

Grenda, Rianna@CPPA

From: Kate Goodloe <KateG@bsa.org>
Sent: Monday, June 2, 2025 10:56 AM
To: Regulations@CPPA
Cc: Meghan Pensyl; Heather Curry
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance
Attachments: 2025.6.2 - BSA Comments to CPPA - Final.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 –

I am attaching comments from the Business Software Alliance (BSA) on the CPPA's proposed updates to the Cybersecurity, Risk Assessment, and ADMT regulations.

We appreciate the opportunity to provide these comments and would welcome a chance to further discuss these issues.

Best,

Kate



Kate Goodloe
Managing Director, Policy
Business Software Alliance

bsa.org

Sign up for [BSA News](#) | [LinkedIn](#)



June 2, 2025

Business Software Alliance Comments on Revised Proposed Regulations

The Business Software Alliance (BSA) appreciates the opportunity to comment on continued rulemaking by the California Privacy Protection Agency (CPPA). The agency's draft rules address critical topics, including automated decisionmaking technologies (ADMT), cybersecurity audits, and risk assessments. We appreciate many changes in the latest draft regulations but continue to believe further revisions are needed to create strong and workable privacy protections.

BSA is the leading advocate for the global software industry before governments and in the international marketplace.¹ Our members create the business-to-business technology products and services that power other companies. They offer tools including cloud storage services, customer relationship management software, cybersecurity solutions, human resources management programs, identity management services, and collaboration software. Businesses entrust some of their most sensitive information — including personal information — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security are fundamental parts of BSA members' operations.

We appreciate recent changes to the proposed regulations but strongly encourage you to further revise all three sets of rules:

1. **Automated Decisionmaking.** The recent revisions better focus the proposed ADMT regulations on ADMT technologies, rather than broader AI tools. However, the proposed regulations should be further revised to: (1) address practical concerns with treating allocation of work as a significant decision; (2) address issues with implementing pre-use notices, opt-outs, and access requests; and (3) harmonize them with other legislative and regulatory efforts.
2. **Cybersecurity Audits.** Strong cybersecurity practices can help protect personal information but poorly targeted requirements will unduly burden companies without commensurate security benefits. We urge the CPPA to revise the proposed regulations on cybersecurity audits to: (1) expressly state that companies satisfy the CCPA's audit requirements if they conduct audits, certifications or evaluations under leading standards like ISO 27001 or SOC 2; (2) ensure any California-specific audit requirements are flexible, risk-based, and harmonized; and (3) limit audit requirements to personal information processed in a company's role as a business, not its role as a service provider.
3. **Risk Assessments.** Although BSA supports the use of risk assessments to identify and mitigate potential privacy risks, California will be an outlier in requiring businesses to proactively provide risk assessment information to the CPPA. We are concerned with this approach and strongly recommend: (1) promoting the use of global risk assessments, rather than California-specific requirements (2) removing requirements to provide information under penalty of perjury, (3) narrowing the set of information to be proactively provided to the CPPA, and (4) treating information provided to the CPPA as confidential.

¹ BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cohere, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Workday, Zendesk, and Zoom Communications Inc.

I. Automated Decisionmaking

BSA supports protecting consumers from high-risk uses of AI. For example, for several years we have called for legislation to ensure companies that develop and deploy AI for high-risk uses conduct impact assessments and adopt risk management programs.

We appreciate several revisions to the most recent proposed ADMT regulations and urge you to retain those changes. These include:

- Narrowing the definition of ADMT. We appreciate the new definition of ADMT as technology that either replaces or substantially replaces human decision-making. (Section 7001.) Narrowing this definition creates a more workable threshold for companies to implement the obligations created by the ADMT regulations, leading to greater certainty for both companies and consumers about which technologies are subject to heightened protections.
- Deleting the definition of Artificial Intelligence. The proposed regulations remove references to AI and instead focus on ADMT. We appreciate this approach, which decreases the potential for the ADMT rules to apply to broader AI systems in ways that are confusing and impractical. (Section 7001.)
- Narrowing the definition of significant decision. The proposed regulations narrow the types of decisions treated as “significant.” We appreciate that the revised term focuses on decisions that result in the “provision or denial” of important benefits and services, rather than “access to” such services, which can inadvertently capture a wide range of non-significant actions. However, the list of significant decisions described in Section 7001(ddd)(1)-(6) should be further narrowed, as described below.
- Tailoring pre-use notices and consumer access requests to ADMTs used for significant decisions and protecting trade secrets. The proposed regulations narrow the requirements for pre-use notices and consumer access requests to ADMTs used for significant decisions, rather than broader uses of ADMTs. This change helps ensure that pre-use notices and consumer access requests apply to the uses of ADMT that have the most significant impact on consumers’ daily lives. We strongly recommend keeping that focus and refining the obligations for pre-use notices and consumer access requests as described below. Additionally, the proposed regulations add new language to clarify that businesses providing pre-use notices or responding to access requests are not required to disclose trade secrets or information that may compromise their ability to protect against security threats and illegal activity. We strongly recommend keeping these provisions and strengthening them as described below. (Section 7220(d), Section 7222(c).)
- Focusing risk assessments on a more specific set of AI-related activities. The prior draft regulations would have required risk assessments for an extremely broad set of activities involving training either ADMT or AI. We strongly encourage you to retain the more focused approach in Section 7150(b)(6), which only requires risk assessments for companies training ADMT for significant decisions or specific sensitive activities.

We also urge you to make further changes to better focus the proposed ADMT regulations. Specifically, we encourage you to make three sets of changes:

First: Address practical concerns with treating allocation of work as a significant decision. The definition of significant decision includes employment or independent contracting opportunities or compensation — and identifies three types of opportunities, including allocation of assignment of work for employees. We are concerned that this part of the definition sweeps more broadly than intended. For example, an AI tool used to assign incoming calls at a call center should not be subject to the same requirements as a tool that accepts or rejects an applicant from the hiring process.

Recommendation:

- Section 7001(ddd) should be revised to clarify that significant decisions are those with material, legal, or similarly significant effects on a consumer. This would ensure that the protections focus on material risks to a consumer, without inadvertently sweeping in activities like work allocation, discussed above.
- The definition should add a provision stating: “An action is not a ‘significant decision’ if it does not have a material, legal, or similarly significant effect on a consumer.”
- The definition of employment or independent contracting opportunities or compensation should be revised to strike allocation or assignment of work for employees.

Second: practical implementation challenges for pre-use notices, opt-outs, and access requests should be addressed.

The proposed regulations require businesses to comply with sweeping obligations before using ADMT for significant decisions. While we appreciate that requirements for pre-use notices, opt-outs of ADMT, and requests to access ADMT have been limited to ADMTs used for significant decisions, rather than applying to other uses of ADMT, these requirements present five concerns:

First, requirements for businesses to provide consumers with pre-use notices will likely result in over-notification to consumers. Pre-use notices to consumers must include at least seven specific explanations. That will result in lengthy notifications that consumers may be unlikely to read, undermining the protections created in the proposed regulations. We strongly recommend narrowing the information required in pre-use notices, so that notices are effective in alerting consumers about processing that may create concerns, not routine and expected processing.

Second, information to be provided for access requests creates practical concerns. The proposed regulations require businesses to disclose to consumers information in response to access requests, including information about the logic used in the ADMT and how the business used the output of the ADMT to make a significant decision about the consumer, the business’s plans to use the outputs of the ADMT to make an additional significant decision concerning the consumer in the future, and the extent of human involvement in future significant decisions. Such sensitive details may include competitive or other confidential information. Although the proposed regulations include some protections for trade secrets, those provisions must be strengthened, as discussed below. Further, providing information about the logic behind individual consequential decisions may pose technical implementation challenges. Finally, we suggest removing requirements in to describe specific details of product improvements in response to access requests — both to avoid overly-long responses to consumers and to prevent disclosure of confidential information.

Third, protections for trade secrets should be expanded. While we appreciate that the proposed regulations provide new trade secrets protections for the pre-use notice and access rights, that language should be expanded. Specifically, it should protect “intellectual property or other confidential information,” in addition to protecting trade secrets, to help ensure that companies can comply with the proposed regulations without putting at risk their business operations.

Fourth, the proposed regulations should clarify the scope of opt-outs to be implemented by service providers. The proposed regulations allow consumers to opt out of ADMTs used when a business makes a significant decision. However, in some circumstances the proposed regulations require a business to comply with a consumer’s opt-out request by instructing all its service providers to remove a consumer from ADMT processing within a specified timeframe. This creates challenges because service providers do not generally have visibility into all the data they process on behalf of a business. Generally, service providers are subject to contractual and other protections that limit their access to personal data. The proposed regulations should be clarified to expressly state that service providers are only to implement opt-outs of the ADMT encompassed by the proposed regulations.

Fifth, exceptions to the opt out rights should be revised to make them workable in practice. The obligations for businesses to respond to consumers' opt out requests create several exceptions, including when ADMTs are used for admission, acceptance, or hiring decisions, and when ADMTs are used for allocation/assignment of work and compensation decisions. As a condition of both exceptions, the proposed regulations require that the ADMT works for the business's purpose and does not unlawfully discriminate based upon protected characteristics. That language in Section 7221 should be revised, because it is unclear how a company would determine that the ADMT "works" for its purposes. Instead, we recommend requiring a business to take reasonable steps to verify that the ADMT works for the business's purpose and to mitigate risks of unlawful discrimination based upon protected characteristics.

Recommendation: The CPPA should:

- Narrow the information required in pre-use notices.
- Ensure the information companies are required to provide in response to ADMT access requests is not unduly burdensome.
- Expand protections for trade secrets to also protect intellectual property and other confidential information.
- Clarify the scope of opt-outs to be implemented by service providers.
- Revise exceptions to opt-out rights in Section 7221 to focus on "taking reasonable steps" to ensure ADMT works for a business.

Third: The regulations should be harmonized with other legislative and regulatory efforts.

Today's technology ecosystem is global, and companies are developing strong compliance programs that can be leveraged across jurisdictions to support the responsible development and use of AI systems. As the CPPA addresses these issues, we strongly encourage you to account for the global context surrounding the draft regulations.

Even within California, legislators and other state regulators are advancing proposals to regulate the use of AI tools in circumstances likely to have the most significant impact on consumers' lives. BSA is concerned that efforts by the legislature, CPPA, and California Civil Rights Council (CCRC) risk imposing three different sets of rules on certain uses of automated tools — particularly in employment contexts — in just one state. Indeed, the broader context of AI regulation also counsels in favor of reading the CPPA's statutory authority to issue regulations on ADMT narrowly. Under the California Privacy Rights Act (CPRA), regulations are to govern "access and opt-out rights with respect to business's use of automated decisionmaking technology, including profiling." This authority is phrased narrowly, to focus on ADMT in the context of the access and opt-out rights already included in CPRA. The proposed regulations appear to go beyond this statutory mandate, in areas where other regulators and lawmakers are proposing and adopting policies.

Recommendation: The CPPA should work with its counterparts in the legislature and at the CCRC to help ensure consistency in proposed frameworks governing the use of automated tools. The CPPA should also read its statutory mandate to issue regulations on ADMT narrowly, to decrease opportunities for potential conflicts in regulatory frameworks.

II. Cybersecurity Audits

Data security is a critical aspect of protecting personal information. We appreciate several recent changes to the proposed regulations on cybersecurity, but strongly recommend the CPPA further leverage internationally-recognized audits and certifications — which in many cases, companies already conduct to demonstrate compliance with leading cybersecurity requirements.

Most importantly: the regulations should clearly treat companies as compliant with the CCPA's cybersecurity audit requirements if they conduct an audit or certification under

leading global cybersecurity standards, like ISO 27001 or SOC 2. Not only does this promote strong cybersecurity practices, it would also greatly reduce the economic impact of the proposed rules, which was a clear priority for several CCPA board members at the May 1 meeting.

We appreciate several revisions to the proposed cybersecurity regulations and urge you to retain those changes. These include:

- Involving a company's executive management team in audit oversight, rather than its board. The revised regulations require audits be reported to a business's executive management team, rather than its board. We strongly support this change, because board members are not themselves subject matter experts and should be able to rely on the expertise of cybersecurity and other personnel for information about cybersecurity risks.
- Referring to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The CSF sets the global standard for managing cybersecurity risks. We are pleased that the revised draft regulations refer to the CSF and strongly encourage you to further leverage this important tool to promote strong cybersecurity practices.

We also urge you to make three changes to improve the draft cybersecurity regulations.

First: The proposed regulations should expressly state that a company satisfies the CCPA's cybersecurity audit requirement if it conducts an audit, certification, or evaluation under leading standards, including ISO 27001 and SOC 2.

Companies already perform cybersecurity audits and assessments under globally-recognized standards and frameworks. The proposed regulations should recognize that these audits and certifications satisfy the CCPA. Not only would leveraging these existing cybersecurity audit tools promote leading cybersecurity practices, it would greatly reduce the economic impact of the regulations without compromising privacy or security. For example:

- In the United States, businesses conduct audits or assessments of their cybersecurity practices to comply with a range of federal laws including the *Sarbanes-Oxley Act (SOX)*, *Federal Acquisition Regulation (FAR)*, and *Defense Federal Acquisition Regulations Supplement (DFARS)*. The United States Government also requires companies supplying products or services to federal agencies to comply with FedRAMP, the U.S. Department of Defense's Cybersecurity Maturity Model Certification (CMMC), and the Federal Information Processing Standards, among other requirements.
- Customers also frequently require their vendors to demonstrate strong cybersecurity practices — creating another layer of certifications and audit requirements that companies already do. For example, customers frequently require vendors to certify they are compliant with the ISO 27000-series of standards, which govern information security management.² Organizations perform internal audits of information security management systems to assess their compliance with the ISO 27001 standard and prepare for external audits, which are required to obtain ISO 27001 certification. This certification can only be issued by an accredited certification body. Likewise, under the American Institute of Certified Public Accountants' System and Organization Controls (SOC) framework, organizations obtain SOC 1, SOC 2, and/or SOC 3 reports and audits. The most comprehensive of these audits is SOC 2, which is an external audit performed by certified public accountants who must be independent of the organization they are assessing.

The CCPA should expressly recognize that existing audits and certifications satisfy the CCPA. The revised regulations take one step in this direction, by stating that a business may utilize a

² See ISO/IEC 27001 and related standards, *available at* <https://www.iso.org/isoiec-27001-information-security.html>.

cybersecurity audit, assessment, or evaluation that it has prepared for another purpose that meets the regulations' requirements — and specifically references the NIST CSF. But the regulations should go farther and list additional specific audits and certifications that satisfy the CCPA's requirements, to avoid imposing duplicative audit requirements without clear security benefits.

Instead of leveraging existing cybersecurity tools, the proposed regulations create California-specific audit requirements. This reinvents the wheel, creating additional and redundant audit obligations. Even worse, the California-specific requirements fail to clearly identify where they create obligations that are stricter than existing global frameworks. As a result, it is difficult for companies to map the existing cybersecurity audits they conduct against California's requirements. As the Regulatory Impact Assessment explains, four common security frameworks (the CSF, CIS Critical Security Controls v.8, ISO/IEC 27001, and SOC 2, Type II) each have "some overlap with the 18 core components" of California's proposed regulations.³ But the proposed regulations do not clearly enable companies to leverage their use of well-established tools and audit frameworks.

The economic impact of this approach is significant. Companies that already conduct cybersecurity audits based on globally-recognized frameworks only reduce their cost of compliance with California's audit requirements by 30%, according to the Regulatory Impact Assessment. That means companies must pay for duplicative California-specific audits without a clear understanding of where the CPPA intends to create new requirements. This approach is also burdensome for the CPPA, because California-specific obligations will have to be updated over time by the agency. That duplicates work already done by other organizations, such as NIST updating its CSF or ISO updating the 27001 standards. We urge you to avoid this approach and instead treat companies as compliant with the CCPA if they already use leading existing audits, certifications, and frameworks.

Recommendation: Recognize that leading cybersecurity audits and certifications satisfy the CCPA. California-specific cybersecurity audits should only be contemplated if companies do not already conduct audits or certifications under existing frameworks. Specifically:

- Section 7123(f) should be modified to state: A business may utilize a cybersecurity audit, assessment, or evaluation that it has prepared for another purpose, provided that it **is reasonably similar in scope to meets all of the requirements of** this Article, either on its own or through supplementation. For example, a business may have engaged in an audit **or certification** that uses the National Institute of Standards and Technology Cybersecurity Framework 2.0, **ISO 27001 certifications, SOC 2 audits, FedRAMP authorization, or similar audits and certifications. Such audits and certifications and meets all of the requirements of** this Article.

Second: Any California-specific audit requirements should be flexible, risk-based, and harmonized.

Companies should only be required to conduct California-specific cybersecurity audits if they do not already conduct the types of cybersecurity audits and certifications discussed above. Any California-specific requirements should be grounded in a flexible and risk-based approach, and promote consistency with existing standards, frameworks, and laws. This is especially important as cybersecurity regulations continue to increase internationally and at the federal and state level, each establishing new requirements and definitions that produce different approaches to compliance. CPPA should also issue guidance, such as crosswalks, that compare security controls under the

³ See Standardized Regulatory Impact Assessment, Page 51 ("We assume that if a company utilizes an existing framework to assess its cybersecurity program, this will result in a 30% reduction in costs to complete the [cybersecurity audit]") (Nov. 22, 2024), *available at* https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_impact.pdf.

proposed regulations to common frameworks, standards, and auditing criteria such as the NIST CSF, ISO 27001, SOC 2, and programs like FedRAMP.

Recommendation: The CPPA should ensure that any California-specific requirements adopt a flexible, risk-based, and harmonized approach that is aligned to leading cybersecurity standards, frameworks, and laws. Such requirements should specifically leverage the NIST CSF, ISO 27001, and SOC 2. In addition, the CPPA should publish guidance including crosswalks between these California-specific requirements and leading frameworks, including the NIST CSF, ISO 27001, SOC 2, and programs like FedRAMP.

Third: The cybersecurity audit provisions should clearly focus on personal information a company processes in its role as a business and not as a service provider.

Businesses that process personal information in a manner that presents “significant risk” to consumers’ security are required to complete cybersecurity audits under the draft regulations.

While this obligation is clearly placed on *businesses*, not service providers, the regulations are based on thresholds that may inadvertently wrap in personal information that a company processes in either its role as a business or its role as a service provider. Under the proposed regulations, processing presents a “significant risk” if a business processes a certain threshold of data. We are concerned that these thresholds do not account for the fact that some companies may process personal information as a business (for some products and services) and also process personal information as a service provider (for other products and services). Because the cybersecurity audit requirements apply to businesses — and not service providers — the proposed regulations should clearly state that the cybersecurity audit requirement and its thresholds only apply to personal information that companies process in their role as businesses.

