

Grenda, Rianna@CPPA

From: Kevin Rodgers <kevinr@car.org>
Sent: Monday, June 2, 2025 11:23 AM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations - REALTORS® Comments
Attachments: CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations - REALTORS® Comments - KR 05.15.25.pdf

This Message Is From an External Sender

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

[Report Suspicious](#)

To whom it may concern,

Thank you for the opportunity to provide comment on the proposed regulations. We appreciate the Board's work on these regulations and hope the attached letter will prove helpful during their development.

We thank you for the opportunity to comment. Please feel free to contact us with any questions you may have.

All the best,

Kevin Rodgers
Regulatory Advocate
California Association of REALTORS®
Governmental Affairs
915 L Street, Suite 1460
Sacramento, CA 95814
Office: (916) 492-5236
Fax: (916) 444-1794
kevinr@car.org



2025 Annual Conference | The Westin Pasadena
Sign up at jamwomanup.com!

This email message, together with any attachments, is intended only for the use of the individual or entity to which it is addressed. It may contain information that is confidential and prohibited from disclosure. If you are not the intended recipient, you are hereby notified that any dissemination or copying of this message or any attachment is strictly

prohibited. If you have received this email in error, please notify the original sender at (916) 492-5236 and destroy this email, along with any attachments. Thank you.



May 30, 2025

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

Re: REALTORS® Comments on the CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations (Modified Text of Proposed Regulations)

To Whom It May Concern:

The California Association of REALTORS® (C.A.R.) respectfully reaffirms the concerns outlined in our February 13, 2025, comment letter related to the proposed regulations on Cybersecurity Audits, Risk Assessments, Automated Decision Making Technology (ADMT), and Insurance.


While the revised language provides some definitional clarity, the underlying structure of the proposed regulations remains unchanged—and with it, the potentially substantial financial and operational burdens that will impact housing and lending participants. The audit and risk assessment requirements still carry projected compliance costs that could exceed tens of thousands of dollars per entity, costs that will inevitably be borne by consumers. These new mandates pose a serious risk to housing affordability, particularly for first-time and first-generation buyers.

Likewise, the modified ADMT provisions continue to require lenders to accommodate consumer opt-outs for significant decisions such as mortgage approvals. In practice, this will likely necessitate manual processing, introducing delays that jeopardize transactions and undermine market stability.

C.A.R. continues to urge the Board and Staff to consider targeted exemptions or phased implementation for sectors like real estate, which are already subject to extensive oversight and play a vital role in expanding economic opportunity. Without such adjustments, the regulations as proposed risk harming the very consumers they aim to protect.

We appreciate the opportunity to comment and remain committed to working with the Agency on a regulatory approach that promotes both privacy and access to homeownership. For additional detail, we respectfully refer you to our original submission.

Sincerely,


Kevin Rodgers
Regulatory Advocate



REALTOR® is a federally registered collective membership mark which identifies a real estate professional who is a Member of the NATIONAL ASSOCIATION OF REALTORS® and subscribes to its strict Code of Ethics.



915 L Street, Suite 1460 Sacramento, CA 95814 | Tel (213) 739-8200 | Fax (213) 480-7724 | car.org

Grenda, Rianna@CPPA

From: Elizabeth Clayberger <eclayberger@calbankers.com>
Sent: Monday, June 2, 2025 4:09 PM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations - 6.2 California Bankers Association
Attachments: 6-2 CBA Public Comment on CCPA Updates Cyber Risk ADMT and Privacy Protection Regulations.pdf

This Message Is From an Untrusted Sender

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

[Report Suspicious](#)

Good afternoon,

Please find attached the updated comments regarding the California Consumer Privacy Act updates submitted by the California Bankers Association.

Thank you for this opportunity to provide written comments. Please let us know if you have any questions.

Best regards,
Elizabeth

Transmitted on Behalf of
Jason Lane
SVP, Director of Government Relations



Elizabeth Clayberger

PAC Administrator, Government Relations Assistant
1303 J Street, Suite 600 | Sacramento, CA 95814

T: (916) 438-4405

www.calbankers.com

Connect: [Website](#) | [Twitter](#) | [LinkedIn](#)

Bringing members **together**. Making our banks better.



June 2, 2025

California Privacy Protection Agency
ATTN: Legal Division – Regulations Public Comment
2101 Arena Blvd.
Sacramento, CA 95834
Via Email: regulations@ccpa.ca.gov

RE: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Privacy Protection Regulations

Dear Agency Members:

The California Bankers Association (CBA), appreciates the invitation and the opportunity to submit written comments in response to the ongoing rulemaking activities undertaken by the California Consumer Privacy Protection Agency as required by the California Consumer Privacy Act of 2018 (CCPA). CBA is one of the largest banking trade associations and regional educational organizations in the United States. CBA advocates on legislative, regulatory and legal matters on behalf of banks doing business in the state of California.

We wish to thank the California Privacy Protection Agency (CPPA) for its continued efforts to refine and narrow the scope of its proposed regulations on cybersecurity audits, risk assessments, and automated decision-making technology (ADMT). The May 2025 draft reflects thoughtful engagement with stakeholder input and demonstrates real progress in several areas—particularly in clarifying definitions and better aligning some provisions with existing privacy and security frameworks. These revisions are encouraging and appreciated. However, despite these improvements, the current draft still raises several serious concerns for the banking sector, particularly due to its overlap with established federal regulatory systems and the operational risks introduced by certain prescriptive state-level mandates.

Cybersecurity Audit Regulations

The CPPA's draft cybersecurity audit regulations adopt an overly prescriptive, one-size-fits-all approach that undermines the flexibility required to effectively manage risk in the

financial sector. Federal agencies such as the Office of the Comptroller of the Currency¹ (OCC), the Federal Reserve, and the Federal Financial Institutions Examination Council (FFIEC)² already impose rigorous, risk-based audit standards on financial institutions. The CCPA's requirement that businesses annually assess and justify every cybersecurity control, regardless of materiality or relevance to the institution's unique risk profile, is misaligned with these federal frameworks.

This rigid methodology may have the unintended effect of weakening security by forcing institutions to spread resources thinly across all control areas, including those of limited relevance or risk, instead of concentrating on high-priority areas. It is also counterproductive for institutions that already conduct audits tailored to their specific risk environments under federal supervision. We therefore urge the CCPA to permit businesses to fulfill the annual cybersecurity audit requirement by demonstrating adherence to existing, federally mandated cybersecurity audit processes.

Moreover, the draft rules do not provide adequate protections for the confidentiality of audit materials. Given the sensitivity of these documents, the final regulations should include provisions explicitly recognizing audit reports as proprietary and exempting them from disclosure under public records laws, litigation discovery, and other forms of compelled production.

Additionally, The revised language in Section 7122(a)(3), which addresses the independence of internal auditors, raises significant concerns for banks subject to Federal Reserve guidance³ that may conflict with the proposal. Under the original draft, a covered entity could rely on internal auditors if the highest-ranking auditor—such as the Chief Audit Executive (CAE)—reported both functionally and administratively to the company's board of directors, where a board existed. The updated language, however, appears to require that the CAE report instead to a member of executive management who lacks direct responsibility for the business's cybersecurity program. This change is problematic for several reasons. First, the prevailing best practice in corporate governance emphasizes that

¹ Office of the Comptroller of the Currency. (2023, July). *Comptroller's handbook: Corporate and risk governance*. <https://www.occ.treas.gov/publications-and-resources/publications/comptrollers-handbook/files/corporate-risk-governance/pub-ch-corporate-risk.pdf>

² Federal Financial Institutions Examination Council. (2020, April). *BSA/AML examination manual: Assessing the BSA/AML compliance program*. <https://bsaaml.ffeic.gov/manual/AssessingTheBSAAMLComplianceProgram/03>

³ Board of Governors of the Federal Reserve System. (2013, January 23). *Supplemental policy statement on the internal audit function and its outsourcing* (SR 13-1 / CA 13-1). <https://www.federalreserve.gov/supervisionreg/srletters/sr1301a1.pdf>

the CAE should report functionally to the board or its audit committee to preserve independence from management. Second, Federal Reserve⁴ supervisory guidance for covered banks explicitly states that the individual responsible for internal audit should have no operational role in the system of internal control and should report functionally to the audit committee—covering matters such as audit plans, findings, and performance evaluation. While that guidance permits administrative reporting to the CEO, it does not contemplate a structure where the CAE reports solely to a member of executive management outside the board's oversight, as now proposed.

Risk Assessment Requirements

The draft risk assessment regulations similarly impose excessive burdens by requiring granular documentation and evaluation of highly subjective impacts, such as "psychological harms" to an "average consumer." These requirements are not only difficult to operationalize, but they also risk exceeding the statutory mandate provided to the CPPA under the California Consumer Privacy Act (CCPA). Financial institutions are already subject to robust risk assessment obligations under the GLBA and oversight by federal regulators.

A particular concern is the potential requirement to disclose trade secrets or proprietary methods as part of compliance documentation submitted to the CPPA. The regulations should expressly clarify that no provision requires a business to reveal trade secrets or other intellectual property. We also recommend adding a confidentiality clause similar to the one proposed for cybersecurity audits, ensuring that risk assessments submitted to the Agency remain protected and proprietary.

Automated Decision-Making Technology (ADMT)

We remain concerned about the ADMT provisions, particularly the expanded definition of "financial or lending services," which now includes routine and operational activities such as transmitting or exchanging funds and check cashing. Combined with the elimination of the fraud and security exemption in Section 7221(b), this expansion would create a serious operational vulnerability. Financial institutions process millions of transactions daily, many of which are automatically reviewed using sophisticated fraud detection systems. Requiring businesses to offer opt-outs or appeals for automated decisions that block or flag potentially fraudulent transactions would directly undermine these critical controls. Worse

⁴ Board of Governors of the Federal Reserve System. (2013, January 23). *Supplemental policy statement on the internal audit function and its outsourcing* (SR 13-1 / CA 13-1). <https://www.federalreserve.gov/supervisionreg/srletters/sr1301a1.pdf>

still, providing consumers—including bad actors—with a clear and simplified appeal pathway could inadvertently create a roadmap for fraud. Such requirements would not only endanger the security of financial systems but also contradict the consumer protection goals of the CCPA.

Financial institutions have developed and refined comprehensive fraud prevention and response systems, including real-time alerts, multi-factor authentication, and dedicated review teams. These mechanisms already allow for timely resolution when legitimate transactions are mistakenly flagged. Forcing institutions to offer opt-outs or to justify every fraud-related action to consumers would dilute these protections and introduce new systemic risks. We therefore urge the CPPA to restore the fraud and security exception and to ensure that ADMT regulations do not apply to transaction monitoring or similar processes that are essential to fraud prevention.

Similarly, the definition of "significant decision" under Section 7001(ddd) remains overly broad. Including "allocation or assignment of work for employees" could be interpreted to include routine task routing tools, such as call center queue systems. These types of automation have no bearing on hiring, compensation, or career advancement and should not trigger compliance obligations under the ADMT rules. A de minimis or materiality threshold should be introduced to ensure that only decisions that genuinely affect employment status are covered.

Amendments to General Consumer Privacy Provisions

We also wish to highlight several concerns with the amendments to existing CCPA regulations. The proposed requirements for granular metadata tracking (e.g., Sections 7023(c), 7023(i), and 7023(k)) impose an unreasonably high burden on data management systems. These provisions would necessitate the tracking of individual data elements across all systems and compel businesses to maintain corrected information indefinitely and across all future data inputs. The marginal benefits to consumers are vastly outweighed by the extraordinary technical and operational costs.

