing to implore you to not mess with our privacy regulations by allowing AI and related technology to target Californians.

Tom Murphy  
Long Beach

Sent from my iPhone

**Grenda, Rianna@CPPA**

---

**From:** Viar, Kate <Kate.Viar@transunion.com>  
**Sent:** Monday, June 2, 2025 3:01 PM  
**To:** Regulations@CPPA  
**Subject:** Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations  
**Attachments:** CPPA ADMT comments TransUnion.pdf

**This Message Is From an External Sender**

WARNING: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Attached please find TransUnion's comments in response to the agency's proposed regulations addressing CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations. Thank you!

Best regards,

**Kate Viar**  
State Government Relations  
kate.viar@transunion.com  
**M:** [REDACTED]

**TransUnion**

*This email including, without limitation, the attachments, if any, accompanying this email, may contain information which is confidential or privileged and exempt from disclosure under applicable law. The information is for the use of the intended recipient. If you are not the intended recipient, be aware that any disclosure, copying, distribution, review or use of the contents of this email, and/or its attachments, is without authorization and is prohibited. If you have received this email in error, please notify us by reply email immediately and destroy all copies of this email and its attachments.*



June 2, 2025

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
400 R Street, Suite 350  
Sacramento, CA 95811

**RE: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations**

To whom it may concern:

Trans Union LLC (“TransUnion”) appreciates this opportunity to provide feedback regarding the California Privacy Protection Agency’s (CPPA) modified proposed regulations relating to the California Consumer Privacy Act (CCPA), specifically the sections addressing Automated Decisionmaking Technology (ADMT). We appreciate the CPPA’s responsiveness to prior public input and submit the following comments to assist in refining the regulations to ensure clarity, effectiveness, and feasibility of compliance.

**1. Definition of Automated Decisionmaking Technology**

TransUnion supports the revised definition of ADMT as “any technology that processes personal information and uses computation to replace human decisionmaking or substantially replace human decisionmaking.” We also appreciate the clarification that “substantially replace human decisionmaking” means a business uses the technology’s output to make a decision without human involvement. These changes promote regulatory focus on systems that warrant the most scrutiny, consistent with the risk-based principles reflected in the statute.

**2. Definition of Significant Decision**

TransUnion urges the CPPA to add a definition of “significant decision” to the regulations to clarify that it means a legal or similarly consequential decision that results in the provision or denial to a consumer.

**3. Integration of Existing CCPA Exemptions**

We respectfully request that the proposed regulations be amended to explicitly include the exemptions outlined in Civil Code §1798.145. The November 2024 draft referenced these exemptions with respect to business’ use of ADMT, yet those exemptions have been stricken from the May 2025 draft. Clear guidance is critical to ensuring regulatory consistency and

---

minimizing compliance disruptions for businesses that have structured their privacy programs around the existing statutory framework.

In addition, TransUnion urges the CPPA to clarify that the commercial credit reporting exemption under §1798.145 applies to ADMT-related opt-out rights.

#### 4. Pre-Use Requirements for ADMT

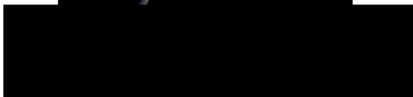
TransUnion appreciates that the revised draft eliminates several overly burdensome elements of the pre-use requirements, such as the need to disclose training use cases, specific personal information categories used in training, and the logic behind ADMT outputs.

While we would prefer the complete elimination of pre-use notice requirements, it is most critical that we can protect proprietary logic under the existing trade secret exemption.

TransUnion thanks the CPPA for its continued work to promote strong privacy protections while ensuring the regulations remain workable for businesses. We urge the CPPA to incorporate the clarifications and refinements discussed above to improve certainty, reduce regulatory friction, and ensure consistent application of statutory exemptions.

Please feel free to contact us with any questions or requests for further information.

Sincerely,

A black rectangular redaction box covering the signature of Kate Viar.

Kate Viar  
Senior Director, State Government Relations

## Grenda, Rianna@CPPA

---

**From:** Seth Smith <seth.smith@uber.com>  
**Sent:** Monday, June 2, 2025 12:26 PM  
**To:** Regulations@CPPA  
**Subject:** Uber Comments on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations  
**Attachments:** Final CPPA Comment Uber 6-2-25.pdf

### This Message Is From an External Sender

WARNING: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Hello CPPA Staff,

Please see attached public comments submitted by Uber Technologies Inc. on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations.

Please let me know if you have any questions and thank you for your time and consideration.

Kind regards,  
-Seth

--

**Seth Smith**  
Public Policy Manager | *California*



June 2, 2025

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
2101 Arena Blvd.  
Sacramento, CA 95834  
regulations@coppa.ca.gov

**Re: Uber Comments on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations**

Uber appreciates the opportunity to comment on the California Privacy Protection Agency's ("the Agency") amended proposed regulations<sup>1</sup> to implement the requirements of the California Consumer Privacy Act ("CCPA"). As a company that facilitates rideshare and delivery services for millions of Californians, we are committed to protecting consumer privacy while facilitating reliable transportation and delivery services to consumers and expanding economic opportunity across the state.

Uber supports the Agency's mission to strengthen the privacy protections of California's consumers consistent with its authority under California law. However, we are concerned that the current draft language of the regulation implicates a broad category of decisions—specifically those relating to independent contracting opportunities and compensation—that are operational in nature and do not present the kinds of privacy risks the CCPA is supposed to address. This language could unintentionally impact core rideshare and delivery features, like matching drivers with riders and couriers with merchants.

We encourage the Agency to remove "allocation or assignment of work" and "per-assignment compensation" from the definition of "significant decision."<sup>2</sup> The Agency should focus on high-risk decisions that materially affect individuals' privacy rights and avoid regulating day-to-day business processes that support the functionality, convenience, and efficiency of services Californians use every day.

Alternatively, if the Agency chooses to retain these categories, we recommend narrowing their scope to apply only within the traditional employer-employee context. Independent contractors, unlike employees, have the autonomy to decide whether to accept or reject specific tasks and earning opportunities. Automated tools that are used to simply offer work opportunities and associated compensation to these contractors for their independent consideration should not be classified as making significant decisions.

**a. The definition of "significant decision" goes beyond the Agency's core mission of protecting consumer privacy.**

---

<sup>1</sup> See California Privacy Protection Agency - Proposed Regulations (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations) (published May 1, 2025).

<sup>2</sup> Proposed regulations §7001(ddd)(4)(B).



The CCPA and CPRA were passed to enhance transparency and accountability in how businesses collect and use personal information. That goal is critical, and we applaud the Agency's efforts to ensure that California consumers' data is collected and used responsibly.

However, the proposed definition of "significant decision"—which includes decisions about "employment or independent contracting opportunities or compensation"—extends the rule's reach to business decisions that do not raise meaningful privacy concerns. In particular, the inclusion of "allocation or assignment of work" and "per-assignment compensation" expands the scope of the regulation well beyond privacy concerns and into the day-to-day operation of businesses.<sup>3</sup> As Board Member Alastair Mactaggart recently noted, this definition of significant decision could include instances where one courier is assigned a task simply because they are closer to a merchant than another courier.<sup>4</sup> These are functional, service-enabling decisions made at enormous scale, and they are central to the seamless consumer experience that Californians expect and rely on when using our services.

These types of decisions do not result in the use or disclosure of sensitive personal information in a way that threatens consumer privacy. Applying the same regulatory requirements to these everyday processes as would apply to high-risk decisions like access to credit or healthcare decisions risks expanding the Agency's scope into areas outside of its core privacy objectives, which could inadvertently divert attention from its efforts and dilute the impact the Agency can make. As Governor Gavin Newsom recently noted, it is important for the Agency to maintain its focus on its core mandate of privacy.<sup>5</sup>

**b. The Agency can strike a balance to protect privacy without threatening necessary services that Californians rely on.**

By striking "allocation or assignment of work" and "per-assignment compensation" from the definition of "significant decision," the Agency can strike a balance to protect consumer privacy while avoiding burdens on the tools that make these services work. The Agency recognized this option when it presented possible fixes to the regulation at the April Board meeting;<sup>6</sup> however, this beneficial amendment was not included in the staff's revised draft regulation. We urge the Agency to reconsider adopting this change.