Recommendation:

- Modify Section 7120(b) to state: A business’s processing of consumers’ personal information presents significant risk to consumers’ security if any of the following is true **for personal information it processes in its role as a business**:
- Modify Section 7123(a) to state: The cybersecurity audit must assess how the business’s cybersecurity program: protects personal information **that it processes in its role as a business** from unauthorized access, destruction, use, modification, or disclosure; and protects against unauthorized activity resulting in the loss of availability of personal information.

III. Risk Assessments

Data protection assessments are an important part of privacy compliance programs. BSA has supported a range of state and global privacy laws that require businesses to conduct data protection assessments of high-risk processing activities, which help companies identify and assess potential privacy risks and to adopt appropriate mitigation measures.

We appreciate several revisions to the most recent proposed regulations on risk assessments and urge you to retain those changes. These include:

- Narrowing the set of AI-related activities that will require risk assessments, by focusing on ADMT. The prior draft regulations would have required risk assessments of all processing used to train AI that is “capable of being used” for five broad activities. We appreciate the effort to more narrowly focus on processing that is intended to train an ADMT, identity verification, or physical or biological identification or profiling. (Section 7150(6).)
- Removing requirements to identify actions taken to maintain the quality of personal information processed by ADMT or AI. The prior draft regulations would have required risk

assessments to identify specific actions the business has taken to maintain quality of personal information, including a vague list of actions that do not easily apply across different types of AI-based processing. (Section 7152.)

- Focusing on information-sharing obligations for companies that make ADMT available to other businesses. The prior draft regulations would have required businesses that train both ADMT and AI and permit others to use it to provide a plain language explanation of limitations on the technology. We appreciate the current draft focuses instead on providing the recipient business with the facts available to the original business. (Section 7153.)
- Narrowing the set of materials to be provided to the CPPA. The prior draft regulations would have required businesses to submit abridged risk assessments to the CPPA, including the categories of personal information they process and the safeguards they implement. But that information is often confidential and disclosure creates trade secrets concerns. We appreciate the current draft narrowing the set of materials businesses must proactively provide to the agency — and recommend further narrowing them, as discussed below.

We also urge you to make five changes to the draft regulations on risk assessments.

First: Promote the use of risk assessments across jurisdictions.

Global companies have conducted privacy risk assessments for more than a decade. As a result, they have established processes for conducting and documenting such assessments, including under global privacy laws like the EU's General Data Protection Regulation (GDPR) and Brazil's General Data Protection Law (LGPD), and under state laws in 17 states.⁴ We appreciate California's recognition that risk assessments are important — but the regulations should not adopt unique documentation requirements that fragment global compliance programs. Companies create stronger compliance programs that better protect consumers when they focus on developing a single set of risk management practices that apply across jurisdictions, instead of diverting resources to address a web of bespoke obligations.

The proposed regulations should promote the use of risk assessments across jurisdictions. The regulations start to acknowledge the importance of global risk assessments through Section 7156, which recognizes that when a business conducts a data protection assessment for the purpose of complying with another jurisdiction's law or regulations, it may also satisfy the obligations under CCPA. We strongly recommend that language go farther, to recognize that impact assessments satisfy the CCPA's obligations if they are reasonably similar in scope to the proposed regulations.

Recommendation:

- Modify Section 7156 to state: A business may utilize a risk assessment that it has prepared for another purpose to meet the requirements in section 7152, provided that the risk assessment ~~is reasonably similar in scope -contains the information that must be included in, or is paired with the outstanding information necessary for, compliance~~ with section 7152.

Second: Do not require risk assessment information be submitted under penalty of perjury.

The proposed regulations require risk assessments be submitted to the agency under penalty of perjury. Specifically, the employee submitting risk assessment information to the CPPA must attest that: (1) the business has conducted a risk assessment, (2) that the employee meets the requirements imposed by the regulations to submit a risk assessment, and (3) that the information is true and correct. That submission is to be made under penalty of perjury.

⁴ See: BSA's Models of State Privacy Legislation, *available at* <https://www.bsa.org/policy-filings/us-2024-models-of-state-privacy-legislation>.

In California, perjury is punishable by up to four years imprisonment.⁵ Imposing criminal penalties under these circumstances is disproportionate to the harm the regulations seek to address, of ensuring that the CPPA is provided truthful information. We strongly urge you to remove any language requiring risk assessment information be provided under penalty of perjury.

Recommendation:

- Modify Section 7157(b)(5) to state: Attestation to the following statement: “I attest that the business has conducted a risk assessment for the processing activities set forth in California Code of Regulations, Title 11, section 7150, subsection (b), during the time period covered by this submission, and that I meet the requirements of section 7157, subsection (c). ~~Under penalty of perjury under the laws of the state of California,~~ I hereby declare that the risk assessment information submitted is true and correct.”

Third: Narrow the set of activities requiring risk assessments.

The proposed regulations require risk assessments for six types of processing. We recommend revising two of the scenarios for which assessments are required:

- First, Section 7150(b)(1) should be narrowed to require a risk assessment when a business sells or shares *sensitive personal information*, rather than all personal information. This can help reduce uncertainty around tracking technologies like cookies, and whether they are deemed to “share” information. Requiring a risk assessment for use of any tracking cookies would significantly expand the requirement to conduct assessments, without clear benefits.
- Second, we recommend clarifying that the processing of sensitive personal information in employment-related contexts is exempt, by broadening Section 7150(b)(2)(A). The current language can be read narrowly, in ways that create different requirements for similar types of employment-related processing activities.

Recommendation:

- Modify Section 7150(b)(1) to state: selling or sharing sensitive personal information.
- Modify Section 7150(b)(2)(A) to state: A business that processes the sensitive personal information of its employees or independent contractors solely and specifically for ~~employment-related purposes of administering compensation payments, determining and storing employment authorization, administering employment benefits, providing reasonable accommodation as required by law, or wage reporting as required by law,~~ is not required to conduct a risk assessment for the processing of sensitive personal information for these purposes. Any other processing of consumers’ sensitive personal information is subject to the risk-assessment requirements set forth in this Article.

Fourth: Clarify that risk assessment information does not include specific types of personal information.

The proposed regulations require businesses to proactively provide the CPPA with specific risk assessment information. This makes California an outlier, and we strongly recommend the regulations avoid requiring disclosure of detailed information about risk assessments. The current text could be read to require companies to disclose specific types of personal information they process, by requiring a business to state “whether the risk assessment . . . involved the processing of each of the categories of personal information and sensitive personal information” covered by the CCPA.

⁵ Cal. Penal Code § 118.

We strongly encourage you to make clear that businesses only need to state in the risk assessment information whether they process either personal information or sensitive personal information, as those terms are defined in the CCPA. The regulations should not require businesses to list the specific types of personal information they process, which can create a range of privacy and security concerns. For example, if cybersecurity company discloses the categories of information it processes to detect threats, it can create a roadmap for bad actors to circumvent security protections. This concern is compounded because the proposed regulations do not appear to limit the CPPA's further disclosure or use of the risk assessment information.

Recommendation:

- Modify Section 7157(b)(4) to state: Whether the risk assessments conducted or updated by the business during the time period covered by the submission involved the processing of **personal information or sensitive personal information, as those terms are defined each of the categories of personal information identified** in Civil Code section 1798.140, subdivisions (v)(1)(A)-(L), (ae)(1)(A)-(G), and (ae)(2)(A)-(C).

Fifth: Treat risk assessment information provided to the CPPA as confidential.

The proposed regulations should also be revised to protect any risk assessment information disclosed to the agency. We strongly encourage you to revise the proposed rules to ensure: (1) risk assessment information provided to the CPPA is treated as confidential and exempt from disclosure under open records law, (2) disclosure of risk assessment information to the agency does not constitute a waiver of attorney-client privilege, work product protection, or other applicable protections.⁶ This will not only help avoid inadvertent disclosure of proprietary data and business practices that may be reflected in a risk assessment, but also create strong incentives for companies to undertake rigorous risk assessments.

Recommendation:

- A new provision should state: **Confidentiality. Risk assessment materials disclosed to the Agency are to be treated as confidential by default and are exempt from open records laws. In addition, providing materials to the Agency does not constitute a waiver of attorney-client privilege, work product protection, or other applicable protections.**

* * *

BSA supports strong privacy protections for consumers, and we appreciate the opportunity to provide these comments. We welcome an opportunity to discuss these important issues.

For further information, please contact:

Meghan Pensyl
Director, Policy
meghanp@bsa.org

Kate Goodloe
Managing Director, Policy
kateg@bsa.org

Business Software Alliance

⁶ This protection is provided by other state privacy laws. See, e.g., Colo. Rev. Stat. § 6-1-1309(4); Conn. Gen. Stat. § 42-529b(f); 6 Del. C., § 12D-108(c); Fla. Stat. § 501.713(3); Ind. Code § 24-15-6-2(b); Ky. Rev. Stat. Ann. § 367.3621(4-5); Md. Code Ann., Com. Law, § 14-4710(d)(3); Minn. Stat. § 325O.08(f); Mont. Code Ann. § 30-14-2814(3)(c-d); Neb. Rev. Stat. § 87-1116(4); N.H. Rev. Stat. Ann. § 507-H:8(III); N.J. Rev. Stat. § 56:8-166.12(b); Or. Rev. Stat. § 646A.586(7); R.I. Gen. Laws § 6-48.1-7(f); Tenn. Code Ann. § 47-18-3307(c); Tex. Bus. & Com. Code Ann. § 541.105(d); Va. Code Ann. § 59.1-580(C).

Grenda, Rianna@CPPA

From: Canter, Libbie <ecanter@cov.com>
Sent: Monday, June 2, 2025 9:57 AM
To: Regulations@CPPA
Cc: Ortiz, Jorge; Patrick Warren; Clara Kim
Subject: Bank Policy Institute: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: Bank Policy Institute comment letter (Jun. 2, 2025).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,

On behalf of the Bank Policy Institute, please find attached comments to the Agency's proposed modifications to its proposed regulations on automated decisionmaking, cybersecurity audits, and risk assessments.

Warmly,
Elizabeth Canter

Elizabeth Canter

Covington & Burling LLP
One CityCenter, 850 Tenth Street, NW
Washington, DC 20001-4956
T +1 202 662 5228 | ecanter@cov.com
www.cov.com

COVINGTON



June 2, 2025

Via electronic mail

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

Re: **Comments on Proposed Cyber, Risk, and ADMT Rules**

The Bank Policy Institute¹ appreciates the opportunity to submit further comments to the California Privacy Protection Agency on its ongoing rulemaking under the California Consumer Privacy Act, as amended by the California Privacy Rights Act (“CCPA”).² In particular, BPI’s members are commenting on the proposed draft rules addressing automated decisionmaking technologies (“ADMT”), risk assessments, and cybersecurity audits.³

BPI’s members are committed to protecting consumers against privacy and other related harms, and, at the same time, encouraging interoperability between future regulations and other legal frameworks. In light of these goals, BPI supports changes that the Agency has proposed in its most recent draft rules, particularly changes to the scope of ADMT.

BPI encourages the Agency to consider additional clarifications and refinements to its rules to ensure that the new rules do not frustrate other federal and state policy goals, such as by undermining cybersecurity and fraud prevention goals. It is critical, for example, that the Agency include robust fraud exceptions to its ADMT rules so that it does not undermine the ability of banks and other businesses to protect themselves and consumers from fraud. In addition, there remain elements of the proposed rules that continue to be overly granular and prescriptive and do not serve to enhance existing privacy protections afforded to consumers.

¹ The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation’s leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost two million Americans, make nearly half of the nation’s small business loans, and are an engine for financial innovation and economic growth.

² Cal. Civ. Code § 1798.100 *et seq.*

³ The proposed rules also include certain other changes to the rules the Agency adopted in March 2023, including to the scope of the sensitive information definition and correction rights (“Amendments to March 2023 Rules”). BPI urges the Agency to consider the Amendments to the March 2023 Rules as part of a separate rulemaking processing that affords the public adequate opportunity to consider and evaluate these proposed changes. The Agency should not rush through these Amendments to the March 2023 Rules as part of the process to develop new rules in highly complicated and important areas.

These fixes are particularly important to the extent that the Agency does not include broader exemptions from its new rules for banking organizations.⁴ However, BPI continues to recommend that the Agency create exemptions from new cybersecurity audit, ADMT, and risk assessment rules for banking organizations. As described in greater detail below, at least two elements of the Agency’s proposed rules interfere with the exclusive visitorial powers over national banks and federal savings associations granted to the Office of the Comptroller of Currency: (1) obligations to conduct, attest to the Agency completion of, and, upon request, submit risk assessments; and (2) obligations to conduct, and certify to the Agency completion of, cybersecurity audits. As BPI noted in its previous letter, for these kinds of banking organizations, all three proposed rules would be preempted since they would interfere with federally authorized banking activities.

I. ADMT

BPI supports the Agency refocusing its ADMT rules on tools that replace human decisionmaking, which helps mitigate the risk that the Agency’s rules would unintentionally capture commonplace uses of software that do not make decisions about consumers. However, BPI urges the Agency to consider further clarifying and scoping these rules in several important respects and to provide additional examples of what constitutes and does not constitute ADMT that are consistent with the comments below.

As context for these recommendations, most of the personal information processed by banking organizations is subject to the Gramm-Leach-Bliley Act (“GLBA”) and therefore exempt, by statute, from the CCPA and its implementing regulations. The Agency’s proposed rules nonetheless threaten to interfere with the fraud prevention and compliance activities of banks and their vendors, which may involve the processing of mixed data sets that include personal information that is not subject to GLBA.

As such, it is critical that the Agency include robust fraud exceptions to its ADMT rules that are at least as broad as the concept of ensuring “security and integrity” contemplated in the underlying statutory framework. *See* Cal. Civ. Code § 1798.140(ac). Unfortunately, the proposed § 7221 removes entirely a partial fraud exception from the opt-out rights under the proposed rules, even though BPI had advocated to broaden the exception. When criminals have stolen an identity to open an account or take over an existing account, they will almost certainly opt the victim’s data out of the ADMT capabilities in order to evade detection, ultimately enabling the criminal to be more successful in executing fraudulent activity. If bad actors or others may opt out of the use of their data (or victim data) for training automated fraud detection or credit underwriting tools or the use of such tools on their loan applications, the Agency would create risk for the consumers it seeks to protect by hobbling banks’ ability to monitor for fraud. As Federal Reserve Governor Michelle Bowman recently noted, “customers are the ones who suffer” where “our regulatory environment is not receptive to the use of AI” for fighting fraud. As a result, “the regulatory system should promote these improvements [through AI tools] in a way that is consistent with applicable law and appropriate banking practices.”⁵

In addition, consistent with BPI’s prior comments, the fraud exemptions that the Agency retained for pre-use notification obligations and ADMT access rights remain too narrow. The fraud exemptions in

⁴ Throughout, BPI uses the term “banking organization” to refer to national and state banks and savings associations and their affiliates, as well as foreign banking organizations and their U.S. branches to the extent the California rules purport to apply to them. BPI provided several alternative language proposals to exempt such organizations, including language providing that: “This Article [9, 10, or 11] does not apply to financial institutions that are subject to examination or supervision by a federal prudential regulator and their affiliates as defined under the Bank Holding Company Act, 12 U.S.C. § 1841(k).”

⁵ Michelle W. Bowman, Gov., Fed. Reserve, Address at 27th Annual Symposium on Building the Financial System of the 21st Century: An Agenda for Japan and the United States: Artificial Intelligence in the Financial System (Nov. 22, 2024), *available at* <https://www.federalreserve.gov/newsevents/speech/bowman20241122a.htm>.

the relevant provisions – that is, § 7220(d)(2) and § 7222(c) – fail to cover fraud prevention activities conducted by banking entities that are not “directed at” only the business or consumers. For example, in the context of payment card transaction processing, fraud may be directed at merchants and other financial institutions. Likewise, illegal actions, such as money laundering and sanctions violations, may be “directed at” entities other than a bank (e.g., the federal government).

Likewise, it should be explicit that the new ADMT obligations do not compromise a business’s ability to further compliance objectives, including to identify and prevent illegal activity. In BPI’s prior comments, it provided the Agency several examples of long-standing and socially beneficial compliance uses of ADMT tools that the Agency’s rules do not adequately address. For example, banks use automation to prevent parties that are subject to economic sanctions from accessing the U.S. banking system; review payment card transactions to complete chargebacks for challenged transactions; and apply lending standards.

An exception for fraud and compliance activities also is necessary given statutory limitations on the Agency’s ability to interpret the CCPA framework in a manner that restricts the ability of businesses to comply with other laws or protect individuals from fraud.⁶ In the case of financial institutions, laws require institutions to protect customers from fraud.⁷ The statute also specifically contemplates that consumers who exercise a request to know are not entitled to data generated to help ensure “security and integrity.” *See, e.g.*, Cal. Civ. Code § 1798.130(a)(3)(B)(iii). The Agency should not craft a more limited fraud exception to its new ADMT access rights than the fraud exceptions in the underlying statute for requests to know. Instead, it should be clear that businesses are not required to provide pre-use disclosures or ADMT access rights, and are not required to honor opt out rights, that would limit their ability to ensure “security and integrity” or to comply with laws, consistent with the underlying statutory framework.

Second, the ADMT provisions addressing significant financial decisions should focus only on credit adjudication and account openings. Currently, the draft rules propose a broad definition of “financial or lending services” to include, for example, “transmitting or exchanging funds” and “check cashing.”⁸ Coupled with the removal of the fraud exemption, such a broad definition could force financial institutions to provide individuals the right to opt-out of security and fraud checks or to appeal transactions that are blocked automatically—something that occurs thousands, if not millions of times per day—and that present real risk of harm to other consumers.⁹ Financial institutions already have well-honed and secure mechanisms to let customers unblock accounts or prove they are a real person. Therefore, BPI recommends narrowing the definition to focus only on adjudication and account openings.

Third, BPI urges the Agency to focus its ADMT provisions only on *material* employment-related decisions, like hiring, promotion, and termination. In particular, the draft rules propose a broad definition of “employment or independent contracting opportunities or compensation” decisions that would include any tool used *to allocate or assign work*.¹⁰ Thus, a broad reading of this language could capture algorithms used for routine business purposes, such as those that use automation to optimize scheduling or manage workflows. This kind of allocation of work is not the same as the other kinds of material

⁶ *See* Cal. Civ. Code § 1798.145(a) (obligations shall not restrict a business’s ability to comply with federal, state or local laws); *id.* § 1798.145(k) (obligations imposed on businesses shall not adversely affect the rights and freedoms of other natural persons).

⁷ *See, e.g.*, 12 CFR Part 41, Subpart J; 12 CFR Part 1005.6; 12 CFR 1026.13.

⁸ *See* § 7001(ddd)(1).

⁹ *See, e.g.*, Stripe, How Stripe responded to a wave of card testing attacks, available at <https://stripe.com/newsroom/news/card-testing-surge> (describing how Stripe’s fraud prevention solution blocked more than 20 million suspected fraudulent payments per day during a surge of credit card fraud).