Similarly, repeated changes to the Service Provider/Contractor Addendum template in Section 7051 create an unnecessary compliance burden. Each change requires large institutions to reassess and revise contractual relationships with hundreds or thousands of vendors, many of which involve time-intensive coordination and education efforts. These constant updates yield minimal consumer protection gains and introduce months of administrative delay.

The proposal to include the personal information of minors under 16 in the definition of Sensitive Personal Information (SPI) in Section 7001(bbb) is another area of concern. Such a change effectively alters statutory definitions and should be pursued, if at all, through legislation. The Governor's recent veto of a similar legislative effort underscores the need for restraint in using regulatory amendments to achieve policy outcomes that lack legislative consensus.

Additionally, we have concerns with the proposed change to Section 7020(e), which effectively transforms a permissive statutory provision into a mandatory regulatory requirement. While the statute allows a consumer to request data going beyond the 12-month default look-back period, the revised regulation would require businesses to proactively offer this option. This creates a new obligation not supported by the statutory text. The regulation should recognize that businesses may no longer retain older data due to lawful record retention policies. Accordingly, a business should not be penalized for being unable to fulfill such requests if the information has been deleted or purged in accordance with those policies. The regulation should clarify that responses are limited to information the business continues to maintain.

GLBA Exemption Clarity

Finally, we were encouraged to hear Chair Urban affirm, during the April 4th Board Meeting, that the Gramm-Leach-Bliley Act (GLBA) exemption under Civil Code §§ 1798.145 and 1798.146 remains intact and continues to apply. Chair Urban noted that, although the exemption does not affect the legal enforceability of the regulations—since GLBA-covered data falls outside the scope of the CCPA—it may be helpful for the Agency to make the exemption more visible or clearly stated within the regulatory text. She observed that some public commenters appeared confused about how the GLBA exemption functions, possibly because it is currently referenced by statute rather than explicitly restated in the draft rules. To address this, she suggested that a general statement be included earlier in the regulations to help stakeholders more easily understand that GLBA-governed data is already exempt. While such a clarification would not alter the legal effect of the regulations, it could provide important context and aid in interpretation. In response, General Counsel Laird acknowledged the suggestion and indicated that staff could consider alternative placement of such a clarification in a future iteration of the rules.

CBA supports efforts to provide additional clarity regarding the application of the GLBA exemption. Clearer language would help avoid confusion and ensure consistent interpretation by both regulated entities and the public.

In summary, while the CPPA's proposed regulations reflect a sincere and diligent effort to strengthen California's privacy framework, we respectfully urge the Agency to more carefully calibrate its approach. The banking sector is already subject to robust and well-established federal oversight that ensures strong consumer protections, rigorous cybersecurity standards, and responsible data use. The imposition of duplicative, prescriptive, and sometimes conflicting state-level mandates threatens to undermine these systems, reduce operational efficiency, and inadvertently compromise the very protections the regulations aim to enhance. We encourage the CPPA to consider more flexible, risk-based approaches, to restore critical exemptions such as those for fraud detection, and to recognize federally regulated institutions through exemptions or safe harbors that promote consistency and interoperability across jurisdictions. We remain committed to engaging constructively with the Agency to ensure that California's privacy rules are effective, balanced, and aligned with the broader national regulatory landscape.

Sincerely,



Jason Lane
SVP, Director of Government Relations
California Bankers Association

JL:ec

From: Evelina Ayrapetyan [REDACTED]
Sent: Monday, June 2, 2025 4:03 PM
To: Regulations@CPPA
Cc: Christabel Randolph
Subject: CAIDP Public Comments on CPPA's Modified text of proposed regulations in the CCPA regarding ADMT
Attachments: CAIDP-CPPA-ADMT-060225.pdf

This Message Is From an Untrusted Sender

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

Report Suspicious

Dear California Privacy Protection Agency:

We write from the Center for AI and Digital Policy (CAIDP) to offer our recommendations to the California Privacy Protection Agency (CPPA) on its modified text of proposed regulations in the California Consumer Privacy Act (CCPA) Regulations regarding Cybersecurity Audits, Risk Assessment and Automated Decision-Making Technology (ADMT).

Below we summarize our recommendations, details of which are set out in the attached document:

1. Require independent socio-technical expert evaluations as part of external stakeholder assessments for risk assessments conducted under §7151
2. Establish standardized incident reporting mechanisms for ADMT
3. Require data minimization for the use of ADMT in making significant decisions
4. Reinstate § 7152(a)(2) transparency requirements to ensure meaningful risk assessment
5. Reinstate § 7221 Requests to Opt-Out of ADMT

ABOUT CAIDP:

CAIDP is an independent, non-profit organization based in Washington, D.C. and Brussels. We advise national and state governments and international organizations on artificial intelligence (AI) and digital policy. CAIDP currently serves as an advisor on AI policy to the OECD, the Global Partnership on AI, the Council of Europe, the European Union, UNESCO, and other international and national organizations. We work with more than 800 AI policy experts in over 80 countries. CAIDP supports AI policies that advance democratic values and promote broad social inclusion based on human rights, democratic institutions, and the rule of law. We launched the CAIDP California affiliate in 2024 to strengthen our focus on AI legislation within the state. We successfully advocated for the passage of AB 2013 in 2024, and are co-sponsoring AB 316: AI defenses, currently in the California Legislative cycle. We have also provided guidance to California lawmakers on federal AI policy, collaborating with AI Caucus Vice Chair Don Beyer (D-VA) and Co-Chair Anna Eshoo (D-CA) on their proposed AI Foundation Model Transparency Act to promote greater transparency in foundation models.

Thank you for your consideration of our views. We would welcome the opportunity to exchange with you further about these recommendations.

Sincerely,

Evelina Ayrapetyan
CA Policy Lead | Center for AI and Digital Policy
Phone 323-719-6910
Website www.caidp.org
Email evelina@caidp.org



THE CENTER FOR AI AND DIGITAL POLICY (CAIDP)
Comments to the CALIFORNIA PRIVACY PROTECTION AGENCY
On the MODIFIED TEXT OF PROPOSED REGULATIONS IN THE CCPA
REGARDING: CYBERSECURITY AUDITS, RISK ASSESSMENT AND AUTOMATED
DECISION-MAKING TECHNOLOGY¹

The Center for AI and Digital Policy (CAIDP) welcomes the opportunity to respond to the California Privacy Protection Agency (CPPA) on the modified text of proposed regulations in the California Consumer Privacy Act (CCPA) regarding Cybersecurity Audits, Risk Assessment and Automated Decision-Making Technology (ADMT).

We commend the CPPA for its diligent work in advancing the rulemaking process and encourage the Agency to resist growing pressure from private industry to weaken safeguards and instead remain steadfast in upholding the civil rights and privacy of Californians. To support this mission, we strongly urge the agency to adopt a comprehensive risk assessment framework grounded in globally recognized standards, including the **NIST AI Risk Management Framework**.² Doing so will help ensure that the CCPA effectively addresses the unique and evolving risks posed by ADMT and remains a powerful tool for consumer protection in California. The CPPA has a critical opportunity to build on its strong privacy foundation and set a national benchmark for ADMT regulation.

We support the draft ADMT regulation. In particular, we urge the CPPA to retain the amendments to §7001, §7150, §7200, §7220, and §7222.

We offer the following recommendations to help guide the development of CPPA's Risk Assessment Framework:

- 1. Require independent socio-technical expert evaluations as part of external stakeholder assessments for risk assessments conducted under §7151**
- 2. Establish standardized incident reporting mechanisms for ADMT**
- 3. Require data minimization for the use of ADMT in making significant decisions**
- 4. Reinstate § 7152(a)(2) transparency requirements to ensure meaningful risk assessment**
- 5. Reinstate § 7221 Requests to Opt-Out of ADMT**

¹ CPPA, *Modified Text to CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations*, 2025, https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_mod_txt_pro_reg.pdf

² NIST, *AI Risk Framework*, (Jan. 2023), <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>

CAIDP Recommendations

1. **Require independent socio-technical expert evaluations as part of external stakeholder assessments under §7151**

The NIST AI RMF recognizes that AI systems are not purely technical but are embedded within and influenced by complex social, organizational and technical contexts.³ However, “with proper controls, AI systems can mitigate and manage inequitable outcomes”.⁴ Because the regulations in §7152 require identifying negative impacts on consumers' privacy including discrimination based on protected characteristics, socio-technical expert evaluations are critical. **We urge the CPPA to require independent evaluation of ADMT by socio-technical experts** to enhance the effectiveness of risk assessments for businesses and society alike, as well as mitigate internal biases and potential conflicts of interest. “The NIST AI RMF functions require diverse perspectives, disciplines, professions, and experiences. Diverse teams contribute to more open sharing of ideas and assumptions about the purposes and functions of technology – making these implicit aspects more explicit. This broader collective perspective creates opportunities for surfacing problems and identifying existing and emergent risks”.⁵

By identifying gaps in ADMT that may be missed from solely a technical evaluation, these experts play a vital role in shaping controls that are not only effective but also equitable and responsive to state and federal law.

With regards to Section § 7151(b), we urge the CPPA to include external evaluators that demonstrate the following characteristics:⁶

- i. Evaluators must have **no financial, operational, or advisory association** with the business developing or using ADMT to prevent conflicts of interest
- ii. Strict **disclosure requirements should be enforced** to ensure transparency in relationships
- iii. Evaluators must possess **domain-specific knowledge** (subject matter expertise (SME)), including AI ethics, technical auditing, cybersecurity, and systemic risk analysis

³ NIST, *AI Risk Management Framework*, p. 6, (Jan. 2023), <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf>

⁴ NIST, *AI Risk Management Framework*, p. 1, (Jan. 2023), <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf>

⁵ NIST *AI Risk Management Framework*, p. 10, (Jan. 2023), <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf>

⁶ CAIDP, *CAIDP Comments to the European Commission On The First Draft General-Purpose AI Code of Practice*, (Nov. 27, 2024), <https://files.constantcontact.com/dfc91b20901/fc5a67a3-fcc4-4a36-b8c5-434f4c1cc6c7.pdf>

- iv. Multidisciplinary teams are encouraged, **combining technical, legal, and societal expertise**
- v. Evaluators must **document their assessments thoroughly and make recommendations** publicly available (within confidentiality constraints)

2. Establish standardized incident reporting mechanisms for ADMT

To address the challenges of measuring AI-related risks, NIST proposes identifying and tracking emergent risks by organizations to enhance their risk management efforts.⁷ **By requiring standardized incident reporting mechanisms**⁸ through consistent, transparent, and actionable documentation to identify problems or failures of ADMT systems privacy protection is more effective as incidents may be observed, documented, reported, and learned from.⁹ There are global best-practices being developed for this purpose. It's important to note that the accumulation of smaller ADMT incidents could lead to a serious incident and reporting mechanisms aim to account for this possibility.¹⁰

A standardized incident reporting system would enable the CPPA to collect consistent data on failures, biases, and harms across businesses utilizing ADMT. Having access to such data can allow the CPPA to identify recurring issues, for instance, if there is systemic bias in “significant decisions”, for example, loan decisions applied across multiple financial institutions using ADMT—and separate isolated incidents from systemic vulnerabilities.