Alternatively, if the Agency does not remove these categories, the Agency can improve the regulation by narrowing their scope to apply only within the traditional employer-employee context and not to independent contractors. Platforms that connect independent contractors with earning opportunities, such as rideshare and delivery offers, rely on automated tools to facilitate matching and pricing of these services on a per-trip basis. However, unlike employees, independent contractors can choose whether to accept or reject individual tasks that Uber and

---

<sup>3</sup> *Id.*

<sup>4</sup> See Comments of CPPA Board Member Alastair Mactaggart (April 4, 2025), at 1:56:55, <https://www.youtube.com/watch?v=qvRonzmjUgY>.

<sup>5</sup> See Letter from Gov. Gavin Newsom to the Agency (April 23, 2025).

<sup>6</sup> See Potential Modifications to Proposed Regulations Presentation (April 4, 2025), slide 8, [https://cppa.ca.gov/meetings/materials/20250404\\_item6\\_presentation.pdf](https://cppa.ca.gov/meetings/materials/20250404_item6_presentation.pdf).

other similar platforms may offer. Independent contractors can also work and receive offers from multiple companies at the same time. These are important distinctions from the traditional employer-employee relationship. Because independent contractors have the power to choose which offers to accept and from which platforms, the use of automated tools to facilitate matching and pricing of these offers does not carry the same implications as employer-directed decisions where an employee would have no such choice, and therefore should not be considered “significant decisions.”

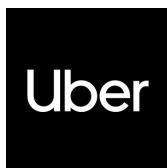
Uber strives to operate in a way that offers flexible economic opportunities while also delivering convenient, reliable, and affordable services to consumers. Matching a driver or courier to a customer request in real time is a central component of our platform—and one that depends on automated processes to function effectively at scale. Automated tools also allow us to set prices for individual trips, which independent contractors can choose for themselves whether to accept or reject. Imposing risk assessments, opt-out mechanisms, or appeals processes on these determinations—potentially hundreds of millions per year—could introduce delays and complexity that are incompatible with real-time service and potentially increase prices. It could also diminish service quality, and reduce flexibility for independent contractors. Low-risk, operational decisions about task offers or pricing fall outside the intended scope of this regulation and do not pose the same kinds of risks as decisions that are truly consequential to a consumer’s privacy.

A more tailored framework would allow the Agency to concentrate its oversight where it is most needed, while also preserving the functionality and consumer benefits of services that millions of Californians use every day.

## **Conclusion**

We appreciate the opportunity to provide input to the Agency’s ongoing work to craft rules that promote both privacy and innovation. We respectfully ask that the Agency refine the definition of “significant decision” to remove “allocation or assignment of work” and “per-assignment compensation.” We also urge the Agency to consider narrowing the rules to apply to traditional employees and not independent contractors. Narrowing the regulation in this way will allow the Agency to maintain its strong focus on privacy, avoid unintended interference with operational functionality, and preserve the ability of companies like Uber to deliver efficient and innovative services to the people of California.

Respectfully submitted,



Uber

## Grenda, Rianna@CPPA

---

**From:** Crenshaw, Jordan <JCrenshaw@USChamber.com>  
**Sent:** Monday, June 2, 2025 9:59 AM  
**To:** Regulations@CPPA  
**Cc:** Richards, Michael; Overstreet, Jack  
**Subject:** Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations  
**Attachments:** 250529\_Comments\_NPRM PrivacyRiskAssessmentsADMT\_CPPA.pdf

### This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

To Whom It May Concern:

Please find attached comments from the U.S. Chamber of Commerce in response to the request for public comment on updates to the CCPA cyber audit, privacy, risk, and ADMT rulemaking.

Thank you again.

Best,

**Jordan Crenshaw**

Senior Vice President  
Chamber Technology Engagement Center  
U.S. Chamber of Commerce  
Direct: 202-463-5632, Cell: [REDACTED]



U.S. Chamber of Commerce

[www.americaninnovators.com](http://www.americaninnovators.com)

@uschambertech



June 2, 2025

VIA ELECTRONIC SUBMISSION

California Privacy Protection Agency  
Attn: Legal Division – Regulations Public Comment  
2101 Arena Blvd.  
Sacramento, CA 95834

Re: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations

The U.S. Chamber of Commerce (“Chamber”) respectfully submits the following comments in response to the California Privacy Protection Agency’s (“Agency”) May 9 Notice of Modified Proposed Rulemaking (“Proposed Rules”).<sup>1</sup> The Chamber supports privacy protections for all Americans; many of the Proposed Rules<sup>2</sup>, however, exceed the Agency’s statutory authority, and its requirements, particularly those requiring privacy risk assessments and Automated Decision-making Technology (“ADMT”), will harm economic growth and innovation, and will be especially burdensome for small businesses. Our comments incorporate by reference the same policy, legal and economic arguments as incorporated by reference in our January 2025<sup>3</sup> comments (“January 2025 Comments”) to the Agency unless otherwise noted. Also given the short window for comments from publication, we urge the Agency to consider comments beyond the June 2 deadline for the record.

I. Introduction, Costs, and Burden on Interstate Commerce

The Chamber is the world’s largest business organization, representing businesses of all sizes across the country. The Chamber wishes to express concerns that the Proposed Rules on Cyber Audits, Risk Assessment, and ADMT impose an undue and impermissible burden on interstate commerce. Furthermore, the costs of the Proposed Rules outweigh the benefits.<sup>4</sup> According to the State of California’s own analysis, the Proposed Rules will impose a \$1.2 billion direct cost on businesses

---

<sup>1</sup> California Privacy Protection Agency—Notice of Modified Proposed Rulemaking (May 9, 2025) *available at* [https://cppa.ca.gov/regulations/pdf/ccpa\\_updates\\_cyber\\_risk\\_admt\\_notice.pdf](https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_notice.pdf).

<sup>2</sup> CALIFORNIA PRIVACY PROTECTION AGENCY – PROPOSED TEXT OF REGULATIONS (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations) (Nov. 2024) *available at* [https://cppa.ca.gov/regulations/pdf/ccpa\\_updates\\_cyber\\_risk\\_admt\\_ins\\_text.pdf](https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf).

<sup>3</sup> Comments of U.S. Chamber of Commerce to CCPA (January 14, 2025) *available at* [https://www.uschamber.com/assets/documents/Comments\\_CCPA\\_CaliforniaPrivacyProtectionAgency.pdf](https://www.uschamber.com/assets/documents/Comments_CCPA_CaliforniaPrivacyProtectionAgency.pdf).

<sup>4</sup> See e.g. *Minnesota v. Clover Leaf Creamery Co.*, 449 U.S. 456, 471 (1981).

subject to the CCPA.<sup>5</sup> In comparison, the Congressional Review Act defines a federal “major rule” as one that has “an annual effect on the [United States] economy of \$100,000,000 or more.”<sup>6</sup>

The Proposed Rules will have an outsized and significant impact on the national economy, particularly regarding AI. Between 2013 and 2023, private investment in AI has amounted to \$335.2 billion<sup>7</sup> with many of the leading AI developers operating in California. Although the Modified Proposal Rules strike direct references to the term “Artificial Intelligence,” it is very likely that AI systems will continue to be regulated under the definition of “automated decision-making systems” (“ADMT”) For this reason, we believe that the cost of implementing ADMT rules will be much higher than the \$143 million cited by the Agency.

## II. Definitions

### A. Automated Decision-making Technology and Significant Decision

The Chamber appreciates the Commission has decided to strike the term “Artificial Intelligence” from the Modified Proposed Rules. We share many of the concerns Governor Newsom highlighted about the lack of authority of the CCPA to make rules regarding AI.<sup>8</sup> However, we continue to have concerns about the definition of ADMT. The proposed definition is overly broad and not sufficiently tailored to focus on high-risk tools that operate without human oversight. We are further concerned with Section 7001(ddd)(4)(B) definition of “significant decision,”

First, we recommend discussions to ensure alignment between proposed state AI legislation and this rulemaking to avoid conflicting definitions of “consequential” and “significant” decisions, which create uncertainty and duplicative compliance burdens for regulated entities.