¹⁰ *See* § 7001(ddd)(4)(B).

human resources decisions contemplated (*e.g.*, hiring, promotion, and termination) and is out of place. BPI therefore recommends modifying § 7001(ddd)(4)(B) to remove the “allocation or assignment of work” language. Alternatively, this language should be tied to ADMT that does more than merely allocate work but could potentially result in some prohibited discriminatory treatment to the consumer.

Fourth, the ADMT rules should more clearly recognize that businesses have flexibility to provide distinct opt-out experiences from different types of ADMT. The current version of § 7221(c) contemplates that businesses will offer consumers methods of submitting a request to opt-out of “ADMT,” without acknowledging that businesses may use ADMT in different contexts, and an individual may want to opt out of the use of ADMT for certain employment purposes, but not others.

II. Risk Assessments

BPI appreciates that the Agency has aimed to further clarify the scope of risk assessments. However, BPI urges the Agency to narrow the risk assessment triggers and minimize prescriptive requirements that have little benefit to customers. In addition, in Section IV, we also discuss legal limitations on the Agency’s ability to compel banking organizations to furnish risk assessment reports to the Agency.

Under the draft rules, the threshold for conducting risk assessments should be aligned to existing risk assessment frameworks and other sections of the draft regulations. As BPI previewed in its prior letter, other privacy frameworks require risk assessments for activities that are “likely to result in a high risk to the rights and freedoms of natural persons.” The Agency appeared to account for such scoping in its revisions to the ADMT requirements, which impose substantive requirements where ADMT makes a “significant decision” that results in the provision or denial of essential services (*e.g.*, financial or lending services, housing, education enrollment or opportunities, employment opportunities).¹¹

In contrast, the Agency’s current draft rules would still require risk assessments for certain activities that do not present analogous risks to consumers. As one example, there is a trigger that requires a business to conduct a risk assessment when a business is using automated processing to infer, among other things, a consumer’s behavior based upon “systematic observation” in their capacity as a job applicant, employee, and independent contractor.”¹² Per the definition of “systematic observation,” this captures any “methodical and regular or continuous observation” of employees.¹³ This is a vague and seemingly overbroad trigger given that important information security, safety, and risk management principles require at least some regular observation of employees in the workplace.

Likewise, risk assessments may be triggered if a business is “processing the personal information of consumers, which the business intends to use to train” ADMT for a significant decision concerning a consumer or certain other technologies, including those that “verif[y] a consumer’s identity.” Preliminarily, the Agency does not have authority under the auspices of regulating automated decision-making to regulate training of systems. Further, this is a convoluted and unclear standard, particularly for businesses in regulated industries that may rely on a mix of data subject to the CCPA and data that is exempt from the CCPA to train tools.

¹¹ See §§ 7001(ddd), 7200(a).

¹² See *id.* § 7150(b)(4). The EU General Data Protection Regulation also requires data privacy impact assessments where there is “systematic monitoring of a publicly accessible area on a *large scale*,” although the Agency’s rulemaking authority is tied to technologies that make *decisions* about consumers, regardless of the scale. Regulation (EU) 2016/679 (General Data Protection Regulation), Art. 35(3)(c) (emphasis added). In addition, the CCPA framework does not apply to publicly available data. Cal. Civ. Code § 1798.140(v)(2).

¹³ See § 7001(eee).

Further, the processing of sensitive information should not trigger a risk assessment when the sensitive personal data is being processed only for purposes specified in § 7027(m) of the Agency’s existing rules. Section 7027(m) recognizes that there are many routine processing activities involving sensitive personal data for which consumers should not have rights to limit the use or disclosure of their information, such as the processing of credit card information to enable consumers to complete transactions. These routine processing activities do not impose the kinds of “significant risks” to consumer privacy that merit a risk assessment, particularly if that assessment must address the prescriptive elements contemplated by the Agency’s proposed rules. Thus, in addition to the exemptions for certain routine human resources purposes, the Agency should make clear that a risk assessment is not required when the sensitive personal data is being processed only for purposes specified in § 7027(m).

Instead, the risk assessment requirements should be more clearly limited to activities that present a significant risk to consumers. BPI recommends that the Agency require risk assessments only for selling, sharing (for cross-context behavioral advertising), processing sensitive information (subject to exemptions for routine processing activities, such as those specified under § 7027(m)), and “significant decisions.” Thus, the Agency should delete the currently proposed §§ 7150(b)(4), (b)(5), and (b)(6) and any corresponding examples in § 7150(c). This will make the CCPA framework more consistent with other jurisdictions and will avoid a requirement that forces businesses to churn out paperwork assessments for run-of-the-mill technologies rather than conducting thoughtful assessments for activities that present a genuine significant risk to consumer privacy. In addition, there should be exemptions for activities that are already subject to examination or supervision by a federal prudential regulator, if not a broader exemption for banking organizations, as discussed in further detail below in Section IV.

With respect to the substantive requirements in a risk assessment, BPI urges the Agency to adjust the requirements in § 7152(a) to be less prescriptive. The risk assessment requirements under § 7152(a)(3) contemplate specific information that does not align with the requirements of risk assessments in other laws and may not always be relevant. Businesses should have discretion to evaluate whether these elements should be evaluated as part of a risk assessment. In addition, the requirement in section 7152(a)(1) to avoid generic terms in describing the purpose of processing will be resource intensive without corresponding benefits. Indeed, this type of prescriptive requirement will be most burdensome for entities with existing risk assessment frameworks with a track record of effectiveness. BPI members may be forced to spend resources re-working existing processes instead of putting resources towards ongoing risk assessments themselves.

Finally, the Agency should also make clear that risk assessments are required only for new processing activities—not those that occurred prior to the effective date of the regulations. Conducting risk assessments for all historical activities that would be covered by the rules would be an enormous compliance burden on businesses without any corresponding consumer benefit. As BPI previously described, for banking organizations, longstanding Bank Secrecy Act (“BSA”), Anti-Money Laundering (“AML”), and Know Your Customer (“KYC”) programs, small business lending, cybersecurity, and anti-fraud programs all require the processing of sensitive information and have been actively risk assessed, audited and examined by federal regulatory agencies for decades. Forcing a massive audit of all these data processing activities and requiring a potential re-do of risk assessments even for activities that have been in place for many years without negative impacts to consumer privacy is neither feasible nor a desirable use of privacy resources.

III. Cybersecurity Audits

BPI appreciates changes made by the Agency to the proposed cybersecurity audit rules, particularly those that seem motivated by interoperability with recognized industry standards, such as those published by the National Institute of Standards and Technology. However, the Agency still lacks

the statutory authority to adopt a prescriptive set of affirmative cybersecurity requirements. Relatedly, the regulations fail to consider, and may even contradict, existing frameworks and best practices, such as those with which banking organizations must comply. As such, BPI urges the Agency to consider further modifications to clarify and refine the scope of the cybersecurity audit provisions.

The Agency's statutory authority is limited to creating provisions on audits, yet it seeks to craft its own idiosyncratic cybersecurity control framework by requiring businesses to justify why they do not deploy any single tactic from a five-page, excessively prescriptive list of cybersecurity measures. In BPI's prior comments, it urged the Agency to permit businesses to conduct cyber audits under other commonly used risk frameworks such as the NIST *Framework for Improving Critical Infrastructure Cybersecurity* ("NIST CSF") and the Cyber Risk Institute Profile ("CRI Profile"). In its latest proposal, the Agency partially incorporated this recommendation by stating that a business may rely on an audit that uses "the National Institute of Standards and Technology Cybersecurity Framework 2.0." Nevertheless, while new language in § 7123(f) acknowledges the NIST CSF, the proposed rule contemplates that such an audit is sufficient only if it "meets all the requirements of this Article." That qualification should be removed. The NIST CSF framework is widely-accepted and non-prescriptive by design, and a significant number of financial institutions have adopted the CRI Profile as a successor to the Federal Financial Institutions Examination Council ("FFIEC") Cybersecurity Assessment Tool ("CAT") that is being sunset on August 31, 2025. Both the NIST CSF and CRI Profile are designed to ensure businesses achieve a desired outcome rather than being a "checklist of actions to perform."¹⁴

Further, an overly prescriptive cybersecurity audit rule does not advance the Agency's policy goals and could impede businesses from focusing auditing resources on elevated risks. For example, the proposed rules still contemplate a *single* annual information security audit. This provision is in tension with the more rigorous approach to cybersecurity audits conducted by banking entities on a rolling basis. The Agency's approach also encourages businesses to adopt a less effective, one-size-fits-all audit approach that would restrict an institution's ability to deploy audit resources consistent with their internal risk assessments and in alignment with International Auditing Standards.¹⁵ Banking organizations conduct annual risk assessments and audit planning to allocate more audit resources for the highest risk entities and issues as required by International Auditing Standards. This enables them to focus audit resources on areas of higher residual risk, often in consultation with their prudential regulators.

The Agency's changes to the reporting requirements for internal auditors highlight the problems with the Agency's overly prescriptive approach. The Agency amended the proposed § 7122 would require the highest-ranking internal auditor to report to a member of the business's *executive management team* who does not have direct responsibility for the business's cybersecurity program. Most banks employ a structure where the chief auditor reports to the board of directors (or an audit committee of the board of directors). This configuration is consistent with the Agency's previous approach, which proposed requiring the auditor to report to the business's *board of directors or governing body*. Such a reporting structure may not be appropriate for all businesses, but the Agency lacks a clear policy rationale to require businesses to abandon their current reporting structure. For banking organizations, requiring internal auditors to report to a member of the business's executive management team would also be

¹⁴ See NIST Cybersecurity Framework at 6.

¹⁵ See, e.g., The Institute of Internal Auditors, Global International Audit Standards, AUDITING CYBERSECURITY OPERATIONS: PREVENTION AND DETECTION (2nd Edition), available at <https://www.theiia.org/en/content/guidance/recommended/supplemental/gtags/gtag-auditing-cybersecurity-operations-prevention-and-detection/>.

contrary to guidance and best practices.¹⁶ The Agency should move away from prescriptive requirements that do not account for reasonable variations in approach among institutions of different sizes.

Further, the draft regulations continue to prohibit auditors from making recommendations on the business's cybersecurity program.¹⁷ Internal auditors frequently make observations as part of their audit reports that businesses can elect to leverage to resolve identified issues and improve their cybersecurity posture. This is seemingly impermissible under the draft regulations and would thereby disincentivize auditors from making actionable observations without any apparent policy rationale.

Consistent with BPI's prior comments, the Agency should adopt a less prescriptive approach that clarifies that specific cybersecurity measures must only be addressed where reasonably determined to be appropriate and clarifies that multiple periodic audits may be used to comply with the statute. Moreover, as discussed in additional detail below, there are serious questions about whether the Agency has authority to impose significant new regulations on how banking organizations manage cybersecurity audits.

IV. Exemptions

BPI continues to urge the Agency to create exemptions from the three new areas of rules for banking organizations to avoid conflict with these organizations' federal regulation and supervision and to prevent unintended and detrimental impacts on the safety and soundness of the U.S. banking and payments systems. As described in detail in BPI's prior comments, the Agency must adopt such exemptions to avoid the potential for legal challenges and preemption given two longstanding principles of preemption: first, the OCC has exclusive visitorial rights for national banks and federal savings associations;¹⁸ and second, the Supreme Court established and has upheld as recently as last year the principle that state regulation of banks is preempted where it prevents or significantly interferes with a bank's ability to conduct federally authorized activities.¹⁹

¹⁶ Indeed, there also are distinctions between *functional* reporting and *administrative* reporting, and banking regulators have encouraged banks to ensure their chief audit executive *functionally* reports to a committee of the board of directors, even if he or she administratively reports to executive management. A reporting requirement that the highest-ranking internal auditor functionally report to a member of the business's executive management team deviates from existing enforceable standards for national banks, including the OCC's Heightened Standards. *See, e.g.*, 12 C.F.R. pt. 30, app. D ("the Chief Audit Executive has unrestricted access to the audit committee with regard to risks and issues identified through internal audit's activities"). *See also* Board of Governors of the Federal Reserve System, Supplement Policy Statement on the Internal Audit Function and Its Outsourcing, at 5 (January 23, 2013), *available at* <https://www.federalreserve.gov/supervisionreg/srletters/sr1301a1.pdf> ("A reporting arrangement may be used in which the CAE is functionally accountable and reports directly to the audit committee on internal audit matters (that is, the audit plan, audit findings, and the CAE's job performance and compensation) and reports administratively to another senior member of management who is not responsible for operational activities reviewed by internal audit. When there is an administrative reporting of the CAE to another member of senior management, the objectivity of internal audit is served best when the CAE reports administratively to the chief executive officer (CEO).").

¹⁷ *See* CPPA Draft Regulations § 7122(a)(2).

¹⁸ *See* 12 U.S.C. § 484. Visitorial powers are defined as (i) examination of a bank; (ii) inspection of a bank's books and records; (iii) regulation and supervision of activities authorized or permitted pursuant to federal banking law; and (iv) enforcing compliance with any applicable federal or state laws concerning those activities. Notably, examination of a bank's books and records is not limited to on-site inspection. *See* 12 C.F.R. § 7.4000. These requirements have been extended to federal savings associations and their subsidiaries. *See* 12 CFR § 7.4010(b).

¹⁹ *See Cantero v. Bank of America, N.A.*, 144 S. Ct. 1290 (2024). Federal preemption applies to federal savings associations in the same way as it applies to national banks. Dodd-Frank Act section 1046, codified at 12 U.S.C. 1465.

As described in BPI's prior comments, elements of the proposed regulations would, if applied to banking organizations, interfere with the exclusive visitorial powers granted to the OCC, irrespective of the application of the GLBA.²⁰ For example, California cannot directly conduct the cyber audits required by the proposed rules for banking organizations, and so it cannot indirectly achieve that result by having banks conduct a highly prescriptive audit on its behalf or requiring an audit certification. These obligations would result in the Agency effectively inspecting and supervising banking activities, which is the exclusive purview of the OCC with respect to national banks and federal savings associations. Likewise for risk assessments: California cannot force banks to conduct risk assessments that meet very specific requirements and then provide an attestation of completion of risk assessments (and, upon request, provide a "risk assessment report," which contains almost all the information in the full version of each risk assessment). This type of direct inspection interferes with the OCC's visitorial rights.

Further, for national banks and federal savings associations, the three new proposed rules would be preempted since they would interfere with federally authorized banking activities.²¹ The standard articulated by the Supreme Court looks to whether a state law "prevents or significantly interferes" with the bank's conduct of a "federally authorized activity."²² As discussed in BPI's prior comments, the proposed new rules interfere with the authority that national banks and federal savings associations have to, among other banking activities, use technology to deliver banking products and services.²³

The Agency unquestionably has authority to create exemptions for banking organizations; indeed, its rulemaking authority contemplates that its regulations should "further the purposes of" the CCPA, which include designing cyber audit and risk assessment protections for businesses whose processing of personal information presents significant risk to consumer privacy and security. It does not serve these purposes to impose the proposed requirements on banking organizations and their affiliates that are subject to prudential examination or supervision on these same issues and that process limited personal information that is subject to the CCPA framework.

While these legal limitations should provide sufficient rationale, there also are strong policy rationales for adopting the exemptions recommended by BPI. Federal financial regulators already closely supervise the cybersecurity and risk assessment practices and use of automated decisionmaking by banking organizations and their affiliates.²⁴ Indeed, as noted in our prior letter, federal supervision of

²⁰ See *Barnett Bank of Marion County, N.A. v. Nelson*, 517 U.S. 25 (1996); 12 U.S.C. § 481 (documenting the OCC's authority to examine and require reporting from national banks); 12 U.S.C. § 484; 12 C.F.R. § 7.4000; 12 U.S.C. § 1465; and *Cuomo v. Clearing House Ass'n*, 557 U.S. 519 (2009).

²¹ 517 U.S. 25 (1996). Under *Barnett*, which was codified for certain purposes by the Dodd-Frank Act, a court typically conducts a two-step analysis. First, the court determines whether the power or activity affected by the state law in question is authorized for national banks. Second, the court evaluates the degree of interference, or impact, the state law has on the national bank's exercise of the power. The court then draws a conclusion about whether the law is preempted.

²² *Id.* See also *Cantero v. Bank of Am., N.A.*, 602 U.S. 205, 221 (2024) (applying the *Barnett* standard).

²³ National banks and federal savings associations are broadly authorized to use technology to deliver products and services so long as the means used are consistent with safety and soundness. 12 C.F.R. § 7.5000 (national banks); 12 C.F.R. Part 155 (federal savings associations).

²⁴ These regulators include federal prudential regulators (i.e., Board of Governors of the Federal Reserve System ("Board"), Federal Deposit Insurance Corporation ("FDIC"), and Office of the Comptroller of the Currency ("OCC")) and, for state-chartered financial institutions, state banking regulators in addition to federal prudential regulators. The federal prudential regulators have developed an extensive inventory of policy statements, toolkits, and other guidance that set regulatory expectations for banks' information security, model risk management, and audit programs, including "regarding the security of all information systems and information maintained by or on behalf of a financial institution" across GLBA and non-GLBA data. FFIEC, IT EXAMINATION HANDBOOK:

these activities is excessive. The supervisory model results in regulators having an ongoing presence within the banks to monitor the effectiveness of cyber programs and monitor compliance with privacy and model risk management rules. Duplicative—yet slightly different—requirements in the draft rules would divert resources from promoting privacy and safeguarding our banking system in accordance with existing federal frameworks without corresponding benefit. At worst, they could disrupt the comprehensively regulated U.S. banking system, including potentially interfering with how banking organizations use automated processes to carry out their core banking activities.²⁵

* * *

V. Conclusion

To sum, BPI encourages the Agency to clarify and refine its rules to ensure that the CCPA does not frustrate other federal and state policy goals, such as by undermining cybersecurity and fraud prevention goals. The Agency’s ADMT draft rules can be further refined to avoid future issues regarding scope and potential conflicts with the underlying statutory language. BPI recommends that the Agency align its risk assessment requirements to other frameworks and remove prescriptive requirements. BPI also requests that the Agency modify portions of its cybersecurity audit requirements to avoid creating conflicts with existing frameworks and federal best practices. BPI continues to recommend that the Agency create exemptions for banking organizations to avoid conflict with these organizations’ federal regulation and supervision and to prevent unintended and detrimental impacts on the safety and soundness of the U.S. banking and payments systems.

These recommendations are consistent with the January 14, 2024 comments that BPI submitted to the Agency, and BPI refers the Agency to its prior comments for recommendations for specific regulatory language.

* * *

The Bank Policy Institute appreciates the opportunity to submit these comments to the California Privacy Protection Agency on its rulemaking on cybersecurity audits, risk assessments, and automated decisionmaking under the California Consumer Privacy Act. If you have any questions, please contact the undersigned by phone at (202) 589-2523 or by email at Patrick.Warren@BPI.com.