In her testimony before the US Congress, CAIDP President Merve Hickok emphasized that “High-risk AI systems replicate existing biases in the datasets, as well as biases and choices of their developers, resulting in discriminatory decisions; disadvantaging people with disabilities in hiring algorithms; health algorithms with inaccurate predictions for Black and brown-skinned individuals; and women being offered lower credit despite having the exact same assets as a male counterpart.”¹¹

⁷ NIST, *AI Risk Management Framework*, p. 5, (Jan. 2023), <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>

⁸ OECD, *Defining AI Incidents and Related Terms*, (2024) https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/05/defining-ai-incidents-and-related-terms_88d089ec/d1a8d965-en.pdf

⁹ CAIDP, *Standardizing AI Incident Reporting for Global Impact*, (Nov. 13, 2023), <https://s899a9742c3d83292.jimcontent.com/download/version/1725366025/module/8526440763/name/CAIDP-Update-5.43.pdf>

¹⁰ OECD, *Defining AI Incidents and Related Terms*, p 12, (2024) https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/05/defining-ai-incidents-and-related-terms_88d089ec/d1a8d965-en.pdf

¹¹ Merve Hickok Testimony. *Advances in AI: Are We Ready For a Tech Revolution?* House Committee on Oversight and Accountability Subcommittee on Cybersecurity, Information Technology, and Government Innovation (March 8, 2023), p. 4, https://oversight.house.gov/wp-content/uploads/2023/03/Merve-Hickok_testimony_March-8th-2023.pdf

Incident reporting could function akin to a data breach notification and would enable the CCPA to identify systemic risks or predatory privacy practices in ADMT applications.

3. Require data minimization for the use of ADMT in significant decisions

We urge the CCPA to require businesses to adopt the principle of Data Minimization,¹² core safeguard in both the NIST AI RMF,¹³ and the EU's General Data Protection Regulation (GDPR).¹⁴ Specifically, **we recommend that the CCPA require businesses to limit data collection strictly to what is necessary for the stated purpose.**¹⁵ For instance, personal health records or social media activity should not be collected or used in employment decisions unless directly relevant and legally permissible. To strengthen compliance with data minimization requirements, we recommend that the CCPA consider the European Data Protection Board's (EDPB) December 2024 guidance on processing personal data in AI models.¹⁶, which outlined practical standards for responsible data use in AI systems.

Embedding these safeguards into the CCPA regulations would establish clear, enforceable standards that limit data collection and use to what is strictly necessary for defined purposes, reducing unnecessary risks and burdens for California consumers.

Data minimization and limiting data collection at the first instance aligns with the CCPA's provision in **§ 7154: Prohibition Against Processing If Risks to Consumers' Privacy Outweigh Benefits**,¹⁷ which states that businesses must not process personal information if the risks to consumers' privacy outweigh the benefits to the consumer, business, or public.

¹² The Data Protection Commission, *Principles of Data Protection*,

<https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection>

¹³ NIST, *AI Risk Management Framework*, p. 16, (Jan. 2023), <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>

¹⁴ The Data Protection Commission, *Principles of Data Protection*,

<https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection>

¹⁵ CAIDP, *ICO Consultation on Purpose limitation in the generative AI lifecycle*, (Apr. 12, 2024),

https://www.linkedin.com/posts/center-for-ai-and-digital-policy_caidp-uk-ico-ai-purpose-specification-activity-7184732869674598400-f6wS/

¹⁶ EDPB, *EDPB opinion on AI models: GDPR principles support responsible AI*, (Dec. 18, 2024),

https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_en

¹⁷ CCPA, *Modified Text to CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations*, 2025,

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

One key strategy the CCPA should adopt is mandating the use of Privacy-Enhancing Techniques (PETs), which help minimize data collection, anonymize personal information, and prevent unauthorized data transfers.¹⁸¹⁹ This recommendation aligns with the CCPA’s foundational privacy protections.²⁰ Extending PET requirements across the data lifecycle will meaningfully strengthen data security and privacy while reinforcing public confidence in AI systems.

With regard to consumer data anonymization, it is essential to assess whether an ADMT trained on personal data can be classified as anonymous.²¹ Businesses should document measures to prevent or limit the collection of personal data during training, reduce the identifiability of individuals, and ensure the model is resistant to data extraction attacks. For an ADMT to qualify as anonymous, the likelihood of directly or indirectly extracting personal data must be extremely low,²² and the chance of unintentionally retrieving such data through queries must also be minimal, considering all reasonably available methods.

Our recommendations align with existing regulations in the CCPA, specifically § 7002,²³ which restricts the collection and use of personal information to what is reasonably necessary and proportionate for the stated purpose, and § 7027,²⁴ which allows consumers to limit the use and disclosure of sensitive personal information. Data minimization standards could make compliance requirements for businesses more straightforward rather than monitoring a wide range of complex regulatory obligations with excessive data collection.

¹⁸ CAIDP, *CAIDP Comments to OSTP on PETs*, (July 8, 2022), <https://www.caidp.org/app/download/8402029763/CAIDP-PETS-OSTP-07082022.pdf> In a 2022 statement to the Office of Science and Technology Policy (OSTP), we emphasized the role of Privacy-Enhancing Technologies (PETs) in fostering trust in data processing, particularly to advance equity for marginalized communities, and recommended requiring independent evaluation of PETs prior to deployment.

¹⁹ CAIDP, *CAIDP Sets out Recommendations for US AI Action Plan*, (Mar. 14, 2025), https://www.linkedin.com/posts/center-for-ai-and-digital-policy_caidp-ostp-ai-action-plan-march-15-2025-activity-7307019123497095169-lhTv In our 2025 response to the OSTP’s U.S. AI Action Plan Request for Information (RFI), we reaffirmed PETs’ critical importance and urged the federal government to invest in AI systems grounded in PETs to drive innovation, strengthen resilience against cybersecurity threats, and support workforce development.

²⁰ CCPA, *Proposed Text to CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations*), p. 111, 2024, https://ccpa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_mod_txt_pro_reg.pdf

²¹ EDPD, *EDPB opinion on AI models: GDPR principles support responsible AI*, p. 14, (Dec. 18, 2024), https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_en

²² EDPD, *EDPB opinion on AI models: GDPR principles support responsible AI*, p. 16, (Dec. 18, 2024), https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_en

²³ CCPA, *Proposed Text to CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations*), p. 12, 2024, https://ccpa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_mod_txt_pro_reg.pdf

²⁴ CCPA, *Proposed Text to CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations*), p. 66, 2024, https://ccpa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_mod_txt_pro_reg.pdf

These additions will allow businesses the knowledge to thoroughly identify and thus mitigate any risks associated with their personal data processing activities.

4. Reinstate §7152(a)(2) transparency requirements to ensure meaningful risk assessment

We strongly urge the CPPA to reinstate the risk assessment provisions outlined in § 7152(a)(2).²⁵ The NIST AI RMF states that “Trustworthy AI depends upon accountability. Accountability presupposes transparency.”²⁶ Provisions requiring businesses to assess the quality of personal information, mitigate bias, and improve data accuracy are essential to protecting California consumers from the well-documented harms associated with the use of ADMT across various sectors.

Eliminating § 7152(a)(2) would reduce ADMT oversight to little more than basic record-keeping, allowing businesses to check boxes rather than confront and address the real-world impacts of their systems.

Transparency is not optional. It is foundational. It enables redress when ADMT outputs result in adverse outcomes and is a prerequisite for fairness. AI systems can potentially increase the speed and scale of biases and perpetuate and amplify harms to individuals, groups, communities, organizations, and society. Bias is tightly associated with the concepts of transparency as well as fairness in society.²⁷

Reinstating robust risk assessment requirements is not only feasible but necessary for ensuring ADMT is deployed in ways that uphold California’s longstanding commitment to privacy, equity, and consumer protection.

5. Reinstate §7221 Requests to Opt-Out of ADMT

The CPPA’s decision to remove the consumer opt-out right from ADMT systems as long as a human appeal process is available,²⁸ is a step in the wrong direction that weakens consumer protections and undermines meaningful choice. As correctly stated by the CPPA in the initial

²⁵ CPPA, *Proposed Text to CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations*), p. 109, 2024, https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_mod_txt_pro_reg.pdf

²⁶ NIST, *AI Risk Management Framework*, p. 15, (Jan. 2023), <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>

²⁷ NIST, *AI Risk Management Framework*, p. 18, (Jan. 2023), <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>

²⁸ CPPA, *Modified Text to CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations*), p. 106, 2025, https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_mod_txt_pro_reg.pdf

Draft Regulation, consumers have a right to opt out of ADMT. The availability of a human appeal is not a substitute for the right to opt out of consequential decisions made by ADMT. Many consumers may not be aware of the appeal process, may lack the time or resources to navigate it, or may experience harm before the appeal is even resolved.

We urge the CPPA to reinstate the opt-out mechanism regardless of whether a human appeal option is offered. Ensuring that individuals can proactively decline the use of ADMT in decisions that significantly affect their lives is fundamental to autonomy, privacy, and fairness.

Without this right, California risks weakening core protections established by the CCPA, protections that must evolve alongside emerging technology, and sets a concerning precedent for ADMT governance across the country.

The CPPA stands at a pivotal moment to reaffirm California's leadership in data protection. To continue serving the will of Californians, the CCPA must evolve to safeguard privacy, dignity, and autonomy when ADMT is deployed. **The CPPA should require robust risk assessments, ensure opt-out rights, and consider best-practices in the NIST AI RMF and GDPR to establish a forward-looking, rights-preserving, and enforceable structure for ADMT oversight.**

Our recommendations are grounded in global best practices, offering a clear path for businesses while ensuring California residents remain protected against the opaque and potentially harmful impacts of ADMT. We urge the CPPA to adopt these measures to create a governance model that promotes transparency, fairness, and accountability while fostering innovation rooted in public trust.



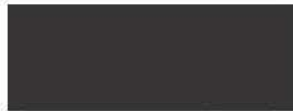
We thank you for the opportunity to consult on the Modified Text of Proposed Regulations.

Sincerely,

Merve Hickok,
President
CAIDP



Marc Rotenberg,
Executive Director
CAIDP



Evelina Ayrapetyan,
CA Policy Lead
CAIDP



Neesha Patel,
Research Assistant
CAIDP



Christabel Randolph,
Associate Director
CAIDP



Adrianna Tan
Research Assistant
CAIDP



Vincent Cortese,
Intern
CAIDP



About CAIDP:

The Center for AI and Digital Policy (CAIDP) is a global, independent, non-profit research and education organization headquartered in Washington, DC. CAIDP's mission is to ensure that AI and digital policies promote a better society, more fair, more just, and more accountable - a world where technology promotes broad social inclusion based on fundamental rights, democratic institutions, and the rule of law.²⁹ CAIDP provides expert guidance on AI policy to governments and international organizations, including UNESCO, OECD, the Council of Europe, G7 and G20, and the European Parliament. CAIDP publishes its annual Artificial Intelligence and Democratic Values (AIDV) report,³⁰ which evaluates global AI policies and practices against democratic principles using a standardized methodology.

²⁹ CAIDP, <https://www.caidp.org/>

³⁰ CAIDP, *Artificial Intelligence and Democratic Values* (2025), <https://www.caidp.org/reports/aidv-2025/>



We launched the CAIDP California affiliate in 2024 to strengthen our focus on AI legislation within the state. We successfully advocated for the passage of AB 2013,³¹ and are co-sponsoring AB 316: AI defenses,³² currently in the California Legislative cycle. We have also provided guidance to California lawmakers on federal AI policy, collaborating with AI Caucus Vice Chair Don Beyer (D-VA) and Co-Chair Anna Eshoo (D-CA) on their proposed AI Foundation Model Transparency Act to promote greater transparency in foundation models.³³

³¹ CAIDP, *CAIDP Advises California Assembly on AI Training and Data Transparency*, (Aug. 19, 2024), https://www.linkedin.com/posts/center-for-ai-and-digital-policy_caidp-california-ab2013-ai-transparency-activity

³² California Legislative Information, *AB-316 Artificial Intelligence: Defenses*, (2025-2026), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260AB316

³³ Congressman Don Beyer, Beyer, Eshoo Introduce Landmark AI Regulation Bill, (Dec. 22, 2023), <https://beyer.house.gov/news/documentsingle.aspx?DocumentID=6052>

Grenda, Rianna@CPPA

From: Vega, Olivia <OVega@cov.com>
Sent: Monday, June 2, 2025 2:44 PM
To: Regulations@CPPA
Cc: Tonsager, Lindsey; Ponder, Jayne
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: CalChamber Comment - CCPA Draft Regulations Cyber Audits, Risk Assessments, ADMT (June 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

To whom it may concern:

Please see comments from the California Chamber of Commerce on the draft CCPA regulations on cyber audits, risk assessments, and ADMT attached.