Additionally, the proposed definition of “significant decision” includes “allocation of assignment of work.” The allocation of assignment of work should not give rise to an AMDT opt-out as it is not a significant impact in that way that automated decisions related to hiring, promotions, or terminations may be. For this

---

<sup>5</sup> Potential Modifications to Proposed Regulations (May 1, 2025) *available at* [https://cppa.ca.gov/meetings/materials/20250501\\_item4\\_presentation.pdf](https://cppa.ca.gov/meetings/materials/20250501_item4_presentation.pdf).

<sup>6</sup> 5 U.S.C. § 804(2).

<sup>7</sup> Charted, U.S. is the private sector A.I. leader, *Axios* (July 9, 2024) *available at* <https://www.axios.com/2024/07/09/us-ai-global-leader-private-sector>.

<sup>8</sup> Letter from Governor Newsom to CCPA (April 23, 2025) *available at* <https://cdn.kqed.org/wp-content/uploads/sites/10/2025/04/CCPA-Letter.pdf>.

reason, we encourage CPPA to strike “allocation of assignment differing from automated decisions related to hiring, compensation, promotions, or terminations.

We further request clarification on the term “automated” within Section 7001(ee), as it is not defined. We request clarification of what is meant by “resources” under Section 7001(t) and recommend clarifying if the intent is to cover electronic systems. The proposed insertion of information systems of third parties not owned by the Business in Section 7001(t) should be excluded from the definition.

### III. Privacy Risk Assessments (Article 10)

#### A. When a Business Must Conduct a Risk Assessment

Although we continue to incorporate by reference the concerns in our January 2025 Comments related to when risk assessments should be conducted, there remain concerns about the statutory authority and impact of the newly inserted Section 7150(b)(4) and (5). We suggest striking this language entirely. The Act already regulates the use of data collected from geo-trackers that identify a consumer’s precise geolocation, regardless of the location. As sensitive data, a controller must still conduct a risk assessment (per these regs) and provide an opt out. The overbreadth would capture low risk activities such as providing discounts

### IV. Cybersecurity Audits (Article 9)

As noted in our January 2025 comments, we reiterate that the Agency should recognize that equivalent audits for other jurisdictions undertaken by businesses should be deemed in compliance with the CPPA. We generally continue to believe that audits should only be required every three years.

### V. Automated Decision-making Technology (Article 11)

#### A. Article 11 Generally

The Chamber remains concerned that the proposed rule would duplicate several existing regulatory efforts in California. We align with Governor Newsom's perspective, as articulated in his letter to the Agency dated April 23rd, emphasizing the necessity for the board to "fulfill its obligations to issue the regulations called for by Proposition 24 without venturing into areas beyond its mandate."<sup>9</sup> Additionally, we draw attention to a letter from State legislators to the board on February 19th, which asserts that "the ADMT regulations currently being considered need to be scaled back

---

<sup>9</sup> *Id.*

to focus on the specific issues identified under Civil Code Section 1798.185 and avoid general regulations on AI.<sup>10</sup>

The Chamber shares these concerns, noting that multiple simultaneous regulations throughout the State pose significant challenges for the business community, creating unnecessary confusion and potentially conflicting rules. Therefore, we believe that no further actions should be taken regarding Automated Decision-Making Technology until the agency has appropriately aligned with the Governors' and State Legislatures' letters to the agency. Should the agency move forward, provide the following feedback regarding ADMT.

## **B. Scope of ADMT Regulation**

We believe the scope of the ADMT regulation is problematic and potentially duplicative with other rules and regulations within the state. As stated above, we also believe the CPPA's regulations exceed the scope of the voter-approved statute.

## **C. Notification Requirements and Fraud**

The Chamber is concerned that the requirement within 7221(g), which mandates a business to inform a consumer why their request was deemed fraudulent, could provide a roadmap for bad actors to infiltrate their systems.

## **D. Pre-Use Notice Requirements**

The proposed rule requires businesses to explain detailed uses and purposes for ADMT, which is considered excessively burdensome. We further believe that CPPA does not have the statutory authority to regulate pre-use notices. We once again highlight our concerns with the prohibition of standard business terms such as "to improve our services" is overly restrictive. We are concerned that pre-use notice requirements could compel companies to disclose trade secrets and sensitive business information.

The current draft's removal of the opt-out exclusion in §7221(b) for a business' use of ADMT for fraud prevention and security-related purposes is problematic and contrary to business' ability to use appropriate technical measures to safeguard personal and confidential information by analyzing potential threats using ADMT and potentially identifiable personal information, such as IP addresses. Individuals opting out for this purpose may be more likely to be bad actors, whose activity would then be

---

<sup>10</sup> Bjerke, Brandon, et al. *Letter to the California Privacy Protection Agency Regarding ADMT Regulations*. 19 Feb. 2025. Privacy World, <https://www.privacyworld.blog/wp-content/uploads/sites/41/2025/03/LegRegLetter.pdf>.

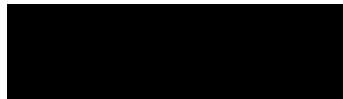
excluded from analysis. Accordingly, we recommend this exclusion be reinstated. Finally, we are concerned about the compliance timeline for the changes to the existing regulations and the risk assessments.

The changes to the existing regulations include some significant additional requirements, such as a process for consumers to confirm certain sensitive data elements. This will require technology solutions that will take time and resources to develop. We urge you to give businesses until January 1, 2027 to come into compliance with the amendments to the existing regulations. This will match the compliance date of the existing regulations.

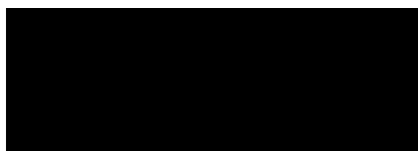
For the risk assessments, although the initial risk assessment is not due until December 31, 2027, there is ambiguity related to new processing and material changes to processing. Accordingly, we recommend the following changes: (a) for all processing requiring a risk assessment that a company is engaged in prior to December 31, 2027, the risk assessment would be due on December 31, 2027; (b) for any new processing initiated after December 31, 2027 that requires a risk assessment, the risk assessment must be done prior to initiation; and (c) any material change after December 31, 2027 to processing requiring a risk assessment, such risk assessment must be updated within 45 calendar days.

If you have any questions, please contact Jordan Crenshaw at [jcrenshaw@uschamber.com](mailto:jcrenshaw@uschamber.com). For questions concerning Article 9, please contact [croberti@uschamber.com](mailto:croberti@uschamber.com).

Sincerely,



Jordan Crenshaw  
Senior Vice President  
Chamber Technology Engagement Center  
U.S. Chamber of Commerce



Christopher D. Roberti  
Senior Vice President  
Cyber, Space, and National Security  
Policy Division  
U.S. Chamber of Commerce



## Grenda, Rianna@CPPA

---

**From:** Paul Eisler <peisler@ustelecom.org>  
**Sent:** Monday, June 2, 2025 7:23 AM  
**To:** Regulations@CPPA  
**Subject:** USTelecom - Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations  
**Attachments:** 2025.6.2 USTelecom CPPA Cyber Audit Comments.pdf

### This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

To whom it may concern,

Please find attached USTelecom's comments on the CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations proceeding.

Kind regards

Paul Eisler  
Vice President, Cybersecurity  
USTelecom – The Broadband Association  
601 New Jersey Avenue NW, Suite 600  
Washington, DC 20001  
M: [REDACTED]

USTELECOM | THE BROADBAND ASSOCIATION

**Before the  
CALIFORNIA PRIVACY PROTECTION AGENCY  
Sacramento, CA 95834**

In the Matter of )  
 )  
Proposed Regulations on CCPA Updates, )  
Cybersecurity Audits, Risk Assessments, )  
Automated Decisionmaking Technology (ADMT) )  
and Insurance Companies )  
 )

**COMMENTS OF USTELECOM – THE BROADBAND ASSOCIATION**

USTelecom – The Broadband Association (“USTelecom”)<sup>1</sup> respectfully submits these comments to the California Privacy Protection Agency (“Agency”) in response to the most recent modifications to the proposed regulations in the above-captioned proceeding. USTelecom strongly supports the Agency’s overarching commitment to enhancing cybersecurity. However, we remain deeply concerned that the proliferation of state-specific cybersecurity mandates may lead to a fragmented regulatory landscape—one that risks undermining a coherent, unified national cybersecurity strategy.