Respectfully submitted,

/s/ Patrick Warren

Patrick Warren
Vice President, Regulatory Technology, BITS
Bank Policy Institute

INFORMATION SECURITY at 1 n.4 (Sept. 2016), available at <https://ithandbook.ffiec.gov/it-booklets/information-security/> (“Information Security Booklet”); see also OCC, COMPTROLLER’S HANDBOOK: MODEL RISK MANAGEMENT (Aug. 2021), available at <https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/model-risk-management/index-model-risk-management.html> (“Model Risk Management Booklet”).

²⁵ This would not be consistent with the statutory design of the CCPA, which sought to avoid interference with federal regulation, including through exemptions for data subject to federal financial privacy frameworks, such as GLBA and the Fair Credit Reporting Act.

Grenda, Rianna@CPPA

From: Gottlieb, Darbi <DGottlieb@advamed.org>
Sent: Monday, June 2, 2025 4:59 PM
To: Regulations@CPPA
Cc: Chang, Terry
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: 2025.06.02_AdvaMed CCPA Comments_ (1).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 see attached for The Advanced Medical Technology Association's comments on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations.

Thank you,

Darbi Gottlieb

Director, State Government & Regional Affairs

P :: 928.830.8735

E :: dgottlieb@advamed.org

advamed.org

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

The Advanced Medical Technology Association (“AdvaMed”) appreciates the opportunity to comment on the California Privacy Protection Agency’s (“CPPA’s/Agency’s”) “Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (“ADMT”), and Insurance Companies.”¹ We appreciate the Agency’s continued public engagement throughout the rulemaking process to address the concerns of all stakeholders and welcome your attention to these important topics.

We believe the proposed regulations represent a step in the right direction. At the same time, we believe that as currently drafted, the proposed regulations regarding ADMT would negatively impact patients and create overly burdensome requirements on top of already extensive patient data protection regulations. Therefore, AdvaMed requests that the regulations include an exemption for medical device manufacturers, particularly where they do not have visibility into the regulated status of the healthcare professional. Implementing this recommendation will help ensure that the ADMT regulations do not impose unnecessary and harmful requirements on medical devices regulated by the U.S. Food and Drug Administration that maintain data in the same manner as covered entities (“CEs”) or business associates (“BAs”).

AdvaMed recognizes and appreciates the existing exemptions for certain types of entities and medical or health information under Cal. Civ. Code § 1798.146, including providers and medical information governed by the Confidentiality of Medical Information Act (“CMIA”) and protected health information that is collected by a CE or BA governed by the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) (“HIPAA”) and its implementing regulations. However, a significant number of data processing activities involving health information are not covered by such exemptions, and it would be inappropriate to subject such data processing to the proposed ADMT regulations.

About AdvaMed

AdvaMed is a trade association that represents the world’s leading innovators and producers of medical devices, diagnostic products, and digital health technologies. Together, our members manufacture much of the life-enhancing health care technology purchased annually in the United

States and globally. Our members are committed to the development of new technologies that allow patients to lead longer, healthier, and more productive lives. The technologies made by AdvaMed members help patients stay healthier longer and recover more quickly after treatment, allow earlier detection of disease, and treat patients as effectively and efficiently as possible.

Entities and Data Processing Activities Outside the Scope of CCPA Exemptions

As an initial matter, HIPAA only regulates a Health Care Provider (“HCP”) when it conducts certain transactions² related to health insurance coverage electronically. As a result, a concierge physician or direct primary care physician³ who does not accept insurance will not engage in HIPAA-covered transactions (electronic transmissions of patient information related to insurance coverage) and, accordingly, will not be a CE under HIPAA.⁴ Thus, data from medical devices used by such providers is not protected under HIPAA.

And while some medtech companies can be CEs or BAs under HIPAA, depending on the services provided, the same companies may technically be neither a CE nor a BA in other scenarios with respect to the same type of device.

Furthermore, some health care providers purchase medtech through third-party distributors. In many instances, the medtech company does not have a means of interacting with clinicians to ascertain whether or not the HCP is a HIPAA CE. Such companies, as well as other HCPs offering products and therapies not directly subject to HIPAA’s privacy and security regulations, will voluntarily handle all patient data from devices in both scenarios as a HIPAA CE must treat protected health information for several reasons, including:

- to ensure a high level of protection for the patient’s data;
- because they lack visibility into identity, and therefore the HIPAA-covered status, of the patient’s HCP; and
- to promote operational consistency within the health care ecosystem and provide assurances to their HIPAA-covered business partners.

Medtech companies that lack visibility into whether data from medical devices is protected under HIPAA will not be able to rely on the exemptions under Cal. Civ. Code § 1798.146.

Extended Exemptions for Medtech Data

The CCPA’s ADMT regulations should regulate health data uniformly and not have different privacy rules based on the type of entity in the health industry handling the same health data. This is especially true given the right for consumers to opt-out of the use of ADMT for significant decisions. This opt-out may not be practicable or safe in the context of medtech data. For example, such uses of ADMT in the medical context may be vitally important to the well-being of a patient. Furthermore, medtech providers may not know the identity of patients’ HCPs and may be unable to communicate such opt-outs to medical providers, resulting in interruptions to patients’ care.

AdvaMed respectfully requests that CCPA clarify that medical device manufacturers are exempt from Article 11 requirements under the Proposed Regulations.

Sincerely,



Darbi Gottlieb
Director, State and Regional Affairs
AdvaMed

Grenda, Rianna@CPPA

From: Hake, Davis Y. <DYHake@Venable.com>
Sent: Monday, June 2, 2025 2:55 PM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: ATAI CPPA Comments to Modifications (06.02.25).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](#)

Thank you for your work and reception of our comments from the Alliance for Trust in AI.

-Davis Hake

Davis Y. Hake | Senior Director of Cybersecurity Services | [Venable LLP](#)
t 415.653.3745 | f 415.653.3755 | m [REDACTED]
101 California Street, Suite 3800, San Francisco, CA 94111

DYHake@Venable.com | www.Venable.com

This electronic mail transmission may contain confidential or privileged information. If you believe you have received this message in error, please notify the sender by reply transmission and delete the message without copying or disclosing it.



Convening stakeholders across industries to craft principles and concrete codes of practice for the development and use of artificial intelligence.

June 2nd, 2025

RE: California Privacy Protection Agency (CPPA) Modifications to the Text of Proposed Regulations for Automated Decisionmaking Technology, Risk Assessments, Cybersecurity Audits, Insurance, and Updates to Existing Regulations

These comments are submitted on behalf of the Alliance for Trust in AI (ATAI), a nonprofit association of companies using artificial intelligence (AI) representing diverse sectors. Members of ATAI seek to ensure that AI can be a trusted tool by promoting effective policy and clear codes of practice for AI.

Thank you for the opportunity to provide comments on the CPPA's modified proposed regulations on automated decisionmaking technology (ADMT). We appreciate the CPPA's constructive engagement and the incorporation of several of our February 2025 suggestions into the modified text. In this letter, we acknowledge key improvements in the latest proposal and recommend further refinements to ensure the rules protect consumers while fostering innovation and effective risk management. Our goal is to collaborate with the CPPA in crafting actionable, balanced rules that promote trustworthy innovation in ADMT.

About the Alliance

The Alliance for Trust in AI (ATAI) brings together companies using advanced AI in many sectors to advocate for ways that we can build trust in all the kinds of AI that empower companies across the country and world. ATAI works with companies developing foundational AI models, creating AI systems, and implementing these systems and models in their own work across industries.

We aim to give organizations concrete guidance on how to build AI responsibly, implement AI principles, support learning and information sharing across sectors, and establish a shared voice for the many users of AI now and in the future. ATAI is building on work done by

technologists, policymakers, and academics to create a shared understanding of how to develop and use AI responsibly. Through multi-stakeholder partnership with members across industries and sectors, ATAI is developing definitions, principles, and codes of practice that ensure that AI is available, and trusted, for everyone.

Acknowledgment of Improvements in the Modified Text

Refined Definition of ADMT

ATAI is pleased to see the refined definition of “automated decisionmaking technology” in the May 2025 modifications. The new text clarifies when an automated tool truly “executes or replaces” human decisions versus when a human meaningfully remains in the loop. These changes directly address our feedback that the prior definition was overly broad. By narrowing the scope to true decision-making systems and exempting ordinary IT utilities, the CPPA has reduced unwarranted compliance burdens on low-risk technologies.

We believe the definition could further be enhanced by revising it to focus on information that is necessary to make decisions, removes language on the replacement of human decision making, and includes “search term software” to help limit unintentional capture of non-related technologies and actions.

Clarified Scope of “Significant Decisions”

We appreciate the updates to the definition of a “significant decision” to better scope which automated decisions warrant regulation. These clarifications align with ATAI’s February comments urging a more nuanced definition focused on truly consequential decisions. By focusing on high-impact decisions and excluding routine or preparatory steps (like eligibility screening or ads), the CPPA’s revisions improve both the *clarity* and *practicality* of the rules.

Structured Opt-Out Exceptions for Security and Safety

ATAI also commends the CPPA for introducing structured exceptions to the consumer’s right to opt out of ADMT in certain important scenarios. Overall, these additions demonstrate the CPPA’s willingness to incorporate stakeholder input and craft exceptions that maintain consumer trust without inadvertently hampering security or beneficial uses of AI.

ATAI thanks the CPPA for these meaningful revisions. By refining definitions and adding sensible exceptions, the modified proposal moves closer to a workable, effective framework. We offer the following suggestions to continue aligning the rules with innovation-friendly, risk-based oversight of ADMT.

Emphasizing Trust and Innovation Through a Risk-Based Approach

In our view, the strength of any ADMT regulation lies in fostering trust, both for consumers in AI-driven services and society's trust that innovation can occur responsibly. We urge the CPPA to continue refining the regulations with an eye toward contextual, risk-based rules that protect individuals while encouraging beneficial innovation. Overly rigid or one-size-fits-all mandates could stifle innovation and divert resources away from productive uses of AI. ATAI's February comments noted that not every automated decision carries the same risk, and the same technology can pose vastly different impacts depending on context. We encourage the CPPA to lean further into this principle. For example, low-risk implementations, such as an AI tool optimizing equipment maintenance schedules or personalizing a user's website experience, should warrant lighter requirements or even exclusion from certain provisions. By calibrating obligations to the likelihood and severity of harm, businesses will be motivated to focus compliance efforts where it truly matters, and consumers will receive protections (and disclosures) that are meaningful rather than superfluous.

We strongly support the need for interoperability in risk assessment requirements across states, at the federal level, and among like-minded international jurisdictions. Risk assessments should not be state-specific, such as requiring a unique California assessment. Instead, businesses should be allowed to rely on assessments conducted to comply with laws that are similar in scope and effect, as is the case under nearly all other U.S. state privacy laws. The purpose of a risk assessment is to ensure that businesses evaluate and weigh potential privacy harms arising from high-risk processing activities. As innovation progresses, the nature of these activities will evolve making it essential that businesses retain flexibility in how they structure and approach assessments to focus on relevant and emerging risks.

However, the approach outlined in the proposed rules are overly prescriptive. It risks turning assessments into a check-the-box exercise, diverting attention from the substantive factors that matter most in evaluating privacy risks. This rigid structure imposes significant compliance burdens without corresponding benefits to consumers. California businesses operate in national and global markets and are already conducting robust assessments to comply with laws such as the GDPR. Yet, the proposed rules do not permit full reliance on those existing assessments, forcing businesses to create California-specific supplements for the same processing activities. The CPPA has not demonstrated how this duplicative requirement provides meaningful additional privacy protections.

Differentiating Developers, Integrators, and Deployers in Compliance Obligations

We respectfully urge the CPPA to recognize within the regulations the distinct roles in the AI ecosystem, specifically the developers of AI models or software, the integrators who incorporate AI modules into larger systems, and the end-user deployers who actually use ADMT in practice. These roles have different capabilities and responsibilities for managing risks, and a nuanced approach would improve both feasibility and effectiveness of compliance. ATAI previously highlighted that developers, integrators, and deployers have distinct roles and abilities to mitigate risks throughout an AI system's lifecycle. For example, a model developer can perform testing and implement technical safeguards in a controlled environment before release. An integrator can evaluate compatibility and address system-level vulnerabilities. The deployer is best positioned to conduct real-world impact assessments and apply appropriate human oversight or controls in the deployment context. The modified regulations would benefit from provisions that tailor requirements or accountability based on these roles. For instance, risk assessment and transparency report obligations might differ for an AI service provider (developer) versus a business utilizing that service (deployer). The current draft's requirements are primarily written as if one entity is responsible for the entire ADMT lifecycle. In reality, compliance might be shared across multiple parties and this should be reflected in regulations.

Tailoring Notice and Opt-Out Requirements to Low-Risk Uses

ATAI recommends further tailoring of the notice and consumer opt-out provisions to avoid overburdening low-risk, routine uses of ADMT that are part of everyday operations. If applied too broadly, notice and opt-out requirements could produce notification fatigue for consumers and heavy compliance costs for businesses with little corresponding benefit. We caution that a similar outcome could occur if every minor use of ADMT triggers a formal notice or opt-out offering. The CPPA's revised definition of "significant decision" and the exceptions for security/fraud uses already help by narrowing scope, and we encourage building on that approach.

We suggest clarifying that pre-use notices and opt-out links are only required for ADMT uses that pose more than minimal risk to consumers or involve decisions of consequence. Moreover, we advocate for flexibility in *how* notices and opt-out choices are presented, to allow integration into user-friendly interfaces rather than one-size-fits-all banner notices. The modified proposal's new language about consolidated or contextual notices is a step in the right direction, but for example, do not limit the pre-use notice requirement to only where ADMT processing is otherwise subject to *access* and *opt-out* rights. As a result, businesses will be required to provide such notices even if they use ADMT for exempt purposes for which consumers do not

have the right to access or opt out. We encourage expanding this concept so businesses can use context-sensitive disclosures that inform consumers without overwhelming them.

Clarifying Use-Based Exemptions for Embedded ADMT Tools in Multi-Purpose Systems

Finally, we urge the CPPA to provide greater clarity and flexibility around use-based exemptions, particularly when ADMT is embedded in multi-purpose systems. Modern AI-driven products often integrate decision-making components for different purposes within a larger system. Under the modified draft, such a business could invoke the security/fraud opt-out exception only if the ADMT in question is used *"solely"* for those protective purposes. We are concerned that this strict interpretation might unintentionally penalize multi-use AI systems. As we noted in our prior comments, *limiting the exemption to ADMT that is "necessary" and "solely" for security or fraud prevention could constrain the cybersecurity and anti-fraud capabilities of platforms that incorporate these functions into broader services*. We recommend the CPPA clarify that businesses can still qualify for the security/fraud exception even if the platform or system has other functions, as long as the particular ADMT use at issue is for one of the protected purposes.

Conclusion and ATAI's Ongoing Commitment

ATAI appreciates the CPPA's modifications and the opportunity to contribute further to this rulemaking. We share the CPPA's goal of promoting consumer protection and trustworthy AI innovation in equal measure. We believe that clear, contextual, and proportionate rules will empower organizations to build and use AI responsibly while keeping California at the forefront of technological competitiveness. ATAI remains committed to assisting the CPPA in crafting actionable, balanced regulations through continued dialogue, technical input, or any other means that the Agency finds helpful. We look forward to working together toward our shared objective of trustworthy AI deployment that benefits consumers and society.

If you have questions, or believe that we can be helpful to your work in any way, please contact the ATAI's coordinator Heather West, at hewest@venable.com.

Grenda, Rianna@CPPA

From: Travis Frazier <tfrazier@ana.net>
Sent: Monday, June 2, 2025 11:00 AM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: FINAL Ad Trade Comments on ADMT and CCPA Regulations - June 2025.pdf

Importance: High

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 Board:

Please find attached comments from the following advertising trade associations in response to the CPPA's request for public comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations: the Association of National Advertisers, the American Association of Advertising Agencies, the American Advertising Federation, the Interactive Advertising Bureau, and the Digital Advertising Alliance. We appreciate your consideration of these comments.

If you have any questions about these comments, please feel free to reach out to Chris Oswald at coswald@ana.net.

Best Regards,
Travis Frazier

Travis Frazier

Senior Manager, Government Relations | **Association of National Advertisers (ANA)**

P: 202.296.2097 | ana.net | [LinkedIn](#)

2020 K Street, NW, Suite 660, Washington, DC 20006

The ANA drives growth for you, your brand, our industry, and humanity. Learn how at ana.net/membership.

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

Dear California Privacy Protection Agency:

On behalf of the advertising industry, we provide these comments in response to the California Privacy Protection Agency's ("CPPA" or "Agency") proposed updates to the state's regulations implementing the California Consumer Privacy Act ("CCPA") and proposed new regulations governing risk assessments, automated decisionmaking technology ("ADMT"), cybersecurity audits, and insurance companies.¹ Below we provide comments on the Agency's proposed ADMT rules and the proposed updates to the existing CCPA regulations.

We appreciate the changes the Agency made to the prior version of the proposed ADMT rules to align their scope with the CCPA and tailor their impact to higher-risk data processing contexts, such as significant decisionmaking. However, the CPPA's current regulatory package would still make significant changes to existing privacy mandates. In particular, the definition of ADMT is still significantly broad and is not cabined to the use of automated processing for significant decisions. In addition, the proposed rules would create costly new assessment, opt-out, and rights request processing requirements. These requirements would disrupt automated processing functions that benefit consumers, stifling the economy, slowing innovation, and burdening both consumers and businesses alike.

We ask the Agency to make certain further revisions to the proposed regulations in line with the suggestions in this submission. We submit comments on the following specific areas with the goal of improving the proposed regulations to benefit consumers and businesses, enhancing clarity in the regulatory text, and furthering the operational workability of new mandates set forth in the proposed rules:

- I. Comments on Proposed Regulations on ADMT**
 - a. The Proposed Definition of ADMT Is Overly Broad
 - b. The Proposed Risk Assessment Requirements are Overly Prescriptive and Onerous
 - c. The Proposed Definition of "Sensitive Location" is Overly Broad
- II. Comments on Proposed Updates to CCPA Regulations**
 - a. Opt-Out Signal Status Display Requirements Should Not Be Required

¹ See *Modified Text of Proposed Regulations*, CALIFORNIA PRIVACY PROTECTION AGENCY (May 9, 2025), available [here](#).