Best,
Lindsey Tonsager
Jayne Ponder
Olivia Vega
Counsel for CalChamber

Olivia Vega

Covington & Burling LLP
One CityCenter, 850 Tenth Street, NW
Washington, DC 20001-4956
T +1 202 662 5505 | ovega@cov.com
www.cov.com

COVINGTON

This message is from a law firm and may contain information that is confidential or legally privileged. If you are not the intended recipient, please immediately advise the sender by reply e-mail that this message has been inadvertently transmitted to you and delete this e-mail from your system. Thank you for your cooperation.

COVINGTON

BEIJING BOSTON BRUSSELS DUBAI FRANKFURT
JOHANNESBURG LONDON LOS ANGELES NEW YORK
PALO ALTO SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

Covington & Burling LLP
Salesforce Tower
415 Mission Street, Suite 5400
San Francisco, CA 94105-2533
T +1 415 591 6000

June 2, 2025

By Electronic Mail

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Boulevard
Sacramento, California 95834
regulations@coppa.ca.gov

Re: CCPA Modified Text Of Regulations On ADMT, Risk Assessments, And Cybersecurity Audits

The California Chamber of Commerce (“CalChamber”) submits these comments in response to the California Privacy Protection Agency’s (“COPA” or “agency”) May 9, 2025 request for public input on modifications to the text of proposed regulations regarding automated decisionmaking technologies (“ADMT”), cybersecurity audits, and risk assessments (collectively, “Modified Text”).¹

As evidenced by the nearly 2,000 pages of written public comments,² including input from Governor Newsom and the California Congressional Delegation, these regulations risk crippling the state’s economy and “could create significant unintended consequences and impose substantial costs that threaten California’s enduring dominance in technological innovation”³ if they are not appropriately tailored to the text of the COPA statute.⁴ CalChamber appreciates the revisions made in the Modified Text, which are a step in the right direction to addressing commenters’ concerns of statutory overreach, inconsistencies with other U.S. laws and standards, substantial burden on California businesses, and constitutional infirmities.⁵ Additional changes are necessary, however, to address the legal and practical problems with the

¹ See COPA, *Modified Text of Proposed Regulations* (May 9, 2025), https://coppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_mod_txt_pro_reg.pdf [hereinafter Modified Text].

² See April 4, 2025 Board Meeting Transcript, 19, https://coppa.ca.gov/meetings/materials/20250404_audio_transcript.pdf [hereinafter April Board Meeting Transcript].

³ Letter from Gov. Gavin Newsom to COPA (Apr. 23, 2025), <https://cdn.kqed.org/wp-content/uploads/sites/10/2025/04/COPA-Letter.pdf> [hereinafter Governor Newsom Letter to COPA].

⁴ See *Written Public Comments Received During the November 22, 2024 – February 19, 2025 Comment Period*, Proposed Regulations on COPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies, https://coppa.ca.gov/regulations/ccpa_updates.html [hereinafter Written Comment Record].

⁵ See, e.g., Letter from CalChamber to COPA (Feb. 18, 2025).

COVINGTON

Modified Text that remain and appropriately tailor the regulations to demonstrable harms to consumer privacy. Specifically, CalChamber requests that the agency:

- Further revise the Modified Text to avoid overreach and conflict with the statutory text and efforts by the Governor, legislature, and other agencies;
- Recognize that harmonizing the regulations with other U.S. privacy frameworks satisfies the clarity standards required under administrative law and is consistent with the statute's intent;
- Ensure that the Board and the public has accurate and complete information about the costs the Modified Text (if adopted) would impose on businesses and the state's economy by updating the original Standardized Regulatory Impact Assessment ("SRIA"), rather than rushing through proposed rules with no clear understanding of their true cost; and
- Amend the Modified Text to avoid remaining concerns with fundamental constitutional protections.

Each of these concerns is discussed further in the sections below. Additionally, CalChamber's comments include an Appendix that offers the CPPA reasonable alternatives that would be equally effective in achieving the important purposes of advancing consumer privacy and security.⁶

I. Further Revisions Are Needed To Prevent Statutory Overreach And Conflict With Actions Taken By The Governor, The State Legislature, And Other Agencies.⁷

CalChamber appreciates the agency's decision to remove references to behavioral advertising and public profiling in response to significant concerns raised by numerous commenters that the draft regulations were "venturing into areas beyond [the agency's] mandate."⁸ As explained below, further revisions are necessary to avoid conflict with legal requirements and policy objectives of other regulators and stretching the agency beyond its regulatory remit.⁹

⁶ See Cal. Gov't Code § 11346.2(b)(4)(A) (requiring that agency provide a description of "reasonable alternatives to the regulation and the agency's reasons for rejecting those alternatives") (noting that reasonable alternatives include "alternatives that are proposed as less burdensome and equally effective in achieving the purposes of the regulation").

⁷ CalChamber understands that the removal of the specific security, fraud prevention, and safety exemption for the ADMT opt-out requirement acknowledges the other statutorily-created exemptions that permit processing activities for security, fraud prevention, and safety activities. See, e.g., Cal. Civ. Code §§ 1798.145(a)(1)(A)-(B), (D)-(E).

⁸ Governor Newsom Letter to CPPA. See April Board Meeting Transcript, 34, https://cppa.ca.gov/meetings/materials/20250404_audio_transcript.pdf ("I agree with many of the critics that the ADMT regulations go far beyond what is justified in the statute.").

⁹ It is a court's "obligation to strike down such regulations" if they "alter or amend the statute or enlarge or impair its scope." *Naranjo v. Spectrum Sec. Servs., Inc.*, 88 Cal. App. 5th 937, 945 (2023), *aff'd* 15 Cal. 5th 1056, 547 P.3d 980 (2024).

COVINGTON

A. The Agency Must Further Amend The ADMT Provisions To Exclude Training And Regulate Solely Automated Decisions.

Numerous commenters expressed concern about the overly broad definition of ADMT in the draft regulations.¹⁰ The Modified Text offers some improvement over the prior version by modifying the ADMT definition to remove the “substantially facilitate” decisionmaking language.¹¹ However, the Modified Text requires further refinement in order to align the definition to the criteria outlined in the statutory text and avoid overreach that “could create significant unintended consequences and impose substantial costs that threaten California’s enduring dominance in technological innovation.”¹²

First, as numerous commenters — including Governor Newsom — have emphasized, the agency must “remove the training of ADMT” from the Modified Text in order to avoid agency overreach beyond the bounds of the statutory text.¹³ This alternative also received support during the April Board meeting.¹⁴ The plain text of the statute limits rulemaking to a business’ “*use of* automated *decision*making technology” to process personal information.¹⁵ Training models is not the “use of” ADMT because the training itself does not result in any “decision” being made for any particular consumer, nor does training ADMT present a significant risk to consumer privacy. Rather, training reflects only the internal, pre-use development of a technology. Because the Modified Text is in conflict with the limited scope of the statute, all references to ADMT training must be removed, including ADMT training requirements for privacy risk assessments.¹⁶

Second, multiple commenters emphasized that the statute requires ADMT to be fully automated in order to fall within the statutory definition. The Modified Text proposes to change “substantially facilitate” to tools that “substantially replace” human decisionmaking.¹⁷ However, this revision fails to cure commenters’ concern of agency overreach. The statutory text is clear — only the “use of *automated* decisionmaking technology” may be regulated. Where a human has involvement in or control over the decision, the tool is — by definition — not “automated.”¹⁸ Additionally, automated tools can be used for profiling that does not result in a decision, as

¹⁰ See Written Comment Record.

¹¹ Modified Text § 7001(e).

¹² Governor Newsom Letter to CPPA.

¹³ *Id.*

¹⁴ April Board Meeting Transcript, 62-170.

¹⁵ Cal. Civ. Code § 1798.185(a)(15).

¹⁶ To determine whether a regulation is “consistent and not in conflict” with the agency’s authorizing statute, courts look to “whether the regulation is within the scope of the authority conferred.” *California Chamber of Com. v. State Air Res. Bd.*, 10 Cal. App. 5th 604, 619 (2017); *see also* Cal. Gov’t Code § 11342.2 (stating that “no regulation adopted is valid or effective unless consistent and not in conflict” with the agency’s authorizing statute).

¹⁷ Modified Text § 7001(e).

¹⁸ The Cambridge Dictionary defines “automated” as “carried out by machines or computers *without needing human control*.” Cambridge Dictionary, https://dictionary.cambridge.org/us/dictionary/english/automated#google_vignette.

COVINGTON

required by the statutory text.¹⁹ By regulating technologies that fall below the specified statutory threshold, the Modified Text remains in conflict with the statute and subject to judicial challenge. Accordingly, the ADMT definition should be limited to the processing of personal information for solely automated decisions.²⁰

The two changes requested above to the definition of ADMT are not only necessary to bring the regulations in line with the statutory text, but also to avoid conflicts with ongoing efforts by Governor Newsom and the state legislature.²¹ Governor Newsom is overseeing a task force of academics and experts that will provide empirical, science-based input to inform regulation across multiple state agencies.²² And California lawmakers introduced numerous bills on ADMT this session, many of which advance far narrower definitions for the regulated technology than the ADMT definition proposed in the Modified Text.²³ As Board Members and others recognized at the May Board meeting, this walking-before-running approach also has the benefit of providing the agency an opportunity to learn more as this relatively nascent industry develops to avoid over-regulating in ways that create unnavigable conflicts for innovators operating in California.²⁴

B. The Modified Text Imposes Explainability Requirements That Exceed The Statute’s Privacy Mandate.

The Modified Text retains explainability requirements focusing on highly technical aspects of ADMT tools, rather than on rights of access providing consumers meaningful information related to the privacy of their personal information. The required information not only extends far beyond the privacy access right authorized under the statute, but also creates significant uncertainty for businesses while offering consumers no measurable privacy benefits.

¹⁹ Cal. Civ. Code § 1798.185(a)(15) (providing authority to issue regulations on “use of automated decisionmaking technology”).

²⁰ Note that this is closest to “Alternative 3” considered during the April board meeting. *See* Potential Modifications to Proposed Regulations, https://cippa.ca.gov/meetings/materials/20250404_item6_presentation.pdf.

²¹ *See* April Board Meeting Transcript at 60 (reflecting Chair Urban’s statements that “I think I am safe in saying nobody on the board wants to . . . conflict with or . . . cause issues with . . . the broad work that is going on”).

²² *See* JOINT CALIFORNIA POLICY WORKING GROUP ON AI FRONTIER MODELS, DRAFT REPORT (Mar. 28, 2025), https://www.cafontieraigov.org/wp-content/uploads/2025/03/Draft_Report_of_the_Joint_California_Policy_Working_Group_on_AI_Frontier_Models.pdf.

²³ *See* CA AB 1018, 2025-2026 Leg. (Cal. 2025); CA SB 420, 2025-2026 Leg. (Cal. 2025); CA SB 468, 2025-2026 Leg. (Cal. 2025); CA SB 503, 2025-2026 Leg. (Cal. 2025); CA SB 833, 2024-2025 Leg. (Cal. 2025) (state agency requirements). *See also* April Board Meeting Transcript at 35.