In the interest of promoting regulatory efficacy without compromising security objectives, USTelecom urges the Agency to adopt a risk-based framework rooted in widely accepted and operationalized industry standards. This approach would preserve the integrity of national cybersecurity efforts while ensuring that regulated entities remain accountable. To that

---

<sup>1</sup> USTelecom is the nation’s leading trade association representing service providers and suppliers for the telecom industry. USTelecom members provide a full array of services, including broadband, voice, data, and video over wireline and wireless networks. Its varied member base ranges from large international publicly traded communications corporations to local and regional companies and cooperatives, serving consumers and businesses in every corner of the country and world.

end, USTelecom has included targeted edits to the proposed rules, designed to advance these objectives in a manner consistent with the Agency’s statutory authority and policy goals.

**Risk-Based Cybersecurity Audits.** The Agency has a statutory mandate to “define the scope of the audit” and to establish “a process to ensure that audits are thorough and independent.”<sup>2</sup> In executing this mandate, the Agency should adopt a regulatory framework that enables a risk-based approach to cybersecurity audits, harmonized with widely recognized and empirically validated industry standards.<sup>3</sup> We respectfully urge the Agency to revise the proposed audit requirements to expressly recognize that adherence to risk-based audit methodologies grounded in established frameworks (such as the National Institute of Standards and Technology (“NIST”) Cybersecurity Framework or SOC 2 Type 2 certifications)<sup>4</sup> is compliant with the California standard. These frameworks represent the culmination of expert consensus and real-world application across industries and geographies and are relied upon by both public and private entities to safeguard sensitive data effectively.

---

<sup>2</sup> Cal. Civ. Code § 1798.185(14)(A).

<sup>3</sup> See, e.g., 23 NYCRR §§ 500.1; 500.9 (defining risk assessment as “the process of identifying, estimating and prioritizing cybersecurity risks to organizational operations (including mission, functions, image and reputation), organizational assets, individuals, customers, consumers, other organizations and critical infrastructure resulting from the operation of an information system. Risk assessments incorporate threat and vulnerability analyses and consider mitigations provided by security controls planned or in place”); see also U.S. Dept. of Health & Human Servs., *Guidance on Risk Analysis* (outlining questions as “examples” that organizations could consider that are “not prescriptive and merely identify issues an organization may wish to consider”), <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es>

<sup>4</sup> Other regulators, including the U.S. Department of Health and Human Services (“HHS”), have recognized that adherence to nationally recognized security standards is indicative of a strong security posture. See, e.g., Public Law 116–321 (requiring HHS to “consider certain recognized security practices of covered entities and business associates when making certain determinations” regarding fines, audit results, or other remedies for resolving potential HIPAA violations, including whether the organization established standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities).

Indeed, qualified cybersecurity auditors are trained in applying risk-based principles and NIST-aligned methodologies. The Agency can thus ensure the audits are “thorough and independent,” as required by statute, by allowing alignment with standards with which auditors possess demonstrable familiarity.

**Alignment with Statutory Language and California Law.** The statute’s grant of authority to the Agency does not necessitate the creation of California-specific audit content or standards that diverge from proven national or international benchmarks. Rather, the statute contemplates a flexible and scalable approach, permitting the Agency to define scope and process while allowing regulated entities to tailor their compliance efforts to their risk profile and operational complexity.

To fulfill the objectives of the statute and remain consistent with the California Administrative Procedure Act’s requirements for reasoned, evidence-based rulemaking, we recommend that the Agency recognize that adherence to such frameworks satisfies the statutory audit requirement, provided the audits are conducted by qualified professionals using risk-based assessments.

**Avoiding Undue Burden and Enhancing Substantive Compliance.** The process of preparing for and undergoing a full audit—particularly within large or complex organizations—entails significant internal coordination, governance approvals, and third-party engagements.

The imposition of rigid, prescriptive, and annual full-scope cybersecurity audits would impose significant burdens on regulated entities without a commensurate increase in data protection. Annual full audits are not standard practice in the cybersecurity community. Industry norms instead reflect a cadence of full audits every three years, with intervening annual

audits/assessments or certifications focused on verifying continued compliance and progress on remediation plans.<sup>5</sup>

This proposed cadence appropriately balances rigor with pragmatism. It enables entities to direct limited cybersecurity resources toward substantive threat mitigation and system hardening, rather than toward duplicative documentation exercises. Requiring annual full-scale audits and certifications would not only misallocate resources, but would also strain both private entities and the Agency, which would be inundated with voluminous and often redundant annual submissions.

### **Proposed Edits to the Cybersecurity Audits Regulation**

#### **§ 7123. Scope of Cybersecurity Audit and Audit Report.**

- b. The cybersecurity audit, at least once every three years, must ~~assess-specifically identify,~~ assess, and document:
- c. The business, in the intervening years of the three year cycle, must complete an intervening audit or assessment to account for materially updated or new conditions.

#### **[Reletter subsequent subsections in § 7123]**

#### **§ 7124. Certification of Completion.**

- a. Each calendar year that a business ~~that~~ is required to complete a cybersecurity audit pursuant to § 7123(b) of this Article, it must submit to the Agency ~~every calendar year~~ a written certification that the business completed the cybersecurity audit as required by ~~set forth in~~ this Article.
- b. The business must submit the certification no later than April 1 following any year that the business is required to complete a cybersecurity audit.
- c. The written certification must be completed by a member of the business's executive management team who:

---

<sup>5</sup> An intervening lighter-touch audit is consistent with the statutory requirement for businesses to “[p]erform a cybersecurity audit on an annual basis,” as the agency can determine the “scope of the audit” and require different degrees of audits for different purposes. Cal. Civ. Code § 1798.185(14)(A). This approach has similarities with other frameworks. See 23 NYCRR § 500.17(b) (requiring annual certifications that the Covered Entity is in compliance with the regulations).

1. ~~Is directly responsible for the business's cybersecurity audit compliance;~~
2. ~~Has sufficient knowledge of the business's cybersecurity audit to provide accurate information; and~~
3. ~~Has the authority to submit the business's certification to the Agency.~~

## CONCLUSION

USTelecom appreciates the opportunity to submit its views on the Agency's proposed regulation concerning cybersecurity audits, in furtherance of our mutual commitment to advancing national security objectives.

Respectfully submitted,

/s/ Paul Eisler

Paul Eisler

Vice President, Cybersecurity

**USTelecom – The Broadband Association**

601 New Jersey Avenue, NW

Suite 600

Washington, DC 20001

(202) 326-7300

June 2, 2025

**Grenda, Rianna@CPPA**

---

**From:** Cohen, Jessica <jessica.cohen@verizon.com>  
**Sent:** Friday, May 30, 2025 9:27 AM  
**To:** Regulations@CPPA  
**Cc:** Rudolph M (Rudy) Reyes Jr  
**Subject:** Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations  
**Attachments:** Verizon Comments - May CPPA Rulemaking.pdf

**This Message Is From an External Sender**

WARNING: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

To whom it may concern:

Please find attached comments on the Agency's current rulemaking on CCPA updates, cyber, risk, and ADMT from Verizon.

Thank you,  
Jessica Cohen

--



**Jessica Cohen**

Counsel, Regulatory Affairs  
Privacy & Cybersecurity

M [REDACTED]  
Cleveland, OH



*Please note: During the state legislative session, I may also be working outside of traditional office hours and providing responses in real time. Please do not feel obligated to respond outside of your typical working hours.*



**360 Spear Street  
Suite 300  
San Francisco, CA 94105**

**Rudolph M. Reyes  
Regional VP & Deputy General Counsel  
Public Policy & Law  
415.370.2557  
rudolph.reyes@verizon.com**

May 30, 2025

California Privacy Protection Agency  
Attn: Legal Division - Regulations Public Comment  
201 Arena Blvd.  
Sacramento, CA 95834

*via email:* [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov)

Re: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations

Dear California Privacy Protection Agency ("CPPA" or "Agency"):

Verizon appreciates the opportunity to submit this comment in connection with the proposed regulations issued by the Agency on May 9, 2025 for public comment.