- b. Notice Requirements Should Be Adaptable Across Various Channels and Allow Flexibility in Connected Device Settings
- c. The Scope of CCPA Applicability for Nonprofits Should Be Clarified and Harmonized with the Law

III. The CCPA Should Provide a Longer Compliance Timeline for its Updates to the CCPA Regulations Given the New Mandates

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of responsible companies across the country that make up and support the digital economy. These companies range from small businesses to household brands, advertising agencies, publishers, and technology providers. Our combined membership includes more than 2,500 companies that power the commercial Internet and the digital economy, which accounted for 18 percent of total U.S. gross domestic product ("GDP") in 2024.² By one estimate, over 1.8 million jobs in California are related to the ad-subsidized Internet.³ Our group has more than a decade's worth of hands-on experience it can bring to bear on matters related to consumer privacy and controls. We would welcome the opportunity to engage with the CCPA further on the points we discuss in these comments.

I. Comments on Proposed Regulations on ADMT

While we acknowledge and agree with changes the Agency has made to the ADMT regulations to narrow their scope, the proposed regulations still include an extraordinarily broad definition of ADMT that would encompass virtually all computing processes that power the modern economy and bestow significant benefits on consumers. The definition itself is not cabined to ADMT in the context of significant decisions. The proposed regulations would also create overly prescriptive risk assessment requirements for certain processing activities and uses of ADMT. These risk assessments would prove challenging and costly to implement, especially for small and mid-sized businesses which may lack the resources to require full participation from all individuals involved in data processing and decision-making. Moreover, the proposed regulations would define "sensitive location" in a manner that includes locations that are not sensitive. We address these issues below.

a. The Proposed Definition of ADMT is Overly Broad

While the Agency has modified its proposed definition of ADMT, the revised proposed definition of ADMT remains overly broad as the term itself is not limited to significant decisionmaking. As drafted, ADMT would include "any technology that processes personal information and uses computation to replace human decisionmaking or substantially replace human decisionmaking... includ[ing] *profiling*" (emphasis added).⁴ "Substantially replace human decisionmaking" means a business uses the technology's output to make a decision

² John Deighton and Leora Kornfeld, *Measuring the Digital Economy*, INTERACTIVE ADVERTISING BUREAU, 8 (April 2025), located at https://www.iab.com/wp-content/uploads/2025/04/Measuring-the-Digital-Economy_April_29.pdf.

³ *Id.* at 130-132.

⁴ Cal. Code Regs., tit. 11, § 7001(e) (proposed), available [here](#).

without human involvement.⁵ Although the substantive ADMT mandates in the proposed rules are cabined to use of ADMT for significant decisions, the ADMT definition itself is still broadly construed, encompassing nearly all types of modern computing processes, including routine data-handling tasks that are automated. In testimony before the Agency and in a letter to the CCPA sent by California legislators, concerns were voiced regarding the sweeping nature of these rules and their failure to differentiate between activities that present minimal or no tangible risk to consumers.⁶ We acknowledge and appreciate steps CCPA has taken steps to hone the ADMT rules' scope. However, further amendments to limit the scope of the definition itself would help to cabin the rules' impact to processing that presents actual risks to consumers. Without amendments to refine and clarify the definition's scope, the regulations could lead to unintended consequences that extend beyond their intended purpose.

In particular, the proposed rules would create opt-out, access, and Pre-Use Notice requirements in the context of use of ADMT for significant decisions. However, the proposed definition of "significant decision" does not clarify that the term applies only to decisions about consumers acting in individual or household contexts and not in commercial or business-to-business contexts.⁷ As drafted, the ADMT definition could be read to be broader, such as applying to decisions about businesses looking to obtain commercial credit or loans. The "significant decision" definition should be clarified so it applies solely to decisions about consumers acting in individual or household contexts and not in commercial or business-to-business contexts. Furthermore, definitions related to rights to opt out of and access ADMT should clearly indicate that they apply solely to use of ADMT for significant decisions. While definitions of key terms, such as "right to opt-out of ADMT," "request to opt-out of ADMT," "right to access ADMT," and "request to access ADMT" apply "as set forth in... Article 11," which creates requirements for use of ADMT for significant decisions, to foster clarity, the definitions should be revised to explicitly state that they pertain exclusively to ADMT within the context of significant decision-making.⁸ Such a clarification would help to squarely limit the impact of new rights to use of ADMT for significant decisions and avoid the potential for scope creep.

In addition, the CCPA's proposed definition of ADMT would include "profiling," and the proposed regulations would broaden the statutory definition of "profiling" in a manner which would result in further expanding the definition of ADMT. The CCPA defines profiling as "any form of automated processing of personal information, as further defined by regulations..., to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."⁹ The Agency's proposed regulations would add elements to the definition, further defining profiling as "any

⁵ *Id.* at § 7001(e)(1) (proposed).

⁶ See *Public Comment on ADMT Regulations*, submitted by Members of the California Legislature (February 19, 2025), available [here](#).

⁷ Cal. Code Regs. tit. 11, § 7001(ddd) (proposed).

⁸ *Id.* at §§ 7001(jj), (qq), (ss), (xx) (proposed).

⁹ Cal. Civ. Code § 1798.140(z).

form of automated processing of personal information to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person’s *intelligence, ability, aptitude*, performance at work, economic situation; health, *including mental health*; personal preferences, interests, reliability, *predispositions*, behavior, location, or movements” (emphasis added).¹⁰

Instead of providing clearer boundaries for what constitutes profiling and ADMT, the expanded profiling definition proposes to introduce additional categories—such as intelligence, ability, aptitude, mental health and predispositions—that would increase regulatory uncertainty regarding the scope of the ADMT rules. While advertising has rightfully been excluded from the context of “significant decisions,” the ADMT term, used in isolation, could be interpreted to include advertising functions due to the broad definition of “profiling” that is included in the ADMT definition. By encompassing a wider range of personal attributes, the new “profiling” definition would extend the scope of compliance requirements for businesses and organizations that process consumer data using ADMT. In effect, rather than achieving clarity, the expansion of the “profiling” definition amplifies the complexity and potential impact of the ADMT definition. The Agency should refine its definition of ADMT, so the term encompasses only high risk automated decisionmaking rather than any automated computing process.

b. The Proposed Risk Assessment Requirements are Overly Prescriptive and Onerous

The proposed regulations include numerous onerous requirements that would be significantly challenging for businesses of all sizes to implement. In particular, prescriptive terms surrounding stakeholder involvement in an assessment, timelines for required assessment updates, executive accountability for assessments, and disclosure of assessments to the Agency contain rigid obligations that would be supremely challenging for small and mid-sized businesses to implement. The proposed requirements surrounding risk assessments should be amended so they are more flexible rather than prescriptive to aid companies of all sizes in completing legally sufficient assessments.

One prescriptive and unclear proposed assessment requirement that is unlikely to be scalable to businesses of all sizes is the requirement for specific stakeholder involvement in the process. The proposed rules state that “[i]ndividuals whose job duties include participating in the processing of personal information subject to a risk assessment must be involved in the risk assessment process for that processing activity.”¹¹ The scope of this requirement is unclear and potentially very broad and could potentially require every employee that in some way “touches” personal information to be directly involved. Additionally, the proposed regulations state that “an individual who determines the method by which the business plans to collect consumers’ personal information for one of the processing activities” necessitating a risk assessment must “provide that information to the individuals conducting the risk assessment.”¹² This requirement

¹⁰ Cal. Code Regs. tit. 11, § 7001(ii) (proposed).

¹¹ *Id.* at § 7151(a) (proposed).

¹² *Id.* (proposed).

also lacks clarity. It is not clear what kind of “information” that a decisionmaker is required to provide to individuals conducting the risk assessment, and how this information must factor into the assessment.

Instead of imposing rigid mandates for stakeholder involvement in assessments, the Agency should take steps to make the requirements more flexible so businesses with different kinds of internal resources (for example, small and mid-sized businesses), teams, and decisionmaking processes are able to conduct risk assessments that meet the regulations’ requirements. The Agency should consider offering scalable guidelines that account for variations in company size and resources, ensuring that all businesses can implement reasonable stakeholder engagement.

In addition, the proposed regulations set an unrealistic timeline for updating risk assessments. Businesses are given over two years to complete their initial risk assessments (with a December 31, 2027 deadline for completion), yet only 45 days to update them following a material change in processing.¹³ This is an insufficient timeframe, considering the complexity of the regulations and scope of the risk assessment requirements. The Agency should update the proposed rules to allow for a more reasonable update period to complete relevant updates in the event of material changes to relevant processing practices. Such a change would allow businesses to conduct thorough updates to assessments without being rushed by an unnecessarily short 45-day timeline for completion.

Moreover, the proposed regulations would impose strict executive accountability requirements. They would require a member of the business’s executive management team to sign an attestation certifying the correctness of the risk assessment under penalty of perjury.¹⁴ This is an extreme measure that introduces the potential for personal legal liability. It is inappropriate to assign this sort of responsibility, with severe penalties, to individuals. Many other omnibus state privacy laws contain risk assessment requirements, but no other state requires executives to certify the accuracy of risk assessments or take on the burden of potential personal liability in the context of risk assessments. The Agency should thus remove this signed attestation requirement from the proposed risk assessment rules.

Finally, the regulations grant the CPPA unrestricted power to request risk assessment reports at any time, with no limits on how often the Agency may make such requests. Businesses would be required to submit reports within 30 days of a request, which is a rigid and demanding deadline.¹⁵ Other states typically permit state agencies to make such requests only in cases involving Civil Investigative Demands (CIDs) or formal investigations, ensuring due process and preventing unnecessary disclosure.¹⁶ This unrestricted submission requirement also raises potential legal risks. Businesses must be allowed to preserve attorney-client and work

¹³ *Id.* at §§ 7155(a)(3), (b) (proposed).

¹⁴ *Id.* at §§ 7157(b)(5), (b)(6), (c) (proposed).

¹⁵ *Id.* at § 7157(e) (proposed).

¹⁶ *See, e.g.*, Va. Code Ann. § 59.1-580(C).

product protections when submitting risk assessments to the Agency. Without these safeguards, they could be forced to disclose sensitive legal analyses and proprietary information.

Overall, the proposed risk assessment regulations create an overly prescriptive framework that increases compliance burdens, legal risks, and operational inefficiencies without necessarily benefitting consumers. Businesses need more flexibility to conduct meaningful risk assessments while ensuring regulatory compliance.

c. The Proposed Definition of “Sensitive Location” is Overly Broad

The Agency’s definition of “sensitive location” and its associated risk assessment requirement could have far-reaching unintended consequences, particularly when applied to commonplace, non-invasive activities like cross-context behavioral advertising. The regulations would require a risk assessment for profiling a consumer based on that consumer’s presence in a sensitive location.¹⁷ This requirement, coupled with the broad scope of the “sensitive location” definition, risks imposing undue risk assessment burdens on businesses of all sizes that engage in benign marketing practices – such as offering a discount at a coffee shop in or near a hospital waiting room or a college cafeteria. In addition, the requirement risks chilling lawful commercial speech and limiting advertising on important topics, including advertising to doctors and healthcare workers. As drafted, the proposed “sensitive location” definition and related risk assessment requirements would unreasonably burden free speech through advertising in or near any location the Agency has deemed to be “sensitive.”

The Agency’s proposed regulation defines “sensitive location” to mean any of the following physical places: “healthcare facilities including hospitals, doctors’ offices, urgent care facilities, and community health clinics; pharmacies; domestic violence shelters; food pantries; housing/emergency shelters; *educational institutions*; *political party offices*; legal services offices; union offices; and places of worship” (emphasis added).¹⁸ By encompassing benign locations such as educational institutions and legal services offices, this definition could complicate standard business marketing operations and frustrate consumer expectations.

For example, a university aiming to sell merchandise to fans of the university’s sports teams through location-based digital outreach would be subject to the same risk assessment requirements as a doctor’s office monitoring patients near an abortion clinic. A person’s presence in an educational institution or a legal services office is not inherently sensitive. Further, this broadly scoped definition also would lead to other non-privacy-related unintended consequences, for example, limiting mixed-use commercial developments when any of the of the physical places deemed sensitive by the CPPA might be in proximity to a retail establishment. As such, the onerous risk assessment requirements set forth in the proposed rules should not apply to automated processing to make inferences about consumers who have visited these locations.

¹⁷ Cal. Code Regs. tit. 11, § 7150(b)(5) (proposed).

¹⁸ *Id.* at § 7001(aaa) (proposed).

In addition, the inclusion of other delineated locations, such as political party offices, in the “sensitive location” definition could chill communications that California residents otherwise value. Political party offices serve as hubs of civic and democratic engagement where individuals often volunteer during campaigns in support of their preferred candidates. If political party offices are deemed “sensitive,” it could create barriers to the free exchange of ideas and information bedrock to our democracy. A more balanced approach would involve the Agency clarifying the definition of “sensitive location” to focus explicitly on places where individuals are in heightened vulnerable states—while providing explicit guidance that educational institutions, legal services offices, and voluntary civic engagement spaces like political party offices are exempt from onerous risk assessment measures.

II. Comments on Proposed Updates to CCPA Regulations

The proposed regulations would create new requirements for the timing of honoring opt-out requests and displaying the status of an opt-out preference signal and new mandates for surfacing required notices and rights. Below we provide recommendations for the CPPA’s consideration in each of these areas, which we raised in our initial submission to the Agency in February on its proposed regulation package.

a. Opt-Out Signal Status Display Requirements Should Not Be Required

The proposed regulations would shift the current voluntary business disclosure of an opt-out preference signal’s status through an “Opt-Out Request Honored” disclosure into a mandatory requirement.¹⁹ This would be a significant burden on businesses, particularly small to mid-size firms. To maintain flexibility, the Agency should preserve the existing approach which allows businesses to decide whether or not to display this status. If the Agency decides to implement a new mandate requiring this disclosure, it must ensure that the regulations carefully define clear exemptions, how the requirement will be enforced, and provide clear guidance on what constitutes a valid opt-out preference signal.

The proposed requirement to display the status of an opt-out preference signal contradicts the underlying text of California law and would create significant compliance challenges.²⁰ The law directs the CPPA to issue specific regulations governing opt-out preference signals. For instance, the CCPA instructs the Agency to issue regulations to “ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business.”²¹ According to the CCPA, the Agency also must issue

¹⁹ *Id.* at §§ 7025(c)(6); 7026(g); 7027(h) (proposed).

²⁰ According to the text of the CCPA, businesses “may elect” to either (a) “[p]rovide a clear and conspicuous link on the business’s internet homepage(s) titled ‘Do Not Sell or Share My Personal Information’” **or** (b) allow consumers to “opt-out of the sale or sharing of their personal information... through an opt-out preference signal sent with the consumer’s consent by a platform, technology, or mechanism, based on technical specifications to be set forth in regulations[.]” Cal. Civ. Code §§ 1798.135(a), (b). The CCPA itself therefore gives businesses the choice to either allow consumers to opt out through a do-not-sell link on their homepage(s) or through user-enabled global privacy controls.

²¹ *Id.* at §§ 1798.135(b)(1), 1798.185(a)(19)(A).

regulations to ensure user-enabled global privacy controls “clearly represent a consumer’s intent and [are] free of defaults constraining or presupposing such intent.”²² However, the Agency has issued no regulations to this effect, leading to a lack of standardization in the marketplace regarding what constitutes a valid opt-out preference signal. As a result, the proposed requirement to indicate the “status” of a signal requires businesses to make assumptions and guess which signals are valid in the absence of clear guidance. Imposing a requirement to note whether signals have been “honored,” without providing corresponding clarity regarding which mechanisms constitute valid signals, would create significant confusion and frustration for both consumers and businesses.

The CCPA should ensure that any requirement to display the status of an opt-out preference signal includes appropriate exceptions or limitations on enforcement to account for the prevailing uncertainty regarding what constitutes a valid signal. For example, the CCPA should ensure exemptions exist for honoring signals that are set by default or are devoid of consumer choice points to initiate the signal. Furthermore, the CCPA should also make clear that entities that offer opt-out preference signals, such as platforms, plug-ins, and browsers, must comply with the signals in the same way as other businesses. By updating the proposed regulations to incorporate reasonable exceptions and clarifications to the requirement to display the status of an opt-out preference signal, the CCPA can help prevent unfair penalties and unfair application of opt-out preference signals. This approach would also help ensure businesses are not held accountable for signals that do not comply with law or circumstances that are beyond their control, fostering a balance between regulatory compliance with operational feasibility.

b. Notice Requirements Should Be Adaptable Across Various Channels and Allow Flexibility in Connected Device Settings

The proposed regulations would require businesses to provide notice “in a manner that ensures that the consumer will encounter” applicable notices before or at the time that connected devices or augmented reality/virtual reality devices may collect personal information.²³ The proposed regulations would also mandate that notice of the right to limit to be provided in the same “manner” in which the business collects sensitive personal information.²⁴ These prescriptive requirements limit businesses’ ability to effectively reach consumers with notices across multiple channels in ways that are more accessible and consumer-friendly. They also fail to acknowledge advancements in technology, which may not permit or may make it impractical to provide notices through the medium that actually collects personal information.

Appropriate flexibility should be given so that businesses can use methods to provide notices in ways that consumers will best receive and understand them. For instance, devices like smart speakers without screens may be best suited to provide requisite notices through companion applications than through the speaker itself, as a written form of the notice may be easier for a consumer to review for pertinent information. Moreover, rigid requirements

²² *Id.*

²³ Cal. Code Regs. tit. 11, § 7013(e)(3) (proposed).

²⁴ *Id.* at § 7014(e)(3) (proposed).

regarding methods of notice are likely to lead to increased administrative burdens, higher costs, and potential compliance issues, especially for small businesses. These costs will ultimately be passed down to consumers in terms of frustrated access to innovative offerings, new AR/VR tools, and new connected devices. The proposed regulations should clarify that requisite notices for connected devices can be provided through a web or app interface. By allowing businesses to adapt notification methods to suit consumers' needs, regulations can promote clarity and accessibility.

c. The Scope of CCPA Applicability for Nonprofits Should Be Clarified and Harmonized with the Law

The proposed regulations would update the definition of “nonbusiness,” subsequently creating confusion regarding the scope of the CCPA’s applicability to nonprofits.²⁵ Under the CCPA, “business” is defined to include any for-profit entity that processes personal information related to California consumers, or on behalf of which such information is processed, and controls the purpose and means of the processing.²⁶ That definition reflects legislative intent to cabin applicability of the CCPA to for-profit entities. In addition, the California Attorney General has stated in FAQs that “[t]he CCPA generally does not apply to nonprofit organizations[.]”²⁷ The Agency should ensure that the proposed regulations align with the CCPA by incorporating text that clearly limits its applicability to nonprofits.

III. The CPPA Should Provide a Longer Compliance Timeline Given the New Mandates

Given the scope and breadth of the regulatory package, the Agency should afford businesses more than a year to comply with new mandates before they become enforceable. New requirements related to CCPA compliance will require businesses to build new processes and functionality. Providing a ramp-up period would help afford much-needed time for businesses to formulate rational approaches to compliance. The CPPA should clarify that civil and administrative enforcement of new regulatory provisions will not commence until at least one year from the date the provisions are in effect.

* * *

Thank you in advance for your consideration of these comments.