²⁴ *See* May 1, 2025 Board Meeting, 1:47, <https://www.youtube.com/watch?v=k7ZqDxHQZpA> (after receiving risk assessment reports, the agency can “amend the regulations accordingly” for clarity); *see id.* at 2:03 (“We can amend these regulations . . . based on what we are observing in the marketplace.”).

COVINGTON

The agency should avoid prescriptive regulations where there is no evidence of consumer harm that needs to be addressed.

For example, the Modified Text mandates businesses provide consumers with “explanations,” which could include “the parameters that generated the output.”²⁵ Some of today’s models reportedly have over a *trillion* parameters.²⁶ Providing consumers explanations of all the different parameters that have resulted in the output (assuming it is possible to even know this information, which is not always the case) is unlikely to provide the consumer with “meaningful information” as required by the statutory text.²⁷ Creating further uncertainty for consumers and businesses, there is no consensus under the current state of explainability research on what information can or should be provided to explain how ADMT technology reaches a decision or how an output is generated.²⁸ These practical challenges are likely to become even more pronounced as technology continues to evolve.

CalChamber proposes alternative language in the Appendix that provides a less burdensome — and equally effective — approach to providing consumers meaningful information about how their personal information is processed by ADMT to reach a significant decision concerning the consumer.

C. The Modified Text Encroaches On Other Regulators And The Legislature By Proposing Overlapping, Conflicting Requirements For ADMT In The Workplace.

To avoid conflicts with the California Civil Rights Department’s (“CRD”) and legislature’s ongoing efforts to regulate ADMT in the workplace, the CPPA should remove employment decisions and “allocation / assignment of work and compensation” from the Modified Text, including in requirements to complete risk assessments.

The inclusion of employment-related decisions overlaps with regulations issued by the CRD on the use of “automated-decision systems” in the workplace to reach employment decisions.²⁹ In addition, lawmakers have introduced a number of bills this session addressing

²⁵ Modified Text § 7222(b)(2).

²⁶ See, e.g., Sarah Kreps, *The global AI race: Will US innovation lead or lag?*, BROOKINGS (Dec. 6, 2024), <https://www.brookings.edu/articles/the-global-ai-race-will-us-innovation-lead-or-lag/> (“Within five years, generative models went from 1.5 billion parameters to over a billion. . .”).

²⁷ Cal. Civ. Code § 1798.185(a)(15).

²⁸ Cynthia Rudin et al., *Interpretable Machine Learning: Fundamental Principles and 10 Grand Challenges*, ARXIV (July 10, 2021) <https://arxiv.org/abs/2103.11251> (describing technical challenges for interpreting machine learning-based systems); Hofit Wasserman-Rozen, Ran Gilad-Bachrach, & Niva Elkin-Koren, *Lost in Translation: The Limits of Explainability in AI*, 42 CARDOZO ARTS & ENT. 391, 432 (2024) (noting that “sometimes models are so complex that they simply cannot be explained in a meaningful way”); Gabriel Nicholas, *Explaining Algorithmic Decisions*, 4 GEO. L. TECH. REV. 711, 727 (2020) (noting that there are no “intrinsic explanations” for certain machine learning algorithms).

²⁹ See Final Unmodified Text of Proposed Employment Regulations Regarding Automated-Decision Systems, <https://calcivilrights.ca.gov/wp-content/uploads/sites/32/2025/03/Attachment-B-Final-Unmodified-Text-of-Proposed-Employment-Regulations-Regarding-Automated-Decision-Systems.pdf> (making it unlawful to use an automated-decision system that discriminates against an applicant, and (continued...))

COVINGTON

workplace ADMT use, many of which substantially overlap with the Modified Text. For example, SB 7's notice requirements for the use of ADMT to make an employment decision duplicate the Modified Text's pre-use notice requirement for overlapping types of employment decisions.³⁰ SB 7 was also amended to remove hiring-related decisions from the majority of the bill to address implementation concerns.³¹ CalChamber urges the agency to remove employment-related decisions from the Modified Text that could risk conflicting requirements for businesses and a confusing experience for California workers.

This includes all references to “allocation / assignment of work and compensation,” which should be removed from the Modified Text.³² Importantly, and as Board Member Mactaggart indicated at the April Board meeting, these activities do not reflect “*significant* decisions” for the purposes of a privacy statute.³³ For example, the assignment of work, such as the creation of schedules for workers, involve routine business operations that present no privacy risk to employees and contractors. Indeed, the CRD seems to acknowledge this, as it focused its regulations on “automated-decision systems” only related to hiring, firing, and promotion.³⁴ Notably, in practice, allocation / assignment of work and compensation encompasses a broad range of activities that would encumber California businesses with burdensome risk assessment, opt-out, access, and notice requirements for low-risk, everyday business operations.

D. Pre-Use Notice Requirements Are In Conflict With The Statute And Must Be Removed From The Modified Text.

Numerous commenters expressed concern that the agency has no statutory authority to require businesses to publish a “pre-use notice” for ADMT and that this prescriptive requirement substantially increases the cost of the regulations with no demonstrated benefit for consumers.

The Modified Text's broad and prescriptive pre-use notice requirements go far beyond the statute's narrow direction to the agency to issue rules governing how “access and opt-out

imposing requirements on the use of automated-decision systems to analyze facial expressions or physical characteristics during interviews).

³⁰ See, e.g., CA SB 7, 2025-2026 Leg. (Cal. 2025); see also, e.g., CA AB 1331, 2025-2026 Leg. (Cal. 2025).

³¹ See April 25, 2025 SB 7 Analysis, Senate Committee on the Judiciary, https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=202520260SB7.

³² Allocation / assignment of work and compensation includes a broad range of employment operations, including specifically “[a]llocation or assignment of work for employees; or salary, hourly or per-assignment compensation, incentive compensation such as a bonus, or another benefit.” Modified Text § 7002(ddd)(4)(B).

³³ See April Board Meeting Transcript at 115 (“[N]o one wants to be in a . . . unfairly surveilled workplace, but this is a privacy statute so I [sic] think the definition of ‘significant decision’ absolutely needs to be scaled back. . . . And, especially, . . . tied to the actual denial of . . . the job that you were looking for.”).

³⁴ See Final Unmodified Text of Proposed Employment Regulations Regarding Automated-Decision Systems, <https://calcivilrights.ca.gov/wp-content/uploads/sites/32/2025/03/Attachment-B-Final-Unmodified-Text-of-Proposed-Employment-Regulations-Regarding-Automated-Decision-Systems.pdf> (making it unlawful to use “automated-decision systems” that discriminates against an applicant, among other requirements).

COVINGTON

rights” operate in the context of ADMT.³⁵ The statute includes two specific notices that must be provided *proactively* to all consumers: (1) a privacy policy and (2) a notice of financial incentives.³⁶ For each of these two notices, the statute prescribes the specific categories of information that must be included.³⁷ None of these categories reference ADMT. To the contrary, when the statute addresses ADMT disclosures, the statute refers only to disclosures made *reactively* in response to a specific consumer’s request to access information about how their personal information has been processed.³⁸ Because the Modified Text requires proactive pre-use ADMT notices that are in conflict with the statute’s mandate that ADMT disclosures be provided only reactively when a specific consumer exercises their access right, the pre-use notice requirements must be removed from the Modified Text.

The regulatory overreach resulting from the pre-use notice requirement is particularly concerning given that these notices would substantially and unnecessarily increase the costs of complying with the regulations. Businesses would be required to undertake additional fact-finding to identify all the highly-technical information required in the pre-use notice, conduct the technical work to update their sites and services to post this entirely new notice, and maintain these separate notices over time. Because the information required to be included in the pre-use notice is highly technical, businesses would need to make careful legal judgments about how to comply with the Modified Text’s requirements without exposing sensitive information that has a significant impact on the ability of California innovators to compete in the global innovation race. The addition of an exception for trade secrets in certain sections does not cure that problem, as businesses still must grapple with difficult, fact-specific judgments to reconcile safeguarding trade secret-protected information with pre-use disclosure requirements. These costs are not offset by benefits to consumers, who – for the same reasons described above in Section I.B – are likely to find the highly technical information required in these pre-use notices to be confusing and overly complicated.³⁹

E. The Threshold For Requiring A Privacy Assessment Remains Too Low And The Content Required In Such Assessment Continues To Be Too Prescriptive.

The proposed risk assessment requirements need substantial further revisions to align with the statutory text and voter intent regarding the processing thresholds and contents for such assessments. First, the agency must delete low-risk processing activities from the activities that require risk assessments, which do not satisfy the statute’s clear direction to require risk assessments for processing activities that present “significant” privacy risk.⁴⁰ For example, as discussed in Section I.C., use of ADMT for allocation / assignment of work and compensation

³⁵ Cal. Civ. Code § 1798.185(a)(15).

³⁶ See Cal. Civ. Code §§ 1798.100(a)-(b); 1798.125(b)(2).

³⁷ See *id.*

³⁸ Cal. Civ. Code § 1798.185(a)(15) (limiting regulations on ADMT to consumer access and opt-out rights).

³⁹ Ample academic and industry commentary underscores that more and longer privacy notices do not improve consumer comprehension and present cost to consumers. See, e.g., Isabel Wagner, et al., *Privacy Policies across the Ages: Content of Privacy Policies 1996-2021*, ARXIV (Jan. 21, 2022) <https://arxiv.org/abs/2201.08739> (quoting a study that the annual economic opportunity cost for reading privacy policies was estimated at \$781 billion for US users).

⁴⁰ Cal. Civ. Code § 1798.185(a)(14)(B).

COVINGTON

activities reflect routine activities that do not present a “significant” privacy risk.⁴¹ Further, and as discussed in Section I.G., presence in a public location does not reflect a “significant” risk to privacy. Risk assessments should be required where the business (1) sells or shares personal information, (2) processes sensitive personal information for purposes other than those identified in section 7027(m) of the regulations, or (3) uses ADMT to reach a significant decision that imposes significant risk to consumer privacy.

Additionally, regarding the contents of the risk assessments, the agency should remove requirements unrelated to privacy and permit businesses flexibility to address criteria relevant for the processing activity. Notably, the statute contemplates *privacy* risk assessments, and thus, discussions of “economic harms,” “physical harms,” and other topics with no relation to privacy should be removed.⁴² Further, the current list of inflexible topics a business “must” consider results in a burdensome paperwork exercise that contravenes the explicit statutory direction to engage in a risk-based balancing exercise.⁴³ The agency provides no evidence that addressing each of these topics is necessary to prevent consumer harm. The agency should therefore prioritize a flexible set of criteria that the business can tailor to the circumstances of a particular processing activity and that is interoperable across U.S. privacy laws, rather than an inflexible check-the-box exercise that is unlikely to keep paces with changes in technologies and divert business resources towards a paperwork exercise without consumer benefit.

F. Physical Or Biological Identification Or Profiling Requirements Overlap With Existing Obligations In The Statute.

All references to “physical or biological identification or profiling” must be removed from the regulations to avoid conflict with the statutory text. The statute makes clear that biometric information reflects physiological, biological, or behavioral characteristics to “establish individual identity,” which shares substantial overlap with the “physical or biological identification or profiling” concept – *i.e.*, identifying or profiling a consumer using information that depicts or describes physical or biological characteristics or measurements.⁴⁴ Businesses processing biometric data would be required to complete a risk assessment; thus, a separate requirement to also undertake risk assessments for “physical or biological identification or profiling” imposes unnecessary costs and a redundant and confusing obligation, without any benefit to consumers. To the extent that the agency is concerned about training ADMT that will

⁴¹ Modified Text § 7150(b)(3) (requiring risk assessments for use of ADMT for “significant decisions”).

⁴² Modified Text § 7152(a)(5)(E)-(F).