The current version of the proposed regulations include a number of important and helpful changes from the version issued on November 2, 2024. The changes to the proposed requirements in connection with a corporate board role in cybersecurity audits and the revisions to the automated decisionmaking (ADMT) requirements, in particular, represent good policy and will be much improved for California businesses and consumers. We are encouraged by these revisions and are grateful that the Agency has recognized the need for these modifications.

As we have done in the past, Verizon is working with its trade associations to develop their comments on this most recent set of proposed regulations. There are a number of critically important issues that prompt us to provide the Agency with information about particular proposed requirements.

I. Cybersecurity Audits

The Agency has the statutory authority to determine the scope of an annual cybersecurity audit. Cybersecurity audits should be risk-based, consistent with industry standards and other cybersecurity frameworks. Such industry standards do not recommend extensive annual audits.



Rather, these standards recognize the importance of balancing the benefits of auditing with the burden of prescriptive compliance requirements that divert resources from protecting the enterprise and personal information.

To mitigate this outcome, businesses should have the flexibility to conduct a full cybersecurity audit every three years with annual audits or assessments only for materially changed or new conditions for the intervening years of the three-year cycle. In addition, certifications of compliance should be required only every three years in connection with the full cybersecurity audit. Our recommended redline edits in Appendix A are indicated by yellow highlighted text to avoid confusion with the redline text that is currently in the document.

## II. Timeline for Compliance

The proposed timelines for compliance for the amendments to the existing regulations and the risk assessment requirements do not provide sufficient time for the necessary work that must be undertaken to meet these new obligations.

### A. Amendments to Existing Regulations

The draft regulations do not provide a timeline for compliance with the additional requirements that will result from the amendments to the existing regulations. A number of these requirements will require time and resources to develop, including the following:

#### 1. Mandatory process with respect to the following data elements:

*Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics.*

In §§ 7023 and 7024, a new requirement for these elements mandates that businesses have a process for consumers to confirm that these data elements are correct. This requirement must be carefully developed because of the risk of fraud, particularly relating to Social Security numbers. Developing a secure process for legitimate, authenticated consumers to confirm these data elements and prevent such information from falling into the hands of fraudsters will take time and resources because of the cross-functional nature of this type of process, which will need to involve customer service, security, and data governance teams, as well as the need to develop and deploy secure technology solutions.

## 2. Privacy policy

The proposed amendments to §7011 (Privacy Policy) will require businesses to add additional detail to their privacy policy, which will require time and resources to develop. In particular, the new requirement in §7011(e)(1)(H) relating to disclosures of categories of personal information shared with a service provider or contractor for a business purpose, will require companies to develop processes to identify this information on a category basis and revise the privacy policy to accurately incorporate the new information.

We ask that businesses be provided until January 1, 2027, to come into compliance with the amendments to the existing regulations; that should give businesses adequate time to properly implement these changes. This compliance deadline will have the benefit of also matching up with the deadline set forth in §7200(b) for the ADMT requirements.

### B. Risk Assessments Timeline

In § 7155(b), the proposed regulations require that risk assessments be completed by December 31, 2027 for any activity that a business initiated prior to the effective date and that continues following the effective date. This provision contains an unknown effective date at this time—the draft indicates that it will be a date OAL designates.

However, § 7155(a)(1) provides that any new processing activity will require a risk assessment prior to being initiated and § 7155(a)(3) provides that a risk assessment must be updated no later than 45 calendar days if there is a material change related to the processing activity. It is unclear how subsections §7155(a)(1) and §7155(a)(3) can be reconciled with the provision in §7155(b) that requires risk assessments be completed by December 31, 2027, for any activity prior to the effective date and continuing thereafter. §7155(a)(1) could be interpreted as requiring a completed risk assessment (in the case of a new processing activity) before such time that the company's initial risk assessment is actually due. § 7155(a)(3) could be interpreted as requiring that an existing risk assessment be updated within 45 days of a material change – but such risk assessment is not actually due until December 31, 2027.

Accordingly, we recommend the changes set forth in Appendix B to align the requirements relating to new processing and material change processing with the initial due date of December 31, 2027. These changes would make the following clear: (a) for all processing requiring a risk assessment that a company is engaged in prior to December 31, 2027, the risk assessment would be due on December 31, 2027; (b) for any new processing initiated after December 31, 2027 that requires a risk assessment, the risk assessment must be done prior to initiation; and (c) any material change after December 31, 2027 to processing requiring a risk assessment, such risk assessment must be updated within 45 calendar days. Our recommended redline edits in Appendix B are indicated by yellow highlighted text to avoid confusion with the

redline text that is currently in the document.

Verizon appreciates the Agency's consideration of these comments, and looks forward to continuing to work with the Agency on these important issues.

Very truly yours,

A solid black rectangular box used to redact the signature of Rudolph M. Reyes.

Rudolph M. Reyes  
Regional Vice President and  
Deputy General Counsel

## Appendix A - Proposed edits to Article 9. Cybersecurity Audits

§ 7123. Scope of Cybersecurity Audit and Audit Report.

\* \*\*

- (b) The cybersecurity audit, at least once every three years, must ~~assess specifically identify, assess, and document:~~

\* \*\*

- (c) The business, in the intervening years of the three year cycle, must complete an intervening audit or assessment to account for materially updated or new conditions.

\* \*\*

### **[Reletter subsequent subsections in § 7123]**

§ 7124. Certification of Completion.

- (a) Each calendar year that a business ~~that~~ is required to complete a cybersecurity audit pursuant to § 7123(b) of this Article, it must submit to the Agency ~~every calendar year~~ a written certification that the business completed the cybersecurity audit as required by ~~set forth in~~ this Article.

~~(b) The business must submit the certification no later than April 1 following any year that the business is required to complete a cybersecurity audit.~~

~~(c) The written certification must be completed by a member of the business's executive management team who:~~

~~(1) Is directly responsible for the business's cybersecurity audit compliance;~~

~~(2) Has sufficient knowledge of the business's cybersecurity audit to provide accurate information; and~~

~~(3) Has the authority to submit the business's certification to the Agency.~~

## Appendix B - Proposed edits to Article 10. Risk Assessments

### **§ 7155. Timing and Retention Requirements for Risk Assessments.**

- (a) A business must comply with the following timing requirements for conducting and updating its risk assessments:
- (1) For initiating a processing activity following December 31, 2027, A-a business must conduct and document a risk assessment in accordance with the requirements of this Article before initiating any processing activity identified in section 7150, subsection (b).
  - (2) At least once every three years, a business must review, and update as necessary, its risk assessments to ensure that they remain accurate in accordance with the requirements of this Article.
  - (3) Notwithstanding subsection (a)(2) of this section, commencing on December 31, 2027, for any material change to a processing activity, a business must ~~immediately~~ update a risk assessment whenever there is a material change relating to the processing activity, as soon as feasibly possible, but no later than 45 calendar days from the date of the material change. A change relating to the processing activity is material if it ~~diminishes the benefits of the processing activity as set forth in section 7152, subsection (a)(4),~~ creates new negative impacts or increases the magnitude or likelihood of previously identified negative impacts as set forth in section 7152, subsection (a)(5), or diminishes the effectiveness of the safeguards as set forth in section 7152, subsection (a)(6).

Material changes may include, for example, changes to the purpose of the processing; the minimum personal information necessary to achieve the purpose of the processing; or the risks to consumers' privacy raised by consumers (e.g., numerous consumers complain to a business about the risks that the business's processing poses to their privacy).