²⁵ *Id.* at § 7001(v) (proposed).

²⁶ Cal. Civ. Code § 1798.140(d).

²⁷ Rob Bonta, Attorney General, *California Consumer Privacy Act Frequently Asked Questions (FAQs)* at Question 6, located [here](#).



Sincerely,

Christopher Oswald
EVP for Law, Ethics & Govt. Relations
Association of National Advertisers
202-296-1883

Alison Pepper
EVP, Government Relations & Sustainability
American Association of Advertising Agencies, 4As
202-355-4564

Michael Hahn
EVP & General Counsel
Interactive Advertising Bureau
212-380-4700

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
202-898-0089

Lou Mastria
CEO
Digital Advertising Alliance
347-770-0322

CC: Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP
Matt Stern, Venable LLP

Grenda, Rianna@CPPA

From: Curtis, Laura E <laura.curtis@apci.org>
Sent: Friday, May 30, 2025 2:15 PM
To: Regulations@CPPA
Cc: Curtis, Laura E
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: APCIA - CPPA Comment Letter_May 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](#)

On behalf of the American Property Casualty Insurance Association ("APCIA") and our members, thank you for the opportunity to provide these comments in response to the California Privacy Protection Agency's updates to existing CCPA regulations; Cybersecurity Audits; Risk Assessments; Automated Decision-Making Technology, and Insurance Companies published on May 9, 2025. We look forward to engaging with you and your staff. Thank you!

Laura Curtis
Assistant Vice President, State Government Relations (AZ & CA)
American Property Casualty Insurance Association (APCIA)
[REDACTED] (cell)
laura.curtis@apci.org





May 30, 2025

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

RE: APCIA’s Response to Request for Comments – Updates to existing CCPA regulations; Cybersecurity Audits; Risk Assessments; Automated Decision-Making Technology, and Insurance Companies (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations).

On behalf of the American Property Casualty Insurance Association (“APCIA”)¹ and our members, thank you for the opportunity to provide additional comments in response to the California Privacy Protection Agency’s (the “Agency”) Notice of Modifications to Text of Proposed Regulations And Additional Materials Relied Upon published on May 9, 2025.² APCIA has been an active participant in the Agency’s proceedings³ since the Agency’s initial efforts to adopt regulations as directed by the California Consumer Privacy Act (“CCPA”). Given recent developments in the California legislature and continued efforts by the Privacy Protections (H) Working Group within the National Association of Insurance Commissioners (“NAIC”), we are writing to reiterate our position that the Agency should *refrain* from adopting the proposed insurance regulations. Any action by the Agency on insurance regulations at this time is more likely to cause consumer confusion and frustration, not improve consumer privacy protections.

APCIA appreciates the Agency’s efforts to incorporate and address the comments and concerns identified by the insurance industry. Unfortunately, however, the new, third illustrative example provided in the updated draft of the proposed regulations does not provide any meaningful clarity – in fact, by conflating the *status* of the data as subject to the Gramm-Leach-Bliley Act with the *purpose* for which it is being processed, the example as currently drafted is actually counterproductive because it is inconsistent with the language of CCPA. Moreover, it does not address the fundamental concern we expressed that the proposed insurance regulations risk exacerbating complexity and resulting consumer and industry uncertainty, without any material

¹ APCIA is the primary national trade association for home, auto, and business insurers.

² *Notice of Modifications to Text of Proposed Regulations And Additional Materials Relied Upon*, California Privacy Protection Agency (May 9, 2025), https://coppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_notice.pdf.

³ Comments of APCIA, Feb. 14, 2025; March 27, 2023, https://coppa.ca.gov/regulations/pdf/rm2_pre_comments_27_52.pdf#page=333; Comments of APCIA, Nov. 18, 2022, https://coppa.ca.gov/regulations/pdf/comments_103_128.pdf; Comments of APCIA, Aug. 23, 2022, https://coppa.ca.gov/regulations/pdf/comments_51_75.pdf.

improvement for consumer privacy or consumer interests generally. We reiterate our prior comments and suggestions for edits to the regulations.

The concerns driving our earlier comments are now particularly acute in light of the legislature's consideration of Senate Bill 354 ("SB 354"), which is sponsored by the California Insurance Commissioner ("Commissioner"). During the Agency's May 2025 Board meeting, Agency staff presented developments on SB 354 and members of the Board recognized that the proposed insurance regulations may need to be modified depending on how the SB 354 plays out. In fact, if either SB 354 or a new NAIC privacy Model Law is finalized and enacted, the Agency's work and regulations would likely be mooted or worse – the dueling regulatory regimes could create even greater compliance problems for insurance companies having to comply with potentially conflicting requirements, and even greater frustration and confusion for consumers trying to navigate an ever more complex privacy regulatory landscape. Either way, moving forward now means the Agency would likely need to commence a new rulemaking process later anyway to cure the unnecessary complexity.

The Agency can avoid this result by simply being patient and allowing these developments to play out before taking unnecessary action. At the very least, the Agency should consider APCIA's previously stated recommendation to add "explicit language that the likelihood of successor legislation will enhance and further clarify current law."⁴ Such language could, for example, preemptively and expressly defer to any successor legislation if and to the extent that there is any perceived conflict between the CPPA's regulations and the legislation. Insurance companies operate in a highly regulated space and have been subject to robust privacy and information security requirements under existing laws in California for decades, and successor legislation that accounts for the unique aspects of the insurance industry is the best policy solution for all stakeholders – most importantly, consumers.

Finally, we reiterate our previously stated position that the proposed regulations regarding Automated Decision-making Technology (ADMT), risk assessments, and cybersecurity audits are overly broad and could impede legitimate business practices, including fraud detection, and impose onerous reporting obligations that may outweigh any potential consumer benefits, and overstep the CPPA's statutory authority. On these points, we are aligned with the comments of the American Council of Life Insurers (ACLI), the Association of California Life and Health Insurance Companies (ACLHIC), and the Insured Retirement Institute (IRI), and echo their concerns, as well as those of the broader business community. At the least, the Agency should allow companies that are subject to similar requirements in other states to leverage existing compliance efforts, to facilitate greater compliance and allow companies to focus on the core mission of all these regulations – better protecting consumer data.

⁴ Comments of APCIA, Feb. 14, 2025, at 5.

We look forward to working with the Agency's Board and staff, and with the Department of Insurance, to develop an approach that protects consumers and provides clarity to the insurance industry.

Sincerely,

/s/ Laura Curtis

Laura Curtis

Assistant Vice President, State Government
Relations (AZ & CA)

American Property Casualty Insurance Association
(APCIA)

Grenda, Rianna@CPPA

From: Tara Hairston <THairston@autosinnovate.org>
Sent: Monday, June 2, 2025 12:14 PM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: Auto Innovators Comments on Modified Text of CPPA Proposed 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

Good Afternoon –

Please find attached comments from Alliance for Automotive Innovation (“Auto Innovators”) on the modified text of the CCPA Updates, Insurance, Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking Technology Regulations.

Auto Innovators appreciates the opportunity to provide additional feedback on the proposed regulations, and we look forward to further engagement on this regulatory proceeding.

Thank you for your time and consideration.

Regards,
Tara Hairston

Tara Hairston
Senior Director – Technology Policy
THairston@autosinnovate.org

C: [REDACTED]

Alliance for Automotive Innovation

1050 K Street, NW - Suite 650, Washington, DC 20001

autosinnovate.org - [twitter \(X\)](#) - [linkedin](#)



June 2, 2025

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

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

To Whom It May Concern:

The Alliance for Automotive Innovation (“Auto Innovators”) appreciates the opportunity to submit additional comments to the California Privacy Protection Agency (“Agency”) regarding its proposed rule on updates to the California Consumer Privacy Act (“CCPA”), cybersecurity audits, privacy risk assessments, automated decisionmaking technology, and insurance regulations. Auto Innovators submits these comments to ensure that California consumers maintain robust privacy protections while also enabling automotive companies to continue offering safe and innovative vehicles, equipment, and services.

Auto Innovators represents the full automotive industry, including the manufacturers producing most vehicles sold in the U.S., equipment suppliers, battery producers, semiconductor makers, technology companies, and autonomous vehicle developers. Our mission is to work with policymakers to realize a cleaner, safer, and smarter transportation future and to maintain U.S. competitiveness in cutting-edge automotive technology. Representing approximately 5 percent of the country’s GDP, responsible for supporting nearly 10 million jobs, and driving \$1 trillion in annual economic activity, the automotive industry is the nation’s largest manufacturing sector.

The U.S. automotive industry continues to prioritize the protection of consumer privacy, and Auto Innovators appreciates that the Agency’s modifications streamline several provisions within the proposed regulations. Some of these modifications reflect revisions that Auto Innovators requested in its previous comments. However, we contend that the proposed regulations would benefit from additional clarity and precision to appropriately balance consumer privacy protection and regulatory burden. Therefore, Auto Innovators recommends additional changes, which focus on the Agency’s proposals relating to business practices for handling consumer requests, cybersecurity audits, risk assessments, and automated decisionmaking technology.

Article 3 – Business Practices for Handling Consumer Requests

- **Requests to know.** Auto Innovators supports the Agency’s efforts to streamline and simplify compliance requirements under Article 3. In particular, we appreciate the additional clarity regarding the time constraints for submitting requests to know under section 7020 (e). However, the requirement to produce all data collected dating back to January 1, 2022, would be burdensome and could inadvertently encourage covered entities to store personal data longer

than they otherwise might. We recommend a more limited lookback period dating back to [January 1, 2024], along with the following edit:

- “the business may ask the consumer to select or input the date range for which the consumer is making the request to know or present the consumer with an option to request all personal information the business has collected **and stores** about the consumer. Use of this method is not required for personal information collected prior to **January 1, 2024.**”
- **Requests to delete.** We support the Agency’s proposed modifications to section 7022 (“Request to Delete”), as they will help ensure that all parties, including service providers and contractors, can more easily comply with the numerous provisions in the section.
- **Complaint notification.** We further support the removal of the requirements throughout Article 3 to inform consumers that they can file a complaint with the Agency and the Attorney General.

Article 9 – Cybersecurity Audits

- **Executive oversight.** Auto Innovators supports the removal of the requirements for Board members, governing body members, or highest-ranking executives to sign statements (section 7122 (i)) and written certifications (section 7124 (c)) regarding cybersecurity audits. We also support the revision of the reporting requirement for auditors to include a member of an entity’s executive management without direct responsibility for its cybersecurity program instead of a Board member (section 7122 (a)(3)).
- **Cybersecurity program components.** While the removal of language requiring cybersecurity audits to document and explain why cybersecurity program components are not necessary (section 7123 (b)(2)) is welcome, Auto Innovators reiterates its recommendation to strike the list of components now included in section 7123 (c). Even though the proposed regulations only direct cybersecurity audits to assess these components “if applicable,” this still does not constitute a risk-based approach to cybersecurity that allows businesses to appropriately tailor audits to the size and complexity of their operations, the nature and scope of processing activities, and customer expectations.
- **Reasonable conformance with international standards.** Section 7123 (f) provides that businesses can use cybersecurity audits, assessments, or evaluations prepared for another purpose, if they meet the requirements in Article 9. This section cites audits that use the National Institute of Standards and Technology Cybersecurity Framework 2.0 as an example. The Framework and other standards (*e.g.*, International Organization for Standardization/International Electrotechnical Commission 27001 standard for information security management systems) are internationally recognized best practices. The Agency should consider reasonable conformance with such standards and frameworks as compliance with the requirements in Article 9, not simply examples that businesses can follow.
- **Substitute cybersecurity audit documentation.** The revisions to section 7124 do not include language to permit businesses that engage in alternative cybersecurity audits, assessments, or evaluations that meet the requirements of Article 9 to submit substitute documentation in lieu of

certifications of completion. Auto Innovators maintains that the Agency should allow for substitute documentation, with recognition of their validity period, to reduce the regulatory burden on affected entities.

- **Affirmative defense.** CCPA provides private rights of action for consumers when certain types of personal information are “subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’ violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information” (see California Civil Code section 1798.150 (a)(1)). Auto Innovators asserts that compliance with the Article 9 requirements meets the definition of “reasonable security procedures and practices;” the Agency should include language that compliance with the Article constitutes an affirmative defense to any claims alleging violations of section 1798.150 (a)(1).

Article 10 – Risk Assessments

- **Threshold for conducting a risk assessment.** We support the Agency’s proposal to modify sections 7150 (3)(A) and (3)(B) through the deletion of provisions relating to “significant decisions” and “extensive profiling.” As we noted in our initial comments, the CCPA provides clear direction regarding the Agency’s regulatory authority with respect to automated decisionmaking technology (ADMT). The statute specifies the issuance of regulations “governing access and opt-out rights with respect to businesses’ use of automated decisionmaking technology.” There is no mention of including ADMT in risk assessments.
- **Sensitive locations.** The modified proposed rules add the concept of “sensitive location,” which would be defined as “any of the following places: healthcare facilities including hospitals, doctors’ offices, urgent care facilities, and community health clinics; pharmacies; domestic violence shelters; food pantries; housing/emergency shelters; educational institutions; political party offices; legal services offices; union offices; and places of worship.” Section 7150 adds a requirement to complete a risk assessment before “profiling a consumer based upon their presence in a sensitive location.” We understand the Agency’s desire to consider heightened protections and analysis for activities that may be associated with these locations. We request that the Agency specify that this list is exhaustive.
- **Stakeholder involvement.** We appreciate the added flexibility regarding stakeholder involvement in the risk assessment process.
- **Timing and retention requirements.** We appreciate the additional clarity regarding the timing for submitting an initial risk assessment, the timing for submitting an updated risk assessment following a material change, what constitutes a material change, and the required retention period for risk assessment documentation.
- **Submission of risk assessments.** We support the Agency’s proposed modifications to the submission requirements in section 7157. We raised concerns in our previous comments about risks relating to the disclosure of confidential business information in unabridged risk assessments. Such a requirement would have also added significant compliance costs to the risk

assessment process to create different versions of the same information. We are therefore appreciative of the Agency's proposal to remove this requirement. Lastly, we support the Agency's proposal to streamline requirements relating to risk assessment review and certification. We are confident that the revised proposal would ensure rigorous internal review and accountability.

Article 11 – Automated Decisionmaking Technology

- **Exempt ADMT use in motor vehicles.** While the Agency has narrowed the scope of the provisions in Article 11, they remain over-broad and overly prescriptive, potentially capturing the use of ADMT in motor vehicles. Modern vehicles use ADMT for driver support and crash mitigation functions, and therefore, allowing consumers to disable or reduce the effectiveness of such functions could negatively impact vehicle safety. The National Highway Traffic Safety Administration remains the appropriate authority to regulate vehicles and vehicle systems that use ADMT as it currently establishes, monitors, and enforces vehicle safety regulations. The Agency should specify that the requirements in Article 11 do not apply to the use of ADMT in motor vehicles.
- **Extend compliance deadline.** The proposed January 1, 2027, compliance deadline for businesses that use ADMT for significant decisions prior to that date (section 7200 (b)) is not feasible. ADMT is a developing and evolving technology, and the Agency should provide ample time for affected entities to comply with any regulatory requirements. Auto Innovators requests that the Agency postpone the compliance date by at least one year to January 1, 2028.
- **Revise pre-use notice requirements.** The Agency proposes modifications that allow businesses to provide pre-use notices in notices of collection in section 7220 (a). However, revisions to sections 7220 (b)(2) and (c)(1) require pre-use notices to include language regarding when businesses plan to process personal information using ADMT and the specific purpose for which businesses plan to use ADMT, respectively. These are overly broad requirements, and the Agency should remove them.
- **Expand pre-use notice exemptions.** The Agency's modifications in section 7220 remove the requirement to provide logic used in ADMT and add language that exempts businesses from having to provide trade secrets and certain other information in pre-use notices. These changes help prevent the disclosure of proprietary information, but they do not go far enough. Auto Innovators recommends that the Agency revise section 7220 (d) to exempt all intellectual property and confidential business information from inclusion in pre-use notices.
- **Remove requirements for human reviewers.** The Agency outlines what businesses must do to qualify for the human appeal exception, including the designation of human reviewers that can review and analyze ADMT outputs, know how to interpret and use ADMT outputs, and have the authority to change related decisions. These requirements are overly restrictive and infringe on the operational prerogatives of affected businesses. Auto Innovators recommends the removal of these requirements.

- **Add exceptions for opt-out rights.** The Agency makes several revisions to the exceptions for businesses regarding the provision of opt-out rights to consumers. Auto Innovators repeats its assertion that such exceptions should include situations where businesses aggregate and de-identify personal information once it is provided for automated decisionmaking. If such information cannot be reasonably associated or linked, directly or indirectly, with a specific consumer or household, it should qualify as an exception to the opt-out requirement. In addition, Auto Innovators suggests that the Agency includes other exceptions similar to those available to personal information deletion rights in California Civil Code §1798.105 (d).
- **Limit access rights to personally identifiable information.** The Agency should limit ADMT access rights to accessing personally identifiable information only. If the affected entity does not store the information in a manner that can be reasonably associated or linked, directly or indirectly, with a particular consumer or household, then it should not be subject to an access request. Such a change would ensure consistency with the right to access information in California Civil Code section 1798.110, as well as general exceptions under sections 1798.145 (j)(1) and (j)(3).
- **Remove logic information requirement in ADMT access rights.** The Agency revises section 7222 to require businesses to provide information about ADMT logic when responding to a consumer access request. Such a requirement could result in the disclosure of intellectual property or confidential business information. Same as the recommendation regarding exemptions for pre-use notices, Auto Innovators urges the Agency to exempt all intellectual property and confidential business information from inclusion in responses to access requests in section 7222 (c).

Auto Innovators appreciates the opportunity to provide additional input on the Agency's proposed regulations and looks forward to further engagement on this regulatory matter.

Sincerely,

[REDACTED]
Tara Hairston
Senior Director, Technology Policy

Grenda, Rianna@CPPA

From: Jake Snow <jsnow@aclunc.org>
Sent: Monday, June 2, 2025 4:11 PM
To: Regulations@CPPA
Cc: David Trujillo; Lee Tien; Hayley Tsukayama; Kara Williams; Emory Roane Contact; Ben Winters; Angel Lin
Subject: Comments on Proposed Risk Assessments and Automated Decisionmaking Technology Regulations
Attachments: 2025-06-02 CPPA ADMT Comments FINAL.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,

Attached are comments on the CPPA's Proposed Regulations relating to Risk Assessments and Automated Decisionmaking Technology. These comments are submitted on behalf of ACLU California Action, Consumer Federation of America, the Electronic Frontier Foundation, the Electronic Privacy Information Center, The Greenlining Institute, and Privacy Rights Clearinghouse.