⁴³ Cal. Civ. Code § 1798.185(a)(14)(B) (requiring the agency to establish risk assessments for businesses to “identif[y] and weigh[] the benefits resulting from the processing . . . , against the potential risks to the rights of consumers associated with that processing”).

⁴⁴ Compare Modified Text, § 7001(ee) (defining “physical and biological identification or profiling” to mean “identifying or profiling a consumer using automated measurements or analysis of their physical or biological characteristics, or automated measurements or analysis of or relating to their body”) with Cal. Civ. Code § 1798.140(c) (defining “biometric information” as “physiological, biological, or behavioral characteristics, including information pertaining to an individual’s deoxyribonucleic acid (DNA), that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity”).

COVINGTON

use biological or physical characteristics for “profiling,” a risk assessment would already likely be required for processing of sensitive personal information.⁴⁵

G. The Agency Cannot Create A New Requirement For Sensitive Location Data Absent A Statutory Amendment.

It is a fundamental principle of California administrative law that an agency’s authority is defined by, and limited to, the bounds of the authorizing statute.⁴⁶ Notwithstanding how laudable or well-intentioned an agency’s purpose might be, authority to enact new legal requirements must remain with the elected members of the state legislature. Accordingly, it is concerning that the Modified Text creates an entirely new legal concept of “sensitive locations” that appears nowhere in the statutory text. Notably, the statute does define “sensitive personal information,” but this definition does not include sensitive locations.⁴⁷ The agency therefore does not have carte blanche authority to issue new regulations on sensitive locations, and references to sensitive locations must be removed from the Modified Text.

H. The Modified Text Remains In Conflict With Statutory Thresholds For Cybersecurity Audits And Should Be Aligned With Existing California Law.

The Modified Text does not address commenters’ concerns that the proposed cybersecurity audit threshold is too low and in conflict with the statutory text.⁴⁸ The plain text of the statute directs the agency to identify processing activities that present a “significant” risk to consumer security based not only the “size and complexity of the business,” but also the “nature and scope of processing activities.”⁴⁹ Notwithstanding this explicit direction, the Modified Text only considers the “size and complexity of the business” and ignores the “nature

⁴⁵ Compare Cal. Civ. Code § 1798.140(z) (defining profiling as “any 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 person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements”) with Cal. Civ. Code § 1798.140(ae)(1)-(2) (defining sensitive personal information to include personal information that reveals “financial account, debit card, or credit card,” “precise geolocation,” “genetic data,” “neural data,” “personal information analyzed concerning a consumer’s health,” and “personal information analyzed concerning a consumer’s sex life or sexual orientation”).

⁴⁶ See *supra* note 8.

⁴⁷ See Cal. Civ. Code § 1798.140(ae).

⁴⁸ To determine whether a regulation is “consistent and not in conflict” with the agency’s authorizing statute, courts look to “whether the regulation is within the scope of the authority conferred.” *California Chamber of Com. v. State Air Res. Bd.*, 10 Cal. App. 5th 604, 619 (2017); see also Cal. Gov’t Code § 11342.2 (stating that “no regulation adopted is valid or effective unless consistent and not in conflict” with the agency’s authorizing statute).

⁴⁹ Cal. Civ. Code § 1798.185(a)(14)(a) (emphasis added) (“Factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities.”).

COVINGTON

and scope of processing activities.” In doing so, the Modified Text inappropriately renders portions of the statutory text surplusage (a result that courts disfavor).⁵⁰

Significantly (and as explicitly recognized in the statutory language), not all businesses of a certain size present a “significant” risk to the security of personal information. For example, a very large business that collects and processes only full name, telephone number, and address (information that is otherwise generally published in the local telephone directory) does not pose a “significant” risk to the security of consumers’ personal information. But a very small business that collects and processes genetic information of individuals suffering from a rare disease in order to market to them might.

Moreover, contrary to the assertion in the Initial Statement of Reasons, revenue is not “a proxy for the complexity of a business.”⁵¹ If that were the case, the statute would not have needed to list it separately as an independent consideration. For example, a company with substantial revenue might have a relatively simple business that processes personal information only internally. In contrast, a company with much less revenue might have a highly complex business that requires disclosing sensitive personal information to numerous vendors for processing.

Because the Modified Text inappropriately focuses on the size of the business and does not also consider the other statutorily-mandated factors when determining whether a cybersecurity audit is required, the Modified Text requires further revision consistent with the text proposed in the Appendix.

In addition, the agency should further amend the Modified Text to align with existing California laws regulating the security of personal information. For example, the definition of “security incident” in the Modified Text should be revised to align with the existing definition of “security breach” in the California data breach notification law.⁵² The CCPA does not have the authority to rewrite the CCPA, which already cross-references that data breach reporting statute.⁵³

Further, the agency should revise the content required for cybersecurity audits to permit a risk-based approach that aligns with industry-recognized cybersecurity standards. The statutory text requires the agency to “define the scope of the audit” and develop a “process to ensure that audits are thorough and independent.”⁵⁴ Rather than develop California-specific standards, the agency should endorse a process through which businesses that satisfy the requirements of vetted, industry-standard frameworks informed by experience and use, such as

⁵⁰ See, e.g., *Dix v. Superior Court*, 807 P.2d 1063, 1072 (Cal. 1991) (“Where reasonably possible, we avoid statutory constructions that render particular provisions superfluous or unnecessary.”).

⁵¹ See California Privacy Protection Agency, *Initial Statement of Reasons on Updates to existing CCPA regulations; Cybersecurity Audits; Risk Assessments; Automated Decisionmaking Technology; and Insurance Companies*, 42, https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_isor.pdf.

⁵² Cal. Civ. Code § 1798.82(a).

⁵³ Cal. Civ. Code § 1798.150(a)(1) (referencing Section 1798.81.5 for the definition of personal information subject to the data breach private right of action).

⁵⁴ Cal. Civ. Code § 1798.185(a)(14)(A).

COVINGTON

SOC 2 Type 2, ISO Certifications, or the National Institute of Standards and Technology Cybersecurity Framework.

II. Harmonization And Interoperability Across Privacy Frameworks Not Only Is Consistent With The California APA But Also Mandated By Statute.

CalChamber agrees with the concerns voiced by the California Congressional Delegation and many other commenters that the regulations “risk creating a fractured regulatory landscape between California and the rest of the country” and place “less resourced companies at a competitive disadvantage.”⁵⁵ Importantly, neither the text of the CCPA nor the California Administrative Procedure Act (“California APA”) presents an obstacle to aligning the regulations to other U.S. state privacy frameworks to address these concerns.

The statements at the May Board meeting that the California APA’s clarity standard is the rationale for not harmonizing the regulations with other U.S. privacy frameworks are misplaced.⁵⁶ For a regulation to be valid, the California APA requires that it provides entities affected by them sufficient clarity, defined as information “written or displayed so that the meaning of regulations will be easily understood by those persons directly affected by them.”⁵⁷ APA regulations provide further detail that proposed regulations cannot be logically interpreted to have more than one meaning and must not “use[] terms which do not have meanings generally familiar to those ‘directly affected’ by the regulation.”⁵⁸ Significantly, clarity is not a requirement unique to the California APA. For example, the Colorado Administrative Procedure Act (“Colorado APA”) incorporates a substantially similar requirement that a regulation must be “clearly and simply stated so that its meaning will be understood by any party required to comply with the regulation.”⁵⁹ Accordingly, the California APA does not present a barrier to harmonizing standards across the Modified Text and other statutes, such as the Colorado Privacy Act.

⁵⁵ Letter from California Congressional Delegation to CPPA (Jan. 14, 2025), https://cppa.ca.gov/regulations/pdf/part4_all_comments_combined_redacted_oral_not_included.pdf.

⁵⁶ See, e.g., May 1, 2025 Board Meeting, 1:40–2:00, <https://youtu.be/k7ZqDxHQZpA>.

⁵⁷ Cal. Gov’t Code § 11349. See also Cal. Code Regs. tit. 1, § 16 (stating that a regulation is presumed to not comply with the “clarity” standard if any of the following conditions exist: “(1) the regulation can, on its face, be reasonably and logically interpreted to have more than one meaning;” “(2) the language of the regulation conflicts with the agency’s description of the effect of the regulation;” “(3) the regulation uses terms which do not have meanings generally familiar to those ‘directly affected’ by the regulation, and those terms are defined neither in the regulation nor in the governing statute;” “(4) the regulation uses language incorrectly;” “(5) the regulation presents information in a format that is not readily understandable by persons ‘directly affected;” or “(6) the regulation does not use citation styles which clearly identify published material cited in the regulation”).

⁵⁸ See Cal. Code Regs. tit. 1, § 16(a)(3); see also *Assoc. Gen. Contractors of California, Inc. v. Dept. of Industrial Relations*, 108 Cal. App. 5th 243 (Cal. App. 2025) (finding that the challenged regulations were substantially clear, in part because contractors will be able to comply with them either by using their own knowledge of the industry or by specifying the work processes to be performed).

⁵⁹ Colo. Rev. Stat. § 24-4-103.

COVINGTON

Indeed, harmonizing the requirements with other state privacy laws is consistent with the CCPA statute's intended goals. For example, risk assessment content requirements can be consistent with other jurisdictions and recognize that risk assessments completed under other jurisdictions' frameworks satisfy CCPA requirements if they are reasonably similar in scope and effect. Specifically, the statutory text requires the agency to issue regulations for businesses to "identify and weigh" the benefits of the processing against potential risks, which is nearly identical to the risk assessment content requirements in other U.S. privacy statutes, such as the Colorado Privacy Act.⁶⁰ Given the substantial overlap in statutory requirements for risk assessments, the Modified Text should conform to those requirements in the Colorado Privacy Act regulations and recognize that risk assessments completed under frameworks with "reasonably similar scope and effect" satisfy the CCPA.⁶¹ These terms and direction meet the California APA's "clarity" requirement, because these terms are already used in the CCPA regulations⁶² and are understood by businesses subject to the CCPA that are subject to other U.S. privacy frameworks that incorporate the same language.⁶³ Unless risk assessment content and the recognition of assessments completed under other frameworks are harmonized with other state privacy laws, businesses will be forced to undertake costly, duplicative paperwork for multiple laws that do not advance privacy interests of consumers.

Other proposed edits to the Modified Text promote interoperability across legal frameworks and satisfy the California APA's clarity requirement. For example:

- Risk-Based Cyber Audits That Recognize Industry Standards: Cybersecurity audits should be risk-based, consistent with industry standards⁶⁴ and other cybersecurity

⁶⁰ Compare Cal. Civ. Code 1798.185(a)(14)(B) ("identify[] and weigh[] the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the 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") with Colo. Rev. Stat. § 6-1-1309(3) ("Data protection assessments must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that the controller can employ to reduce the risks.").

⁶¹ The recognition that assessments completed under laws that are reasonably similar in scope and effect. See, e.g., Conn. Gen. Stat. § 42-522(e); Tenn. Code Ann. § 47-18-3206(e); Tex. Bus. & Comm. Code § 541.105(f).

⁶² For example, the existing CCPA regulations use the term "reasonably" thirty-one times.

⁶³ See *supra* note 54 and accompany text.

⁶⁴ Proposed edits in the Appendix include eliminating the onerous and unnecessary requirement that an individual make an attestation concerning the audit report under penalty of perjury. At an absolute minimum, this attestation must not include the assertion that "the business has not made any attempt to influence the auditor's decisions or assessment" because that assertion is diametrically opposed to generally accepted audit practices. Business stakeholders are *always* to be engaged if potential issues are identified to ensure a meeting of the minds when possible and the accuracy of the final report. See, e.g., *Global Internal Audit Standards™*, *The Institute of Internal Auditors, Inc.*, Standard 13.1 ("At the end of an engagement, if internal auditors and management do not agree on the engagement results, internal auditors must discuss and try to reach a mutual understanding of the issue with the management of the activity under review.").