- (b) ~~A business must retain its risk assessments, including original and updated versions, for as long as the processing continues or for five years after the completion of the risk assessment, whichever is later.~~

For any processing activity identified in section 7150, subsection (b), that the business initiated prior to December 31, 2027, [OAL to fill in the effective date of these regulations] and that continues after [OAL to fill in the effective date of these regulations], the business must conduct, and document as set forth in section 7152, a risk assessment in accordance with the requirements of this Article ~~within 24 months of the effective date of these regulations no later than~~ December 31, 2027. The business must comply with the submission requirements

set forth in section 7157, subsection (a)(1).

- (c) A business must retain its risk assessments, including original and updated versions, for as long as the processing continues or for five years after the completion of the risk assessment, whichever is later.

**Grenda, Rianna@CPPA**

---

**From:** Mikayla Jakubecy-Gibson <mikayla@vica.com>  
**Sent:** Monday, June 2, 2025 12:01 PM  
**To:** Regulations@CPPA  
**Cc:** Stuart Waldman  
**Subject:** Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations  
**Attachments:** Proposed Automated Decisionmaking Technology (ADMT) Regulations.pdf

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Dear California Privacy Protection Agency,

Attached is a written public comment from the Valley Industry & Commerce Association (VICA) opposing the proposed Automated Decisionmaking Technology (ADMT) regulations.

Thank you for your consideration.

Warmly,



Mikayla Gibson, MA  
Legislative Affairs Manager  
[Valley Industry & Commerce Association](#)  
C: [REDACTED]  
O: (818) 817-0545





June 2, 2025

California Privacy Protection Agency  
2101 Arena Blvd.  
Sacramento, CA 95834

**RE: Opposition to Proposed Automated Decisionmaking Technology (ADMT) Regulations**

To Whom it May Concern,

The Valley Industry and Commerce Association (VICA) opposes the California Privacy Protection Agency's proposed Automated Decisionmaking Technology (ADMT) and Risk Assessment regulations. While we appreciate the agency's efforts to incorporate public feedback, the revised draft remains overly expansive, misaligned with the agency's core consumer privacy mission, and imposes excessive burdens on businesses that far outweigh any potential consumer benefit.

The agency estimates that California businesses could face over \$1.2 billion in compliance costs in the first year alone—an unprecedented financial impact that would force employers to divert significant resources toward regulatory compliance, rather than job creation or innovation. The regulations would require companies of all sizes to undertake costly audits of internal systems, provide new opt-out rights to consumers and employees, and disclose proprietary business processes, even when the systems in question pose little to no privacy risk.

The definition of “automated decisionmaking” remains overly broad and would apply to routine business tools, including software that supports managerial decisionmaking such as employee performance reviews, safety compliance, or incentive calculations. These technologies have been in use for decades and function primarily as support systems, not autonomous decisionmakers. Regulating such systems as high-risk technologies misinterprets the intent of Proposition 24 and would result in unnecessary oversight of low-risk tools

We are especially concerned with the removal of the exemption for fraud prevention systems. These technologies are vital to maintaining security, safeguarding consumer data, and protecting businesses from malicious activity. Requiring opt-out provisions for fraud detection tools undermines their effectiveness and compromises public safety.

While we share the agency's goal of protecting consumer privacy, these proposed rules would capture an unreasonably wide range of business operations, threatening to stifle innovation and upend standard internal processes without delivering meaningful improvements in consumer protection. Rather than focusing on high-risk, emerging technologies such as emotion recognition or facial scanning, the agency's broad approach diverts attention and resources away from areas where regulation is truly needed.

VICA urges the California Privacy Protection Agency to reconsider and significantly revise the proposed ADMT regulations. A more targeted, risk-based approach is needed—one that focuses on genuine privacy harms without imposing undue burdens on California's employers or interfering with normal business operations.

Sincerely,



Stuart Waldman  
VICA President

**From:** William Calvin Witcher <[REDACTED]>  
**Sent:** Sunday, May 11, 2025 10:46 PM  
**To:** Regulations@CPPA; [REDACTED]  
**Subject:** Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations

**This Message Is From an Untrusted Sender**

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

**To the California Privacy Protection Agency Rulemaking Division:**

I appreciate the opportunity to submit public comment on the modified proposed regulations under the California Consumer Privacy Act (CCPA), particularly those concerning cybersecurity audits, risk assessments, automated decision-making technology (ADMT), and consent mechanisms.

I am a Doctoral Candidate in Cybersecurity and Information Assurance at Capella University, where my dissertation research focuses on non-compliance with the CCPA among Small and Medium-Sized Enterprises (SMEs) in Southern California. I also serve as Vice President of Information Technology at Inglewood Park Cemetery, overseeing enterprise cybersecurity, compliance operations, and data governance strategy. This dual lens gives me a unique vantage point on how the proposed updates impact academic understanding and real-world implementation across sectors.

**1. Scalability of Cybersecurity Audits for SMEs**

The requirement for businesses that process sensitive or large-scale consumer data to conduct annual cybersecurity audits and prepare formal Cybersecurity Audit Reports (§7120–7123) raises critical questions of feasibility and proportionality for SMEs. While well-intentioned, the current language does not sufficiently distinguish between enterprise-level capabilities and those of small businesses operating with lean IT staffing and budgets.

**Example 1:** A 20-person law firm handling probate cases may store Social Security numbers, death certificates, and estate documentation. Despite the sensitivity of this data, the firm lacks in-house cybersecurity personnel and outsources its IT to a local managed services provider. Mandating a board-reviewed, NIST-aligned cybersecurity audit could cost upwards of \$25,000 annually, making it financially unsustainable for many such firms.

**Example 2:** A regional e-commerce SME selling custom apparel collects address, payment, and behavioral data but uses third-party platforms for fulfillment, marketing, and payments. The business owner may be unaware they're still considered a “business” under the CCPA. The layered tech stack and

lack of visibility into third-party controls make audit preparation extremely complex, despite limited direct data processing.

**My Recommendation:** I urge the CPPA to adopt a tiered audit framework similar to Colorado’s Privacy Act Rule 6.09, where applicability thresholds are based on data risk level and business size or revenue. This would maintain accountability without imposing disproportionate burdens.

## 2. Clarification of ADMT Applicability in Common Business Workflows

The expanded definition of Automated Decisionmaking Technology (ADMT) under §7001(e) and the associated consumer rights (§7220–7222) present a timely and necessary regulation of algorithmic decision systems. However, the line between advanced analytics and regulated ADMT remains unclear, especially for SMEs using off-the-shelf software or "low-code/no-code" automation tools.

**Example 1:** A hiring manager using LinkedIn Talent Insights or an ATS that screens resumes based on keyword scoring may unknowingly be engaging in profiling under ADMT, especially if these scores are used in a “significant decision” such as hiring. Yet, few businesses understand this distinction or have workflows to support opt-out mechanisms.

**Example 2:** A B2C company using Salesforce Marketing Cloud to segment customers and automate personalized discounts based on purchase behavior is likely engaging in profiling. While human review may occur, the automated score or segment label often dictates outcomes. This could trigger ADMT provisions, yet many small marketers lack documentation or consumer-facing disclosures.

**My Recommendation:** CPPA should provide industry-specific ADMT compliance playbooks, with concrete examples and decision trees that help SMEs assess whether their tools, configurations, or vendors fall under this regulation. Pre-use Notices and opt-out rights should also account for third-party platform use where configuration may not be fully under the business’s control.

## 3. Designing Consent Interfaces Without Dark Patterns

The CPPA’s stance against **dark patterns** in user interfaces is a crucial step toward meaningful consumer choice. However, the guidelines in §7004 could be further operationalized for non-enterprise digital environments. Many SMEs use third-party CMS systems, mobile templates, or e-commerce builders (like Wix, Shopify, or Squarespace), which may limit their ability to control consent flows fully.

**Example 1:** A nonprofit using a website plug-in that defaults to “Accept All” cookies with no equivalent “Decline All” button technically violates the symmetry principle. However, the tool’s customization limitations and cost barriers prevent the nonprofit from complying without hiring external developers.

**Example 2:** A mobile app developer uses a consent pop-up with an "X" to close and an "Agree" button but no clear opt-out path. Though unintentionally deceptive, this design fails the “freely given, informed, and unambiguous” consent standard. The developer relies on mobile frameworks with limited flexibility.