Best regards,

Jake Snow
Senior Staff Attorney
Technology and Civil Liberties Program
ACLU of Northern California
he/him/his | (415) 293-6325 | @snowjake



June 2, 2025

California Privacy Protection Agency
2101 Arena Boulevard
Sacramento, CA 95834

Re: Comments on Proposed Risk Assessments and Automated Decisionmaking Technology Regulations

Sent via email to regulations@coppa.ca.gov

Dear Board Members, Executive Director, and Agency Staff,

We write in response to the California Privacy Protection Agency's ("CPPA" or "the Agency") request for comment on the Agency's proposed Risk Assessment and Automated Decisionmaking Technology ("ADMT") Regulations ("Proposed Regulations") under the California Consumer Protection Act ("CCPA").

The revised draft regulations released on May 9, 2025 represent significant concessions by the Agency and its board to a campaign of industry pressure. In November of 2020, Californians voted for a privacy law that promised to put in place regulations that would give them meaningful rights to control how their personal information was used, including in automated and algorithmic systems. With the most recent draft regulations, the Agency is poised to deprive Californians of the benefit of one of the most important provisions of the state's privacy law. We urge the Agency to reverse course.

In this letter, we address three key changes to the draft regulations: First, the narrowed definition of ADMT. Second, the removal of "criminal justice" related decisions from the definition of "significant decision." And third, the removal of the prohibition on processing personal information when the risks outweigh the benefits.

The Narrowed Definition of ADMT Threatens to Undermine the Core Purpose of the CCPA’s ADMT Regulations

In our February comments we emphasized the importance of preserving a definition of “Automated Decisionmaking Technology” that protected people against the harm that ADMTs were causing today.¹ Our concern with the previous draft was that it was limited to algorithmic systems that “execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking.”² As we explained in those comments, companies will have a strong incentive to characterize their systems as providing only one input of many to a human—thus making it arguably not a “key factor” in the decision—but nevertheless create implicit policies that make clear to the human decision-makers that the automated factor is the one to be trusted.³

The changes made in the most recent draft go even farther than allowing companies to self-certify that they should not be subject to regulation: it explicitly carves out ADMTs where a human has even glancing involvement in making the decision. Under this new narrower standard, many more consumers will be denied the notice and opt-out protections they need and deserve. The definition of ADMT, which by statute must include instances where people’s behavior and performance at work are predicted⁴, therefore falls short of that proper scope.

Cutting “Criminal Justice” from the Definition of “Significant Decision” Will Harm the Most Vulnerable Californians.

The revised draft regulations also eliminate “criminal justice” from the definition of a “significant decision.”⁵ In our February 2025 comments, we highlighted that the inclusion of “criminal justice” should be expanded to include a variety of decisions that are among the most impactful that a government can make on a person’s life. These include algorithmically driven pretrial risk assessments and sentencing and parole decisions, among others. Our letter recommended including the following detailed definition of significant decisions in the “criminal justice” area.

¹ Coalition Comments on Proposed Risk Assessments and Automated Decisionmaking Technology Regulations, February 19, 2025, pp. 5-6, <https://www.aclunc.org/sites/default/files/2025-02-19%20ACLU%20CA%20Action%20EPIC%20EFF%20CFA%20PRC%20CPPA%20Comments.pdf>.

² *Id.*

³ *Id.* at 6.

⁴ Civil Code § 1798.185(a)(16).

⁵ Compare CA PRIVACY PROTECTION AGENCY – MODIFIED TEXT OF PROPOSED REGULATIONS, May 9, 2025, Section 7150(b)(3) (cutting entire definition of “significant decision” that includes “criminal justice (e.g., posting of bail bonds).”) with Section 7001(ddd) (new definition of “significant decision” that does not mention decisions that arise in the criminal justice system, or that impact a person’s physical liberty.).

https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_mod_txt_pro_reg.pdf

1. Risk assessments for pretrial decisionmaking, including, but not limited to, decisions related to pretrial detention, release on one's own recognizance, the granting or setting of monetary bail, and the conditions of pretrial release;
2. Sentencing;
3. Parole;
4. Probation and any other form of supervised release;
5. Deployment of law enforcement resources;
6. Decisions related to conditions of confinement, including, but not limited to, housing, classification, and programming.

The elimination of criminal justice from the definition of “significant decision” opens the door to a panoply of tech-mediated cruelty by the criminal legal system, from keeping people incarcerated to swarming already overpoliced neighborhoods with more officers. The CCPA’s promise was to give people *meaningful control* over how their information was used. That meaningful control is not realized through the ministerial management of records in a database. It requires that systems that operate through the processing of people’s personal information be modified to ensure that the people have some measure of power over how those systems impact their liberty, their communities, and their lives. Cutting the definition of “significant decision” to eliminate decisions that are part of the criminal legal system deprives some of the most vulnerable Californians of autonomy and privacy when they need it most.

The Regulations Should Direct That Processing Where the Risks Outweigh the Benefits Are Restricted or Prohibited.

Risk assessments are required by the CCPA for a simple reason: when the risks to privacy of processing of consumers’ personal information outweigh the benefits, the processing should be restricted or prohibited outright. As the statute makes explicit, risk assessments weigh the risks “with the goal of *restricting or prohibiting such processing* if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public.”⁶

The CCPA requires, and Californians are entitled to expect, that risk assessments include the company’s actual weighing of risks and benefits, and that the regulatory “goal” is “restricting or prohibiting” such processing if the specified risks outweigh the benefits.⁷ It is not enough to simply list various risks and benefits and assert that the risks are outweighed.

⁶ Civil Code § 1798.185(a)(15)(B) (emphasis added).

⁷ *Id.*

The November 2024 draft regulations included an explicit prohibition on processing personal information when the specified risks outweigh the benefits, but that language was removed in the most recent draft.⁸ Instead of prohibiting the processing, the regulations merely recite the language of the statute regarding the goal of the regulations. This is inadequate.

Imagine a processing activity that risks significant harm to vulnerable consumers—like people searching for housing or employment—but which is marginally profitable for a business. When a business self-certifies that the processing’s benefits outweigh the costs, it is the Agency’s role under the statute to review that certification and the supporting analysis and determine *independently* whether the business has, under the law, properly performed the cost-benefit analysis. If the business’s assessment is inconsistent with the law, then the processing, in the language of the statute, must be restricted or prohibited.

We urge the Agency to take the steps recommended in these comments to ensure that consumers' privacy rights are protected.

Sincerely,

Jacob Snow
Senior Staff Attorney
ACLU of Northern California

David Trujillo
Executive Director
ACLU California Action

Ben Winters
Director of AI and Data Privacy
Consumer Federation of America

Emory Roane
Associate Director of Policy
Privacy Rights Clearinghouse

Angel Lin
Tech Equity Policy Fellow
The Greenlining Institute

Lee Tien
Legislative Director and Adams Chair
for Internet Rights
Electronic Frontier Foundation

Sara Geoghegan
EPIC Senior Counsel
Electronic Privacy Information Center

⁸ May 9, 2025 Draft Regulations, § 7154 (showing changes from previous draft striking language requiring that the “business *must not process personal information* for any processing activity” if the risks outweigh the benefits.”).

Grenda, Rianna@CPPA

From: Annette Bernhardt <[REDACTED]@com>
Sent: Monday, June 2, 2025 3:09 PM
To: Regulations@CPPA
Cc: Annette Bernhardt
Subject: Group Comment on Proposed Risk Assessment and ADMT Regulations
Attachments: June 2nd CPPA comment letter.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](#)

Greetings,

Attached please find our group letter responding to the CPPA's May 9, 2025 request for public comment, signed by 52 unions, privacy, and civil rights organizations and individuals.

Best,
Annette Bernhardt

June 2, 2025

California Privacy Protection Agency
2101 Arena Boulevard
Sacramento, CA 95834

Dear Executive Director Kemp, Agency Staff, and Board Members,

The signed organizations and individuals write to respond to the California Privacy Protection Agency's May 9, 2025, request for comments on the most recent draft of proposed regulations for the California Consumer Privacy Act (CCPA). We want to acknowledge the hard work of Agency leadership, staff, and board members on these regulations in a difficult and fast-changing policy environment at both the state and federal level.

That said, we are deeply disappointed at the substantial weakening of the proposed regulations – and at the lack of responsiveness to our coalition of labor and civil society groups, which represent hundreds of thousands of workers and consumers. Our organizations have invested significant time over the past two years analyzing draft regulations, gathering evidence from workers and consumers, summarizing academic research, writing responses, and giving public comments at board meetings, all with limited resources.

None of the recommendations in our January 9, 2025, letter were adopted. The principles we articulated in our February 26, 2024, letter are absent from this current draft. Instead, each iteration of the proposed regulations has conceded more and more to concerns of the business community and the tech sector. And the most recent draft, after what we understand to be an intense campaign to influence the direction of the regulations, does the most damage to workers' and consumers' rights.

As a result, it is our assessment that the current proposed ADMT (automated decisionmaking technology) and Risk Assessment regulations do not provide the protections that consumers and workers deserve under the CCPA and that the law itself clearly intended.

This is a profound lost opportunity, especially for workers. The emergence of data-driven technologies represents one of the most important issues that will shape the future of work in California for decades to come, affecting workers' privacy, wages and working conditions, race and gender equity, right to organize, and autonomy and dignity. By fully covering worker data and workplace technologies in the CCPA regulations, California could give workers a voice over their future. We strongly urge Executive Director Kemp, Agency staff, and board members to reconsider the current trajectory of the proposed regulations.

In what follows, we briefly lift up the main shortcomings of the revised proposed regulations. We do not duplicate here the recommendations and cited research provided in our January 9, 2025, letter, all of which remain fully relevant.

1. Definitional changes leave large swaths of workers and consumers unprotected by the proposed regulations.

The revised definitions of ADMTs and “significant decision” narrow the scope of regulation to such a degree as to render them meaningless to many Californians.

For workers in particular, the narrowing of scope to only automating uses of ADMT creates a large opening for companies to side-step the accountability that the CPPA was charged to develop through its regulations. Essentially, an employer can self-certify itself out of coverage under the CCPA by simply deciding that a given automated system does not “replace” or “substantially replace” human decisionmaking. Given the current definition, even a modicum of human involvement would put the use of an ADMT out of regulatory scope. Meanwhile, the employer could be drawing on the system to make highly consequential decisions regarding the terms and conditions of employment for its workers. But because under the proposed regulations, no one needs to be alerted that the employer is using the tool at all, neither workers nor the Agency would be able to challenge the company’s unilateral assessment of the automated system’s role in its decision-making process.

In short, the extreme narrowing of the ADMT definition creates a self-regulation regime for employers hoping to escape oversight. To be clear, this was already a problem in earlier drafts of the proposed regulations. With this latest narrowing, workers are effectively dropped from protection by any ADMT provisions in the proposed regulations.

Also detrimental are the changes to the definition of “significant decision.” For example, employer decisions about the “allocation or assignment of work” for independent contractors will no longer be covered, even as misclassified independent contractors are subject to constant data collection and algorithmic management (like robo-firings) by gig platforms. The use of worker data to train ADMTs will also no longer be covered by the proposed ADMT regulations, even as this is one of the main scenarios where workplace technology products can have significant negative impacts on workers (such as deskilling and job loss). Finally, the specific use of physical or biological identification or profiling to make significant decisions is also no longer covered under the ADMT regulations, even as these often error- and bias-prone systems are increasingly marketed for workplace applications.

At the May 1, 2025, meeting of the CPPA board, Agency staff provided preliminary economic updates based upon the modified regulations. In particular, staff estimated that as a result of the narrowing of the above two definitions, only 10% of firms covered by the CCPA would be subject to the ADMT regulations. Note that this means even fewer than 10% of the firms’ workers would be protected by the ADMT regulations, since not all workers at a given firm are likely to be subject to all ADMTs in use at the firm. This assessment also demonstrates that the agency views the revised regulations as substantially narrowing the scope of the proposed regulations.

2. The revised notice and data access regime will not work for workers and consumers.

One of the hallmarks of the CCPA is that it recognizes the importance of transparency and disclosure in order for consumers and workers to make informed decisions about their data privacy. But currently, the biggest obstacle to ensuring responsible use of data-driven technologies in the workplace is that they are largely hidden from both policymakers and workers.

Especially in the workplace, achieving transparency and disclosure requires both pre-use notice and use-notice. Workers need to know which data collection and ADMT systems are being used in the workplace, *and they need to know when one of those systems has actually been used to make a significant decision about them*. Without the latter use-notice, a fast food worker, for example, won't know that an algorithm was used to fire them – and without that knowledge, they won't be able to exercise their right to access data about that decision.

Unfortunately, the revised regulations delete the use-notice requirement when an ADMT was used to make an adverse decision – in the case of workers, having their compensation decreased or being suspended, demoted, or terminated.

Essentially, it means that a worker or consumer must somehow magically divine that an adverse decision was made about them using an ADMT, in order to know that they should request details about that use. This is a critical loss in the proposed regulations, since data access is the first step in Californians' ability to identify and challenge errors and unfair treatment. And even if a worker does request more information about a firing decision, for example, the current ADMT regulations no longer require the employer to share the actual output that was used in making that decision – rendering the ADMT access provisions a hollow promise.

3. The revised ADMT opt-out provisions have become even more inaccessible to workers.

In our January 9, 2025, letter, we explained in detail how the draft regulations at that time effectively eliminated the ability of workers to protect themselves by opting out of consequential ADMT systems because a series of broad exemptions would allow employers to easily escape coverage. Revisions in the current regulations only serve to further exacerbate the problem by removing the few barriers that existed to employers claiming the exemptions.

As a result, an employer can simply pronounce that it is using a given ADMT solely for work allocation and assignment or compensation and that the ADMT does not discriminate. It is hard to imagine scenarios where an employer would not avail itself of this exemption. (Previously, the employer was required to first conduct an evaluation of the ADMT and to implement accuracy and nondiscrimination safeguards).

4. The Risk Assessment requirements have become weak tools for identifying and addressing ADMT harms.

Early drafts of the proposed regulations began to lay out an important set of procedures for providing notice of risk assessments of data collection and ADMT systems. In the workplace context, conducting risk assessments prior to implementation has the potential to be a critical tool to ensure transparency and identify negative impacts; it is not fair to workers to wait until invasions of privacy and other harms have already occurred to begin regulatory oversight. That is why in our January 9, 2025, letter, we laid out a set of recommended improvements to ensure full transparency and accountability to workers in the employers' use of these systems.

Instead, the current revised regulations only serve to dilute the utility of risk assessments. For example, the ADMT risk assessment provisions no longer require businesses to: document whether they evaluated a given ADMT to ensure it works and does not discriminate; disclose the criteria they used to identify negative impacts to consumer privacy; and identify how their safeguards address any negative impacts identified in the risk assessment. Moreover, businesses no longer have to submit an abridged version of the risk assessment to the Agency. And perhaps most important, a critical provision in previous drafts, stating that businesses must not process personal information for use by an ADMT if the risks to consumers' privacy outweigh the benefits, was eliminated.

5. In sum, the revised regulations fail to meet the spirit and substance of the rulemaking charge that was given to the CCPA by voters, particularly in the area of automated decisionmaking technology.

In passing Prop 24 and in survey after survey, Californians have been very clear that they want the collection and use of their personal information fully protected—and that includes future-proofing the CCPA by developing regulations around cybersecurity, harm identification and mitigation, and algorithmic systems. What's at stake are highly consequential decisions impacting access and equity in our communities and our workplaces.

In our assessment, however, the current draft of the regulations falls short of the intent of voters and the directives of the CCPA itself. For example, the law requires, and Californians are entitled to expect, that risk assessments include the company's actual weighing of risks and benefits, and that the regulatory "goal" is "restricting or prohibiting" such processing if the specified risks outweigh the benefits. It is not enough to simply list various risks and benefits and assert that the risks are outweighed. Further, the definition of ADMT, which by statute must include instances where people's behavior and performance at work are predicted, falls short of that proper scope. ADMTs are one of the main ways that businesses use consumer and worker data, and so the numerous deletions and weakening of ADMT provisions in the revised regulations are especially harmful.

More generally, we do not believe that the draft regulations currently meet the broad goals of the CCPA, which are to ensure that consumers and workers have the information necessary "to exercise meaningful control" of businesses' use of their data and have "meaningful options" over how that data is collected, used, and disclosed.

At a moment when we are witnessing a multi-front assault on the very idea that civil society has the right to govern new technologies, California should model the development of regulations that support the development and deployment of responsible AI for consumers and workers. The CCPA should complete its rulemaking by issuing rules that can form the foundation for an innovative, safe, and equitable future, free from undue influence and fully responding to the charge given by voters.

Sincerely,
The signed organizations and individuals

Organizations:

American Civil Liberties Union California Action
American Federation of Musicians Local 7

Athena Coalition
AWU - CWA Local 9009
California Employment Lawyers Association
California Federation of Labor Unions, AFL-CIO
California Immigrant Policy Center
California Nurses Association
California Teachers Association
Center for Inclusive Change
Communications Workers of America Union (CWA)
Communications Workers of America District 9
Consumer Federation of California
Data & Society
Economic Security California Action
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Gig Workers Rising
International Cinematographers Guild, Local 600 IATSE
Los Angeles Alliance for a New Economy (LAANE)
Media Alliance
National Domestic Workers Alliance
National Employment Law Project
National Union of Healthcare Workers
San Francisco Labor Council
SEIU California
Surveillance Technology Oversight Project
Teamsters California
Tech Oversight California
TechEquity Action
TechTonic Justice
The Collaborative Research Center for Resilience
UC Berkeley Labor Center
UDW/AFSCME Local 3930
UFCW Western States Council
United for Respect
Upturn
Warehouse Worker Resource Center
Working Partnerships USA
Worksafe
Writers Guild of America West

Individuals (affiliations listed for identification purposes only):

Rosemary Batt (Cornell University)
Chris Benner (University of California, Santa Cruz)
Kate Bronfenbrenner (Cornell ILR Global Labor and Work)
Ileen DeVault (Cornell University)

Veena Dubal (University of California, Irvine)

Sayuri Falconer (UCSF)

Shannon Gleeson (Cornell University School of Individual and Labor Relations and Brooks School of Public Policy)

Adam Seth Litwin (Cornell University)

Seema N. Patel (UC College of the Law San Francisco (UC Law SF) [formerly UC Hastings])

Dan Raile (The Worker Agency)

Chris Tilly (University of California Los Angeles)

Grenda, Rianna@CPPA

From: Tasia Kieffer <tasia.kieffer@bizfed.org>
Sent: Monday, June 2, 2025 3:09 PM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: CPPA BIZFED PUBLIC COMMENT 6.2.docx

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,

On behalf of the Los Angeles County Business Federation (BizFed LA), I am attaching our formal public comment statement regarding ADMT draft rules. Please see attached.

If you have any questions, please let me know.

Thank you!