COVINGTON

frameworks.⁶⁵ To allow businesses to allocate resources to protecting personal information rather than towards paperwork exercises, businesses should be permitted to conduct a full cybersecurity audit every three years with annual intervening audits and certifications of compliance.⁶⁶ Further, cybersecurity audits that adhere to guidance in NIST and similar industry standards should be recognized to comply with the CCPA.⁶⁷ Because the statute provides the agency discretion to “defin[e] the scope of the audit and establish a process to ensure that audits are thorough and independent”⁶⁸ and professionals conducting cybersecurity audit will be deeply familiar with risk-based audits and NIST frameworks, the agency can harmonize cybersecurity audit regulations in a way that is consistent with the statutory text and that satisfies the California APA requirements.

- Solely Automated Significant Decisions: The agency must amend the definition of ADMT to avoid a “complex patchwork of state regulations” that “discourage[s] entrepreneurialism.”⁶⁹ These changes are required by the California APA to avoid overreaching the statute,⁷⁰ and they also meet clarity requirements for those businesses affected by the regulation. Not only is the term “solely” already used in the CCPA

⁶⁵ See, e.g., 23 NYCRR §§ 500.1; 500.9 (defining risk assessment as “the process of identifying, estimating and prioritizing cybersecurity risks to organizational operations (including mission, functions, image and reputation), organizational assets, individuals, customers, consumers, other organizations and critical infrastructure resulting from the operation of an information system. Risk assessments incorporate threat and vulnerability analyses and consider mitigations provided by security controls planned or in place”); see also U.S. Dept. of Health & Human Servs., *Guidance on Risk Analysis* (outlining questions as “examples” that organizations could consider that are “not prescriptive and merely identify issues an organization may wish to consider”), <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es>.

⁶⁶ An intervening lighter-touch audit is consistent with the statutory requirement for businesses to “[p]erform a cybersecurity audit on an annual basis,” as the agency can determine the “scope of the audit” and require different degrees of audits for different purposes. Cal. Civ. Code § 1798.185(a)(14)(A). This approach has similarities with other frameworks. See 23 NYCRR § 500.17(b) (requiring annual certifications that the Covered Entity is in compliance with the regulations).

⁶⁷ Other regulators, including the U.S. Department of Health and Human Services (“HHS”), have recognized that adherence to nationally recognized security standards is indicative of a strong security posture. See, e.g., Public Law 116–321 (requiring HHS to “consider certain recognized security practices of covered entities and business associates when making certain determinations” regarding fines, audit results, or other remedies for resolving potential HIPAA violations, including whether the organization established standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities).

⁶⁸ Cal. Civ. Code § 1798.185(a)(14)(B).

⁶⁹ Letter from California Congressional Delegation to CPPA (Jan. 14, 2025), https://cppa.ca.gov/regulations/pdf/part4_all_comments_combined_redacted_oral_not_included.pdf.

⁷⁰ See Section I.A.

COVINGTON

regulations,⁷¹ but businesses separately have deep familiarity with the term from its use in other U.S. state privacy statutes.⁷²

- **Privilege & Confidentiality:** The Modified Text should be amended to recognize that risk assessments and cyber audits, including those materials provided to a regulator, do not weaken claims of attorney-client privilege or work product protection and are protected by confidentiality from public disclosure. Such a provision would be clear to affected businesses, as privilege and confidentiality are commonly understood terms, used by other U.S. privacy statutes, and already endorsed by the California legislature.⁷³

III. The Modified Text Imposes Significant Burden On California Businesses, Which Is Underestimated In The SRIA.

Multiple Board Members and commenters underscored that the cost of these three regulations – based on less than 25 lines of text in the entire 65 page CCPA statute – will exceed by multiples the cost of the rest of the CCPA statute combined.⁷⁴ These concerns are substantiated by the extensive evidence contained in Michael Genest’s memo submitted to the CPPA by CalChamber.⁷⁵ Rather than rushing to complete the rules by an arbitrary deadline,⁷⁶ the agency should update the SRIA to ensure that the actual cost of the Modified Text is fully understood to allow the Board to assess whether the right balance has been struck across the range of available alternatives for the regulatory text.⁷⁷

Notwithstanding the significant impact these regulations will have on the world’s fourth largest economy, the agency appears on the cusp of rushing the rulemaking forward to avoid missing an arbitrary, self-imposed November deadline rather than taking the time to update the SRIA to accurately assess the updated cost of the proposed regulations on businesses operating in California. Even assuming *arguendo* that the SRIA was correctly calculated, the agency’s \$3.5 billion projected costs to businesses in the first year⁷⁸ is 70 times the threshold for what

⁷¹ See CCPA Regulations §§ 7024(c)(2); 7101(e).

⁷² See, e.g., Conn. Gen. Stat. § 42-518.

⁷³ The California Age Appropriate Design Code contemplates that a business may conduct data protection impact assessments under attorney-client privilege, and businesses are not required to provide state authorities with these assessments unless specifically requested. See Cal. Civ. Code § 1798.99.31(a)(4).

⁷⁴ See April Board Meeting Transcript at 31 (noting that the proposed regulations stem from “two relatively tiny clauses in a 56-page bill”).

⁷⁵ See Letter from Michael Genest and Brad Williams, Capitol Matrix Consulting, to CalChamber (Nov. 1, 2024), https://advocacy.calchamber.com/wp-content/uploads/2024/11/CMC_comments_on_CCPA_SRIA_11-1.pdf.

⁷⁶ See April Board Meeting Transcript at 21 (“In order to meet our November deadline. . .”).

⁷⁷ *Id.* at 49 (“[H]ow are we really impacting people financially? So there’s – there’s more work to do.”).

⁷⁸ See Letter from Michael Genest and Brad Williams, Capitol Matrix Consulting, to CalChamber (Nov. 1, 2024), https://advocacy.calchamber.com/wp-content/uploads/2024/11/CMC_comments_on_CCPA_SRIA_11-1.pdf.

COVINGTON

California law considers a “major regulation.”⁷⁹ To account for the substantial costs of the regulation on businesses and the potential to meaningfully impact the California economy, CalChamber urges the agency to conduct an updated SRIA to make an informed assessment of the costs involved with the Modified Text’s proposals.

An updated SRIA is particularly important because – notwithstanding the changes made in the Modified Text – the costs of the regulations likely remain as high as the original SRIA amount of \$3.5 billion in the first year because the prior SRIA failed to (1) reflect the impact on out-of-state businesses subject to the CCPA, (2) accurately reflect the operational costs of cybersecurity audits and risk assessments, (3) account for technical and resource costs of ADMT opt-out and access rights, and (4) address the elements for a SRIA that are required under California law.

The Modified Text would impose significant costs on California businesses without countervailing benefits to consumers. For example, the work required to comply with the Modified Text’s requirements for overly broad and redundant ADMT opt-outs and assessments in the employment context, training, and pre-use notice requirements, would create extraordinary costs on businesses. The employee resources and time required for overly-prescriptive and inflexible risk assessments and cybersecurity audits would require costly personnel resources and meaningful opportunity costs in the form of diverting employees away from privacy- and security-enhancing operations. Further costs associated with the regulations also include hiring third parties to assist with or undertake these efforts, a dynamic that disproportionately burdens small- and medium-sized businesses who may require additional support to comply with the regulations’ prescriptive and idiosyncratic requirements. Importantly, the SRIA fails to account for these and other costs on out-of-state companies, as the SRIA only considers those businesses with employees in California. Consequently, CalChamber urges the agency to revise the SRIA and consider the full scope of costs on California businesses and the state before rushing forward regulations.

The Modified Text continues to levy on businesses and the state intangible opportunity costs. As identified in Michael Genest’s memo, the SRIA failed to address an element required under California law for the impact of proposed regulation on incentives for innovation.⁸⁰ For example, businesses deterred by the compliance requirements of implementing ADMT would bear the costs of lost productivity or benefits from not using technology. The Modified Text’s onerous requirements are also likely to stifle promising research in the areas of science, health care, transportation, or climate protection.⁸¹ Rather than rushing the Modified Text towards a

⁷⁹ See California Department of Finance, Major Regulations, <https://dof.ca.gov/forecasting/economics/major-regulations/> (stating that a major regulation has an economic impact exceeding \$50 million); see also April Board Meeting Transcript at 42–43, (reflecting Board Member Mactaggart’s comments that “three regulations vastly outweighs the cost of the entire bill by, like an order of magnitude . . . so I think we got to get this right”).

⁸⁰ Cal. Gov’t Code § 11346.3(c)(1)(E).

⁸¹ See Letter from Michael Genest and Brad Williams, , Capitol Matrix Consulting, to CalChamber (Nov. 1, 2024), https://advocacy.calchamber.com/wp-content/uploads/2024/11/CMC_comments_on_CCPA_SRIA_11-1.pdf.

COVINGTON

self-imposed deadline, the agency should consider the full scope of costs on the state and California businesses.

IV. The Modified Text Conflicts With Fundamental Constitutional Protections.

The Modified Text does not address all of commenters' constitutional concerns.

A. The Draft Regulations Raise Concerns Over Compelled Speech In Violation Of The First Amendment.

Proposed requirements in the Modified Text require revision to address tension with the First Amendment. The First Amendment protects against compelled speech, such as when the government requires companies to adopt a given policy.⁸² For example, the Ninth Circuit concluded in *X Corp. v. Bonta* that requirements for social media companies to prepare reports detailing content moderation practices require "insight into whether a social media company" considers certain factors in its content, which reflects "constitutionally protected speech" that the state cannot compel without satisfying strict scrutiny.⁸³

To address First Amendment protections, the CPPA must revise the Modified Text, including by addressing the following:

- The Modified Text's risk assessments compel speech and do not satisfy strict scrutiny. Risk assessments reflect judgments by the business, including (for example) on risks and appropriate safeguards. Even assuming that these requirements further a compelling government interest, their breadth and lack of flexibility make clear that they lack narrow tailoring.
- The cybersecurity audits raise similar compelled speech concerns. Numerous aspects of the cybersecurity audit and audit report reflect the business's judgment, such as the cybersecurity audit report's requirement to address plans to address gaps and weaknesses and the status of gaps or weaknesses of certain policies and procedures.⁸⁴
- The prescriptive ADMT pre-use notice compels speech by requiring the disclosure of detailed information about business plans and operations. For example, disclosures about how an ADMT output is used to make a significant decision and what factors the

⁸² See *Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc.*, 570 U.S. 205 (2013) (holding that a law violated the First Amendment where it conditioned funding for certain organizations on their adopting a particular "policy" opposing prostitution). The Supreme Court has articulated three basic steps to assessing a compelled speech claim. *First*, the court considers whether the challenged law compels "speech as speech," or whether it only incidentally compels speech as part of regulating conduct. *Nat'l Inst. of Fam. & Life Advoc. v. Becerra* ("NIFLA"), 585 U.S. 755, 770 (2018). If the former, then the law implicates the First Amendment; if the latter, it may still implicate the First Amendment if the conduct is inherently expressive. See *Rumsfeld v. F. for Acad. & Institutional Rts., Inc.*, 547 U.S. 47, 62, 65–66 (2006). *Second*, if the law implicates the First Amendment, then the court must determine what level of scrutiny applies. Laws that compel speech ordinarily receive strict scrutiny, meaning that they must be narrowly tailored to serve a compelling state interest. See *NIFLA*, 585 U.S. at 766. *Finally*, the court decides whether the law is constitutional under the applicable scrutiny standard.

⁸³ *X Corp. v. Bonta*, 116 F.4th 888, 902 (9th Cir. 2024).

⁸⁴ Modified Text § 7123(e).