**My Recommendation:** CPPA should consider issuing UI/UX implementation templates for consent, ideally tailored for popular platforms and mobile contexts. This would empower SMEs to meet legal expectations without incurring costly redevelopment. A “compliance kit” with open-source designs could significantly reduce violations due to lack of technical access or awareness.

#### 4. Enabling Compliance Through Practical Support Tools

One of the most effective ways to increase compliance is not more regulation, but better enablement infrastructure. The CCPA regulations are deeply legalistic, and many SMEs cannot afford to hire privacy counsel or in-house compliance leads. Without accessible self-service tools, even well-meaning businesses will fall short.

**Example 1:** A small funeral home in California using paper-based contracts, legacy accounting software, and local file servers may process highly sensitive data (death records, SSNs, next-of-kin). They likely lack awareness that they’re subject to CCPA at all, much less how to classify sensitive data or respond to a data subject request.

**Example 2:** A new Black-owned skincare brand collecting health-related data for product matching is unknowingly gathering sensitive personal information under §7001(bbb). Without visibility into the obligations or access to step-by-step instructions, the business risks noncompliance through no fault of its own.

**My Recommendation:** CPPA should develop and publish a self-paced online toolkit that includes:

- Compliance checklists for SMEs by industry
- Risk assessment templates
- Pre-use notice and privacy policy generators
- FAQs in multiple languages

This kind of public resource model, used effectively by agencies such as the UK ICO and the Colorado Department of Law, can dramatically reduce barriers to compliance for non-enterprise stakeholders.

#### Conclusion

I commend the California Privacy Protection Agency for advancing privacy protections that reflect today’s data ecosystem. However, without intentional flexibility, operational clarity, and scalable implementation support, these regulations risk leaving many SMEs behind—businesses foundational to California’s economy and community fabric.

Also, I thank you again for your leadership and for considering this perspective. I would be honored to contribute further to outreach, SME pilot projects, or future policy forums focused on equitable compliance.

Respectfully,

**William Calvin Witcher**

Doctoral Candidate – Cybersecurity and Information Assurance

Capella University (Doctoral Research Focus: CCPA Non-Compliance in Southern California SMEs)

Vice President, Information Technology

Inglewood Park Cemetery



## Grenda, Rianna@CPPA

---

**From:** Barbara Cosgrove <barbara.cosgrove@workday.com>  
**Sent:** Monday, June 2, 2025 3:45 PM  
**To:** Regulations@CPPA  
**Cc:** Chandler C. Morse; Jarrell Cook; Lev Sugarman  
**Subject:** Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations  
**Attachments:** Workday\_Comments on Revised CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations.pdf

### This Message Is From an External Sender

WARNING: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

[Report Suspicious](#)

Attached please find Workday's comments on the revised proposed CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations.

Thank you for the opportunity and please feel free to reach out at any time.

Best regards,  
Barbara





# Workday Comments on Revised Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies

June 2, 2025

Workday appreciates the opportunity to comment on the California Privacy Protection Agency's (CPPA) revised proposed rulemaking regarding cybersecurity audits, risk assessments, and automated decisionmaking technology (ADMT). [Workday](#) is a leading enterprise platform that helps organizations manage their most important assets – their people and money. The Workday platform is built with AI at the core to help customers elevate people, supercharge work, and move their business forever forward. Workday is used by more than 10,500 organizations around the world and across industries – from medium-sized businesses to more than 60% of the Fortune 500.

Workday is committed to the responsible development and deployment of AI and ADMT, and to robust cybersecurity and privacy protections. We previously submitted comments on the proposed rulemaking in [February 2025](#), under the CPRA in [November 2021](#), the CPPA's provisions on service providers in [August 2022](#), and the initial proposed rulemaking for cybersecurity audits, risk assessments, and automated decision-making draft regulations in [March 2023](#). While we commend the CPPA for incorporating positive revisions in the latest draft, there are further revisions we believe are necessary to ensure the regulations are workable and effective in practice.

We welcome the opportunity to discuss these comments further with the CPPA. Please do not hesitate to contact Barbara Cosgrove, Chief Privacy and Digital Trust Officer at [barbara.cosgrove@workday.com](mailto:barbara.cosgrove@workday.com) if you have any questions or would like further information.

## Cybersecurity Audits

Workday recognizes the critical importance of robust cybersecurity practices. We suggest retaining key improvements in the proposed regulations, including:

- **Removing Board Reporting Mandate.** We appreciate and strongly support the removal of the requirement on audit reporting and oversight by the "senior-most executive in the business who is responsible for oversight of cybersecurity governance" or the "executive management team," rather than direct board reporting. This aligns with our February comments and allows for more effective operational oversight.
- **Recognizing Third Party Audits, including NIST CSF, May Be Used to Meet Cybersecurity Audit.** We appreciate the revised regulations state that a business may use an existing audit or assessment prepared for another purpose if it meets the regulation's requirements. However, as further mentioned below, we do not believe this revision goes far enough to reflect industry standard security practices and will create unnecessary cost and confusion for both businesses

and broader value chains.

- **Distinguishing between Cybersecurity Audits and Reports.** It's common for companies to share a report covering the scope of a cybersecurity audit and any material deficiencies with their executive management, and potentially customers. The new definition for Cybersecurity Audit Report and requirement that only the Report be provided to executive management, better aligns with how companies function and enables a more transparent audit process.

### ***Recommendations for Further Improvement***

In addition to these improvements, we recommend that the CPPA:

- **Explicitly Recognize Existing Standards as Meeting the Cybersecurity Compliance Requirements.** We strongly reiterate our recommendation that the CPPA explicitly state that organizations (businesses and service providers) can satisfy CCPA cybersecurity audit requirements by conducting audits or obtaining certifications under established, globally respected industry standards such as ISO 27001, SOC 2, as well as by demonstrating alignment with the NIST CSF. This approach would leverage existing, rigorous frameworks, promote strong security, and avoid imposing duplicative mandates. Without this change, companies will be required to invest in and conduct unique audits for California without any marginal benefit for consumers or cybersecurity outcomes. It's standard practice for businesses to require vendors to demonstrate that they have appropriate data protection practices in place by providing proof of independent certifications to the applicable ISO 27000 standard, or independent audits under the American Institute of Certified Public Accountant's System and Organizations Controls Framework.
  - Should the CPPA maintain California-specific audit requirements for businesses not audited under other recognized global standards, these should be designed to be risk-based, and harmonized with existing leading frameworks.
  - We reiterate our prior recommendation that the CPPA publish mappings between any California-specific requirements and widely adopted standards like NIST CSF, ISO 27001, and SOC 2 to aid compliance and help companies demonstrate alignment.
- **Clarify Audit Scope Pertaining to Business vs. Service Provider Data.** The regulations should clearly stipulate that cybersecurity audit obligations and their associated thresholds apply only to personal information that a company processes in its capacity as a "business," excluding data processed solely in its role as a "service provider" for its customers. The cybersecurity audit provisions as written do not differentiate between these roles when assessing data processing thresholds, which will lead to confusion as some companies act as a business in some situations for processing personal data and a service provider for other products and services. Specifically we recommend modifying sections 7120(b) and 7123(a) to include language clarifying that the thresholds apply to personal information a company processes in its role as a business.
- **Maintain Clear and Manageable Audit Scope.** We continue to advocate for clearly defined audit scopes, agreed upon via a pre-established audit plan, and caution against open-ended provisions that create ambiguity and management difficulties. The CPPA should further amend the language to explicitly allow service providers to share standardized evidence of industry standard audits and certifications about their products and services.