Tasia Kieffer, Advocacy Manager
(213) 316-8775 - tasia.kieffer@bizfed.org
Instagram: [tasia_kieffer](#)
Los Angeles County Business Federation

Sign up now for BizFed LA & BizFed Central Valley's [Sacramento Days](#) June 10th & 11th "Affordability First" – Advocacy that Works!

June 2, 2025

California Privacy Protection Agency
ATTN: PRA Coordinator
400 R Street
Suite 330
Sacramento, CA 95811

RE: Public Comment in Opposition to Revised ADMT Regulations

To the Board Members of the California Privacy Protection Agency:

On behalf of the Los Angeles County Business Federation (BizFed LA), a grassroots alliance of over 240 business organizations that collectively represent more than 420,000 employers with 5 million employees in Southern California, we write to express our continued opposition to the revised draft of the CPPA's proposed regulations concerning Automated Decisionmaking Technology (ADMT).

While we appreciate that the May 2025 draft includes certain improvements, such as delaying implementation and reducing some disclosure burdens, critical concerns remain that render the draft untenable in its current form. The revised regulations still pose significant operational, financial, and legal challenges to California businesses and exceed the statutory authority granted under the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).

We respectfully urge the CPPA to either significantly amend the draft regulations or restart the rulemaking process altogether. Specifically, we recommend the following changes:

1. Remove All References to ADMT Training

The CPPA lacks the statutory authority to regulate the *training* of ADMT models. The statute allows rulemaking only concerning the *use* of automated decisionmaking technology to process personal information. As multiple commenters, including Governor Gavin Newsom, have emphasized, training does not constitute a "use" of ADMT, because it does not result in a decision affecting any particular consumer. The inclusion of ADMT training in the regulatory scope is therefore an overreach and must be eliminated to ensure legal compliance and regulatory clarity.

2. Limit the Definition of ADMT to "Solely Automated" Decisions

The current language continues to exceed statutory limits by regulating tools that merely "substantially replace" human decisionmaking. This fails to respect the statutory mandate, which limits regulation to *fully automated* systems that independently process personal data. If a human is involved in the decision, the process is not, by definition, automated. We urge the CPPA to revise the language

to align with the statute and limit its scope to technologies that result in *solely automated* decisions.

3. Remove Requirements for Highly Technical Notices

The draft's explainability requirements are unreasonable and disconnected from the statutory privacy framework. Requiring businesses to provide detailed explanations about "parameters that generated the output" of an ADMT system—which can involve trillions of variables—is both infeasible and unhelpful to consumers. Instead of offering meaningful transparency, such mandates create confusion and compliance burdens while providing no measurable privacy benefit. We urge the CPPA to refocus disclosures on actionable privacy protections and eliminate overly technical notice requirements.

4. Eliminate Duplicative Profiling Risk Assessments

The regulations improperly introduce a separate risk assessment requirement for "physical or biological identification or profiling," which substantially overlaps with existing requirements for biometric data under the CPRA. This duplication increases compliance costs and creates confusion without enhancing consumer privacy. Businesses already conducting risk assessments for sensitive biometric information should not be subjected to redundant obligations.

5. Remove the Unauthorized "Sensitive Location" Category

The proposed inclusion of "sensitive locations" is unsupported by the statute. While the CPRA clearly defines "sensitive personal information," it does not include or authorize the creation of a new category for "sensitive location" data. Expanding regulatory authority in this way violates fundamental principles of administrative law. Any expansion of covered data categories must come from the legislature, not through agency rulemaking.

6. Reinstate the Fraud Exception for Opt-Out Rights

The revised draft removes a previously included and critically important exemption for systems designed to detect fraud, data breaches, or malicious activity. Requiring businesses to offer opt-outs for anti-fraud systems compromises their efficacy and exposes consumers and companies to unnecessary risk. This exception must be reinstated to protect public safety and business integrity.

7. Reassess the Economic Impact

According to the Agency's own estimates, the current regulations will cost California businesses over **\$1.2 billion in the first year alone**. These burdens affect businesses of all sizes and are particularly detrimental to small and mid-sized enterprises. Many of the systems that would fall under this regulation, such as those used for basic workplace productivity tracking or incentive payouts, pose no

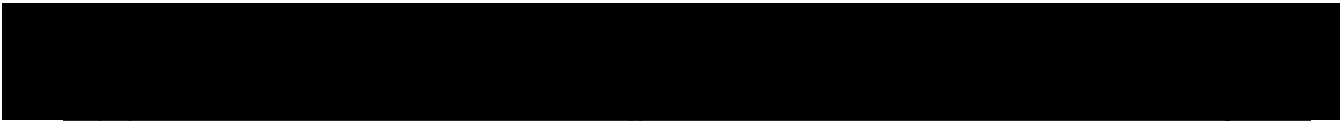
consumer privacy risks and should not be within scope. These excessive and misaligned costs will stifle innovation and economic growth.

Conclusion

The CPPA's current regulatory approach threatens to dramatically expand the scope of its authority beyond legislative intent, impose disproportionate costs, and entangle routine business functions in unnecessary red tape—all without demonstrable privacy benefits to consumers. We strongly recommend that the CPPA substantially revise the proposed regulations or restart the rulemaking process to ensure alignment with statutory authority and practical implementation realities.

We appreciate your attention to these concerns and are available to provide additional feedback or participate in further discussions.

Sincerely,



Angela Gibson-Shaw
BizFed 2025 Chair
GLAAACC

David Fleming
BizFed Founding Chair

Tracy Hernandez
BizFed Founding CEO
IMPOWER, Inc.

David Englin
BizFed President

BizFed Association Members

Action Apartment Association
 Advanced Medical Technology Association
 Alhambra Chamber
 American Beverage Association
 Antelope Valley Chamber formerly Lancaster Chamber of Commerce
 Apartment Association of Greater Los Angeles
 Apartment Association of Orange County
 Apartment Association, CA Southern Cities, Inc .
 Apartment Association of California
 Arcadia Association of Realtors
 AREAA North Los Angeles SFV SCV
 Armenian American Business Association
 Armenian Trade & Labor Association
 Arts District Los Angeles
 ASCM Inland Empire Chapter
 Associated Builders & Contractors SoCal (ABC SoCal)
 Associated General Contractors
 Association of Independent Commercial Producers
 AV Edge California
 Azusa Chamber
 Bell Chamber
 Beverly Hills Chamber
 BioCom
 Black Business Association
 Black Professional Network
 Boyle Heights Chamber of Commerce
 Bridge Compton Org
 Building Industry Association - LA/Ventura Counties
 Building Industry Association of Southern California
 Building Industry Association- Baldyview
 Building Owners & Managers Association of Greater Los Angeles
 Burbank Association of Realtors
 Burbank Chamber of Commerce
 Business and Industry Council for Emergency Planning and Preparedness
 Business Resource Group
 CalAsian Chamber
 CalChamber
 California African American Chamber of Commerce
 California Apartment Association- Los Angeles
 California Asphalt Pavement Association
 California Bankers Association
 California Black Chamber of Commerce
 California Business Properties
 California Business Roundtable
 California Cleaners Association
 California Contract Cities Association
 California Council for Environmental & Economic Balance (CCEEB)
 California Fuels & Convenience Alliance- Formerly California Independent Oil Marketers Association (CIOMA)
 California Gaming Association
 California Grocers Association
 California Hispanic Chamber
 California Hotel & Lodging Association
 California Independent Petroleum Association
 California Infrastructure Delivery Coalition
 California Life Sciences Association
 California Manufacturers & Technology Association
 California Metals Coalition
 California Natural Gas Producers Association
 California Restaurant Association
 California Retailers Association
 California Self Storage Association
 California Small Business Alliance
 California Travel Association (CalTravel)
 California Trucking Association
 Californians For Smarter Sustainability
 Carson Chamber of Commerce
 Carson Dominguez Employers Alliance
 Central City Association
 Century City Chamber of Commerce
 Chatsworth Porter Ranch Chamber of Commerce
 Citrus Valley Association of Realtors
 Civil Justice Association of California CJAC

Claremont Chamber of Commerce
 Commerce Business Council formerly Commercial Industrial Council/Chamber of Commerce
 Compton Chamber of Commerce
 Compton Community Development Corporation
 Compton Entertainment Chamber of Commerce
 Construction Industry Air Quality Coalition
 Construction Industry Coalition on Water Quality
 Council of Infill Builders
 Crenshaw Chamber of Commerce
 Culver City Chamber of Commerce
 Downey Chamber of Commerce
 Downtown Alliance
 Downtown Long Beach Alliance
 DTLA Chamber of Commerce
 El Monte/South El Monte Chamber
 El Salvador Corridor Association
 El Segundo Chamber of Commerce
 Employers Group
 Energy Independence Now EIN
 Engineering Contractor's Association
 EXP The Opportunity Engine
 FastLink DTLA
 Filipino American Chamber of Commerce
 Friends of Hollywood Central Park
 FuturePorts
 Gardena Valley Chamber
 Gateway to LA
 Glendale Association of Realtors
 Glendale Chamber
 Glendora Chamber
 Greater Antelope Valley AOR
 Greater Bakersfield Chamber of Commerce
 Greater Coachella Valley Chamber of Commerce
 Greater Downey Association of REALTORS
 Greater Lakewood Chamber of Commerce
 Greater Leimert Park Crenshaw Corridor BID
 Greater Los Angeles African American Chamber
 Greater Los Angeles Association of Realtors
 Greater Los Angeles New Car Dealers Association
 Greater San Fernando Valley Chamber
 Harbor Association of Industry and Commerce
 Harbor Trucking Association
 Historic Core BID of Downtown Los Angeles
 Hollywood Chamber
 Hospital Association of Southern California
 Hotel Association of Los Angeles
 ICBWA- International Cannabis Women Business Association
 Independent Cities Association
 Independent Hospitality Coalition
 Industrial Environmental Association
 Industry Business Council
 Inglewood Board of Realtors
 Inland Empire Economic Partnership
 Irwindale Chamber of Commerce
 Kombucha Brewers International
 La Cañada Flintridge Chamber
 LA County Medical Association
 LA Fashion District BID
 LA South Chamber of Commerce
 Larchmont Boulevard Association
 Latin Business Association
 Latino Food Industry Association
 Latino Golfers Association
 Latino Restaurant Association
 LAX Coastal Area Chamber
 Licensed Adult Residential Care Association- LARCA
 Long Beach Area Chamber
 Long Beach Economic Partnership
 Long Beach Major Arts Consortium
 Los Angeles Area Chamber
 Los Angeles Economic Development Center
 Los Angeles Gateway Chamber of Commerce
 Los Angeles Latino Chamber
 Los Angeles LGBTQ Chamber of Commerce
 Los Angeles Parking Association
 Los Angeles Regional Food Bank
 MADIA Tech Launch
 Malibu Chamber of Commerce

Manhattan Beach Chamber of Commerce
 Manhattan Beach Downtown Business & Professional Association
 Marina Del Rey Lessees Association
 Marketplace Industry Association
 Monrovia Chamber
 Motion Picture Association of America, Inc.
 MoveLA
 MultiCultural Business Alliance
 NAIOP Southern California Chapter
 NAREIT
 National Association of Minority Contractors
 National Association of Theatre Owners CA/ Nevada
 National Association of Women Business Owners
 National Association of Women Business Owners - LA
 National Association of Women Business Owners- California
 National Federation of Independent Business Owners California
 National Hookah
 National Latina Business Women's Association
 Norwegian American Chamber of Commerce
 Ofiso Community Foundation
 Orange County Business Council
 Orange County Hispanic Chamber of Commerce
 Pacific Merchant Shipping Association
 Panorama City Chamber of Commerce
 Paramount Chamber of Commerce
 Pasadena Chamber
 Pasadena Foothills Association of Realtors
 PGA
 Pharmaceutical Care Management Association PhRMA
 Pico Rivera Chamber of Commerce
 Pomona Chamber
 Rancho Southeast REALTORS
 ReadyNation California
 Recording Industry Association of America
 Regional CAL Black Chamber, SVF
 Regional Hispanic Chambers
 San Gabriel Valley Economic Partnership
 San Pedro Peninsula Chamber of Commerce
 Santa Clarita Valley Chamber
 Santa Clarita Valley Economic Development Corp.
 Santa Monica Chamber of Commerce
 Secure Water Alliance
 Sherman Oaks Chamber
 Signal Hill Chamber
 South Bay Association of Chambers
 South Bay Association of Realtors
 South Gate Chamber of Commerce
 Southern California Contractors Association
 Southern California Golf Association
 Southern California Grantmakers
 Southern California KFC Franchise
 Southern California Leadership Council
 Southern California Minority Suppliers Development Council Inc.
 Southern California Water Coalition
 Southland Regional Association of Realtors
 Specialty Equipment Market Association
 Structural Engineers Association of Southern California
 Sunland/Tujunga Chamber
 Sunset Strip Business Improvement District
 Swiss American Chamber of Commerce
 Thai American Chamber of Commerce
 The Bridge Network
 The LA Coalition for the Economy & Jobs
 The Los Angeles Taxpayers Association
 The Two Hundred for Homeownership
 Torrance Area Chamber
 Tri-Counties Association of Realtors
 United Chambers – San Fernando Valley & Region
 United Contractors
 United States-Mexico Chamber
 Unmanned Autonomous Vehicle Systems Association
 Urban Business Council
 US Green Building Council
 US Resiliency Council

Valley Economic Alliance, The
Valley Industry & Commerce Association
Venice Chamber of Commerce
Vermont Stlauson Economic Development
Corporation
Veterans in Business
Vietnamese American Chamber
Village of Sherman Oaks BID
Warner Center Association
West Covina Chamber
West Hollywood Chamber
West Hollywood Design District
West Los Angeles Chamber
West San Gabriel Valley Association of Realtors
West Valley/Warner Center Chamber
Westchester BID
Western Electrical Contractors Association
Western Manufactured Housing Association
Western Propane Gas Association
Western States Petroleum Association
Westside Council of Chambers
Westwood Community Council
Whittier Chamber of Commerce
Wilmington Chamber
World Trade Center
Yes in My Backyard
7-Eleven Franchise Owners Association of
Southern California

Grenda, Rianna@CPPA

From: Matthew Powers <mpowers@aclhic.com>
Sent: Monday, June 2, 2025 2:26 PM
To: Regulations@CPPA
Cc: John Shirikian; John W. Mangan; Sarah Wood
Subject: ACLI, ACLHIC & IRI Comments on CPPA's Modified Draft Regulations
Attachments: ACLI, ACLHIC and IRI Comments on 5.9.25 CPPA Rulemaking Proposal (Final).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,

On behalf of the American Council of Life Insurers (ACLI), the Association of California Life and Health Insurance Companies (ACLHIC), and the Insured Retirement Institute (IRI), please find attached our joint comment letter in response to the California Privacy Protection Agency's 15-day modification of proposed regulations, as noticed on May 9, 2025.

We appreciate your time and consideration of our comments, and we welcome the opportunity to continue engaging with the Agency on this important process.

Best regards,
Matt

Matthew Powers
ACLHIC
P: 916-442-3648
www.aclhic.com



June 2, 2025

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

Email: regulations@coppa.ca.gov

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

Dear CPPA Board Members and Staff,

The American Council of Life Insurers (ACLI), the Association of California Life and Health Insurance Companies (ACLHIC), and the Insured Retirement Institute (IRI) submit this comment letter in response to the California Privacy Protection Agency's 15-day modification of proposed regulations, as noticed on May 9, 2025. We appreciate the opportunity to provide additional feedback.

As stated in our January 14, 2025, joint letter, we are aligned with the broader business community in our overarching concerns with the Agency's proposed rulemaking. While we appreciate the significant revisions the Agency has made to the regulatory text—particularly the removal of references to artificial intelligence and the narrowing of the Automated Decisionmaking Technology (ADMT) provisions—you will continue to hear from many of our counterparts about remaining areas of concern across the broader package. We echo those concerns.

For the purposes of this submission, however, we are focusing solely on the limited revisions made to the section specifically impacting insurers.

Article 12 (Insurance Companies):

We note that the Agency's only substantive change to Article 12 is a revision to an illustrative example under Section 7271(b). While we again appreciate the intent to clarify the boundaries of the CCPA's applicability to insurance data, we are concerned that the example continues to reflect a misunderstanding of the data level exemptions in CIV 1798.145(c), (d)(1), and (e).

Specifically, in illustrative example 7271(b)(3), the revised language describes a scenario in which a consumer ("Sloane") submits personal information as part of a claim for fire damage. The Agency concludes that this information is "used to service the insurance policy" and thus "not subject to the CCPA." We agree with the conclusion but believe the rationale must be more clearly anchored in the CCPA's statutory exemption for Gramm-Leach-Bliley Act (GLBA) data.

In this case, Sloane is a consumer as defined in GLBA, and the personal information submitted in connection with her claim is protected under GLBA. Accordingly, it is categorically exempt from the

CCPA under Civil Code section 1798.145(c)—not merely excluded based on its use in an insurance transaction as defined under IIPPA.

We urge the Agency to update the example to reflect that this exemption flows from the *status of the data* (GLBA-regulated), rather than the *purpose* or *use* of the data. Ambiguity on this point could inadvertently sweep clearly exempt data back into CCPA scope, creating unnecessary compliance confusion.

Therefore we request that illustrative example 7271(b)(3) be revised to read:

(3) Sloane submits personal information to her insurance company as part of a claim for losses incurred by a fire at her home. This information is used to service the insurance policy, and thus subject to the Gramm-Leach-Bliley Act, the California Financial Information Privacy Act, and the Insurance Code and its regulations. This nonpublic personal information is not subject to the CCPA.

In line with this requested clarification, to preserve consistency and avoid any ambiguity between the illustrative examples and Section 7271 (a), we believe that Section 7271(a) should also be revised to read:

(a) Insurance companies that meet the definition of “business” under the CCPA shall comply with the CCPA with regard to any personal information not subject to the Insurance Code and its regulations, or that is otherwise exempt under California Civil Code Section 1798.145. ~~For example, those insurance companies shall comply with the CCPA for personal information that is collected for purposes not in connection with an insurance transaction, as that term is defined in Insurance Code, section 791.02.~~

Current Legislative Efforts

We also want to highlight pending legislation **SB 354 (Limón)**, which seeks to update California’s Insurance Information and Privacy Protection Act (IIPPA). Our organizations are actively engaged with the California Department of Insurance, sponsor of the bill, and with Senator Limón.

If enacted, SB 354 could substantially update how insurers handle personal information in California, likely rendering Article 12 unnecessary or obsolete. Given this active legislative effort, we respectfully recommend that the Agency defer final action on Article 12 until SB 354 is resolved and stakeholders have a clearer understanding of the updated statutory framework.

Thank you for the opportunity to provide these comments. We remain available to engage further as the rulemaking progresses.

Sincerely,

John Mangan, American Council of Life Insurers
Matthew Powers, Association of California Life and Health Insurance Companies
Sarah Wood, Insured Retirement Institute

Cc: California Department of Insurance