## Risk Assessments

Workday supports the use of impact and risk assessments as valuable internal tools for identifying and mitigating technology risks. Widely-used in the privacy and data protection context, risk assessments are familiar to companies and are a pragmatic tool to effectively manage AI-related risks. We appreciate several key revisions that refine the scope and requirements for risk assessments:

- **Narrowing of ADMT & AI Training Risk Assessment Triggers.** Consistent with our February comments, we appreciate the narrowing of ADMT and AI training as broad triggers for risk assessments. As noted previously, the training process itself does not pose the same direct consumer risks associated with the processing of personal information for decision-making.
- **Risk Assessment Submissions.** We appreciate the revisions to the scope of materials that businesses must proactively provide to the CPPA. Providing abridged risk assessments created serious confidentiality challenges and would have resulted in an unmanageably large amount of information for the CPPA to process and retain.

### *Recommendations for Further Improvement*

- **Explicitly Acknowledge Employment-Related Exemptions for Risk Assessments.** The exemption around processing sensitive personal information in employment-related contexts is likely to create confusion due to the current approach of listing specific examples, which are too narrow and may lead to inconsistent interpretations among companies. To avoid this confusion, we recommend amending Section 7150(b)(2)(A) by adding the phrase "specifically for employment-related purposes, including" before the existing list of exemptions. This modification would clarify that the listed examples, such as administering compensation payments, are illustrative and not exhaustive limitations, thereby allowing for a more nuanced and practical application of the risk assessment requirements.
- **Service Provider Obligations to Support Risk Assessments.** Similar to cybersecurity audit obligations, businesses and service providers need to have their roles clearly defined. The CPPA should further amend the language in §7050(h)(2) and §7153(a) to prevent unintended burdens on service providers. To efficiently support their numerous business customers with risk assessments, regulations should explicitly allow service providers to share standardized, replicable information about their products and services. This approach ensures customers get the necessary details without overwhelming providers with individualized requests, fostering a more streamlined and effective compliance process for everyone.

## Automated Decisionmaking Technology (ADMT)

Several revisions in the draft regulations provide greater clarity in their application and improve their workability for businesses and their service providers. We urge the CPPA to retain these changes, which include:

## Definitions & Scoping

- **Narrowed Definition of ADMT.** We support the revisions to focus the ADMT definition on specific applications of ADMT that replace or substantially replace human decision-making. We also appreciate the addition of "without human involvement" in the definition of "substantially replace human decisionmaking," which aligns with the approach taken by other states and the federal government in establishing similar thresholds, such as the concept of "principal basis." On balance, these changes help ensure that the proposed regulations squarely consider the extent to which ADMT outputs influence human-decision-making, which is a critical element in any effective risk-based approach. As a result, the scope of the ADMT regulations is more appropriately focused on those applications of ADMT that generally operate without a human in the loop and therefore pose potentially greater risks. This revised scope also better aligns California's privacy framework with other state privacy laws, which generally only govern fully or substantially automated decisionmaking technologies.
- **Removal of "Artificial Intelligence" Definition.** We appreciate the removal of "artificial intelligence" from the scope of the ADMT regulations. The inclusion of "artificial intelligence" in earlier proposals created confusion and substantially broadened the scope to an impractically large array of systems. This change also more closely aligns the proposed regulations with the rulemaking authority granted by the CCPA.
- **Refined "Significant Decision" Definition.** We support the revised definition of "significant decision" which is limited to the "provision or denial" of important benefits and services, while removing the broader "access to" language. This revision is in line with Workday's February comments and ensures that the regulations target decisions with direct and material impact on consumers, which is an important element of an effective and nuanced risk-based approach. This change would also align California's regulations with every other state privacy law that governs similar decisions, all of which are limited to "provision or denial" only.
- **Scoping Notice and Access Rights to Significant Decisions.** Requiring pre-use notice and access requirements only for ADMT used to make significant decisions is a positive step. This ensures that these obligations apply where potential impacts to consumers are most direct and avoids over-application to less impactful uses of ADMT where the risks are relatively lower.

## Notice

- **Consolidated Notice.** Allowing the pre-use notice to be provided in the larger Notice at Collection under certain circumstances is a practical and efficient approach. This consolidation reduces duplicative notice requirements and streamlines the regulations without diminishing transparency for consumers.

## Opt Out

- **Problematic Exemption Conditions Removed.** In line with Workday's February comments, we strongly support the removal of language that would have allowed a business to claim the opt-out exemption by relying on the ADMT developer's evaluation. This mechanism was unworkable given the distinct roles that entities hold in the AI value chain: while a developer can evaluate an ADMT

for risks “in the lab,” it has no visibility into, or control over, the ADMT once deployed “in the field.” Additionally, it is the business, rather the developer, that uses the ADMT to make a significant decision and interacts directly with consumers. Because assessing for risks of unlawful discrimination is a context-dependent and fact-intensive exercise, only the business deploying the ADMT and making significant decisions is positioned to make this evaluation. By contrast, the revised opt out exemption is more workable as it relies solely on information in the custody of the business, which is best-placed to assess those factors.

## **Access**

- **Removal of Duplicative Requirements for Adverse Significant Decisions:** We support the removal of specific notice requirements for "adverse significant decisions" within the Access section. These requirements previously created a parallel and duplicative notice regime within the Access requirements, leading to unnecessary complexity.

## **Recommendations for Further Improvement**

In addition to retaining the revisions above, Workday offers the following recommendations to further improve the clarity and workability of the proposed regulations.

- **Definitions - Employment or Independent Contracting Opportunities or Compensation:** The definition of “significant decision” contains a subcategory of employment-related decisions, including “Allocation or assignment of work for employees.” We are concerned that this language sweeps broadly, and could capture a substantial amount of mundane employment activities that do not pose risks to consumers. For example, “allocation or assignment of work for employees” could include rote tools that enable automatic email response delegation or customer service call routing.

We recommend aligning this language with the equivalent provision in the EU AI Act, which classifies as high-risk those AI systems that are intended to be used “to allocate tasks based on individual behaviour or personal traits or characteristics.” This approach is more appropriately targeted to the subset of allocation/assignment use cases that could pose risks to consumers, while retaining the apparent policy objective in the proposed regulations.

- **Access – Information about the Logic of the ADMT:** While we agree that businesses should provide key information about the ADMT to consumers, the proposed regulations would require businesses to provide information "which may include the parameters that generated the output as well as the specific output with respect to the consumer." Neither of these highly technical attributes are likely to be useful or actionable for consumers.

Parameters vary across models and can be highly technical in nature, making them difficult for a typical consumer to parse or interpret meaningfully. Providing such detail out of context may lead to confusion rather than clarity. Similarly, providing specific outputs may not provide useful information. For example, sharing match scores or raw outputs does not necessarily provide useful information to the consumer regarding the decision and lacks key context. We recommend reconsidering the inclusion of the parameters that generated the output and the specific output with respect to the consumer.

- **Opt Out – Notification to Service Providers:** The requirement for businesses to notify service providers "that the consumer has made a request to opt-out of that ADMT and instructing them to comply with the consumer's request to opt-out of that ADMT within the same time frame" is unclear and potentially unworkable.

It is unclear what "comply with the consumer's request to opt-out" means in practice for service providers, who, by virtue of their role, do not make significant decisions about consumers. Rather, their enterprise customers—i.e., businesses—make these decisions. Service providers typically process data on behalf of their customers and do not have the direct relationship with the consumer that would enable them to "comply" with an opt-out request related to a significant decision

This challenge aside, service providers generally maintain very restricted visibility into customer data in line with regulatory requirements, contractual obligations, and long-standing privacy and security best practices. As a result, service providers are not technically capable of effectively implementing an opt-out that requires granular and potentially intrusive access into customer data. We recommend removing or clarifying this requirement to ensure it is workable in light of service providers' role in the ADMT value chain.

- **Harmonization with Concurrent Legislative & Regulatory Initiatives:** Consistent with our previous comments throughout the rulemaking process, we are concerned that the proposed regulations will overlap and even conflict with the AI laws enacted by California in 2024, the California Civil Rights Council's recently-adopted regulations on automated decision systems used in employment, and the dozens of AI bills under consideration by the California Legislature this year. We urge the CPPA to prioritize harmonization with these concurrent legislative and regulatory initiatives to ensure consistency and avoid a fragmented regulatory landscape that could meaningfully impact innovation without commensurate benefit for consumers.

Workday looks forward to continuing to work with the CPPA as it develops these important rules under the CPRA.