COVINGTON

business consults in reaching a significant decision reflect judgments by the business about its operations and use of technologies.⁸⁵

- Information required by the business in response to an ADMT access right also compel constitutionally protected speech. In response to a verified consumer ADMT access request, the business would be required to explain the outcome of a decisionmaking process.⁸⁶ The breadth of the required disclosures with respect to individual consumers underscores that the requirements would fail strict scrutiny.

B. Sections Of the Modified Text Are Preempted By Federal Law.

The agency must revise the Modified Text because it seeks to regulate areas that are preempted by federal law in violation of the Supremacy Clause of the U.S. Constitution⁸⁷ or that conflict with federal law.⁸⁸ As noted in our prior submission, the Defend Trade Secrets Act protects business trade secrets, which the agency cannot abrogate. Nevertheless, the Modified Text requires a business to disclose business sensitive and trade secret-protected details, such as a plain language explanation of the “logic of the ADMT” for an ADMT access request.⁸⁹ Additionally, the recognition that certain information need not be disclosed if it implicates a trade secret was not added to the section on ADMT opt-outs.⁹⁰

C. Terms And Concepts In The Modified Text Are Impermissibly Vague.

Both the federal and California Due Process Clause prohibit the enforcement of laws – including administrative rules – that are so vague that they do not give fair notice to the public regarding the conduct being regulated.⁹¹ Because numerous provisions in the Modified Text “fail[] to provide a person of ordinary intelligence fair notice of what is prohibited, or [are] so standardless that it authorizes or encourages seriously discriminator enforcement,”⁹² they require significant revisions. These constitutional infirmities include the following:

⁸⁵ See, e.g., Modified Text § 7220.

⁸⁶ See, e.g., Modified Text § 7222(b).

⁸⁷ The Supremacy Clause prohibits states from regulating conduct “in a field that Congress, acting within its proper authority, has determined must be regulated by its exclusive governance.” *Arizona v. United States*, 567 U.S. 387, 399 (2012).

⁸⁸ State laws are preempted where they stand “as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress.” See *Mik v. Fed. Home Loan Mortg. Corp.*, 743 F.3d 149, 165 (6th Cir. 2014) (holding that a federal statute with similar saving clause for state laws providing greater protection for tenants preempted a state law that was less protective of tenants because it presented an obstacle to the federal law’s objective of ensuring that tenants have notice of foreclosure).

⁸⁹ Modified Text § 7222(b)(2).

⁹⁰ Modified Text § 7221.

⁹¹ A “fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required.” *F.C.C. v. Fox Television Stations, Inc.*, 567 U.S. 239, 253–55 (2012).

⁹² *Id.* (quotation marks and citation omitted). Additionally, well-settled California law reflects similar concerns and standards for unconstitutional vagueness. See *Teichert Constr. v. California Occupational* (continued...)

COVINGTON

- ADMT disclosure requirements are broad and unclear, such as the requirement to disclose “[a]dditional information about how the ADMT works to make a significant decision,” without direction as to what such additional information would entail and types of outputs generated.⁹³
- The Modified Text requires risk assessments where the business “intends to use” personal information to train ADMT, but it is unclear what degree of planning reflects “intent” to determine when risk assessments would be required.⁹⁴

V. The Modified Text Must Be Amended To Provide Businesses With Time To Enter Into Compliance.

The timing requirements must be amended to address the practical difficulties presented by the Modified Text. First, the risk assessment timing requirements conflict and lack foundation in practice. Risk assessments would be required to be completed prior to December 31, 2027 for activities initiated prior to the effective date that continue following the effective date.⁹⁵ However, new processing activities will require a risk assessment prior to being initiated, and risk assessments must be updated in no more than 45 days if there is a material change to the processing activity.⁹⁶ The Modified Text separately imposes restrictions on new processing activities until a risk assessment is done, even though the risk assessment is not due until December 31, 2027. Accordingly, the Modified Text should be revised to make clear the requirements for processing activities engaged in before the date on which risk assessments begin, for new processing activities initiated after that date, and material changes.

Additionally, even assuming the regulations are finalized by the end of 2025, the Modified Text provides businesses little time to enter into compliance. The requirements in the regulations have changed substantially over the course of the rulemaking process, and the proposed requirements will demand substantial time and engineering resources. For example, the scope of the ADMT opt-out has evolved significantly, even in the last month, and will require business resources to design and implement the opt-out. Accordingly, and to allow businesses with sufficient time to come into compliance with the requirements reflected in the Modified Text, the agency must update all timelines, including for provisions in the regulations that modify existing privacy regulations, to enter into effect 24 months after the regulations are finalized.

Safety & Health Appeals Bd., 140 Cal. App. 4th 883, 890–91 (2006) (noting that a “statute violates due process of law if it forbids or requires the doing of an act in terms so vague that persons of common intelligence must necessarily guess at its meaning and differ as to its application”).

⁹³ See, e.g., Modified Text §7220(c)(5).

⁹⁴ Modified Text § 7150(b)(6).

⁹⁵ Modified Text § 7155(b).

⁹⁶ Modified Text § 7155(a)(3).

COVINGTON

CalChamber appreciates the CPPA's consideration of these comments, and we look forward to continuing to work with the agency on these important issues.

Sincerely,



Lindsey Tonsager
Jayne Ponder
Olivia Vega
Counsel for CalChamber

APPENDIX

MODIFIED TEXT OF PROPOSED REGULATIONS

TITLE 11. LAW

DIVISION 6. CALIFORNIA PRIVACY PROTECTION AGENCY CHAPTER 1. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS

The original text published in the California Code of Regulations has no underline. The initial proposal (noticed on November 22, 2024) is illustrated by blue underline for proposed additions and ~~red strikethrough~~ for proposed deletions, unless otherwise indicated, as in Articles 9, 10, and 11. Changes made after the 45-day comment period are illustrated by purple double underline for proposed additions and ~~orange double strikethrough~~ for proposed deletions

CalChamber's proposed changes are **bolded** and highlighted in **yellow text**.

ARTICLE 1. GENERAL PROVISIONS

§ 7001. Definitions.

In addition to the definitions set forth in Civil Code section 1798.140, for purposes of these regulations:

- (a) "Agency" means the California Privacy Protection Agency established by Civil Code section 1798.199.10 et seq.
- (b) "Alternative Opt-out Link" means the alternative opt-out link that a business may provide instead of posting the **two** separate "Do Not Sell or Share My Personal Information," **and** "Limit the Use of My Sensitive Personal Information," **and ADMT opt-out** links as set forth in Civil Code section 1798.135, subdivision (a)(3), and specified in section **s 7015 and 7221.**
- ~~(c) "Artificial intelligence" means a machine based system that infers, from the input it receives, how to generate outputs that can influence physical or virtual environments. The artificial intelligence may do this to achieve explicit or implicit objective. Outputs can include predictions, contents, recommendations, or decisions. Different artificial intelligence varies in it levels of autonomy and adaptiveness after deployment. For example, artificial intelligence includes generative models, such as large language models, that can learn from inputs and create new outputs, such as text, images, audio, or video; and facial or speech recognition or detection technology.~~
- (c) ~~(d)~~ ~~(e)~~ "Attorney General" means the California Attorney General or any officer or employee of the California Department of Justice acting under the authority of the California Attorney General.
- (d) ~~(e)~~ ~~(d)~~ "Authorized agent" means a natural person or a business entity that a consumer has authorized to act on their behalf subject to the requirements set forth in section 7063.

(e) (4) "Automated decisionmaking technology" or "ADMT" means **any solely automated technology that processes personal information and uses computation to make a ~~to execute a decision~~ significant decision about a consumer, ~~replace human decisionmaking, or substantially replace~~ facilitate human decisionmaking.**

~~(1) For purposes of this definition, "technology" includes software or programs, including those derived from machine learning, statistics, other data processing techniques, or artificial intelligence.~~

~~(2) **For purposes of this definition, to "substantially replace" facilitate human decisionmaking" means a business uses the technology's output to make a decision without human involvement, using the output of the technology as a key factor in a human's decisionmaking. This includes, for example, using automated decisionmaking technology to generate a score about a consumer that the human reviewer uses as a primary factor to make a significant decision about them. Human involvement requires the human reviewer to:**~~

~~**(A) Know how to interpret and use the technology's output to make the decision;**~~

~~**(B) Review and analyze the output of the technology, and any other information that is relevant to make or change the decision; and**~~

~~**(C) Have the authority to make or change the decision based on their analysis in subsection (B).**~~

~~(2) (2) Automated decisionmaking technology **ADMT includes profiling;**~~

~~(3) (4) Automated decisionmaking technology ADMT does not include the following technologies, provided that the technologies do not execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking web hosting, domain registration, networking, caching, website-loading, data storage, firewalls, anti-virus, anti-malware, spam- and robocall-filtering, spellchecking, calculators, databases, search term software, and spreadsheets; provided that they do not replace human decisionmaking or similar technologies. A business must not use these technologies to circumvent the requirements for automated decisionmaking technology set forth in these regulations. For example, a business's use of a spreadsheet to run regression analyses on its top performing managers' personal information to determine their common characteristics, and then to find co-occurrences of those characteristics among its more junior employees to identify which of them it will promote is a use of automated decisionmaking technology, because this use is replacing human decisionmaking. By contrast, a manager's use of a spreadsheet to input junior employees' performance evaluation scores from their managers and colleagues and then calculate each employee's final score that the manager will use to determine~~

~~which of them will be promoted is not a use of automated decisionmaking technology, because the manager is using the spreadsheet merely to organize human decisionmakers' evaluations.~~

~~(g) "Behavioral advertising" means the targeting of advertising to consumer based on the consumer's personal information obtained from the consumer's activity both across businesses, distinctly branded websites, applications, or services, and within the business's own distinctly branded websites, applications, or services.~~

~~(1) Behavioral advertising includes cross-context behavioral advertising.~~

~~(2) Behavioral advertising does not include nonpersonalized advertising, as defined by Civil Code section 1798.140, subdivision (t), provided that the consumer's personal information is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business, and is not disclosed to a third party.~~

(f) ~~(h)~~ ~~(e)~~ "Categories of sources" means types or groupings of persons or entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity. They may include the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

(g) ~~(h)~~ ~~(f)~~ "Categories of third parties" means types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party. They may include advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

(h) ~~(i)~~ ~~(g)~~ "CCPA" means the California Consumer Privacy Act of 2018, Civil Code section 1798.100 et seq.

(i) ~~(h)~~ ~~(h)~~ "COPPA" means the Children's Online Privacy Protection Act, 15 U.S.C. sections 6501 to 6506 and 16 Code of Federal Regulations part 312.

(j) ~~(h)~~ "Cybersecurity audit" means the **annual** cybersecurity audit that every business whose processing of consumers' personal information presents significant risk to consumers' security as set forth in section 7120, subsection (b), is required to complete.

(k) ~~(h)~~ "Cybersecurity program" means the policies, procedures, and practices that protect personal information from unauthorized access, destruction, use, modification, or disclosure; and protect against unauthorized activity resulting in the loss of availability of personal information.

- (i) "Cybersecurity audit report" means the document that every business must create as part of its cybersecurity audit. The cybersecurity audit report includes the information set forth in section 7123, subsection (e).
- ~~(n) "Deepfake" means manipulated or synthetic audio, image, or video content that depicts a consumer saying or doing things they did not say or do and that are presented as truthful or authentic without the consumer's knowledge and permission.~~
- (m) ~~(e)~~ ~~(i)~~ "Disproportionate effort" within the context of a business, service provider, contractor, or third party responding to a consumer request means the time and/or resources expended by the business, service provider, contractor, or third party to respond to the individualized request significantly outweighs the reasonably foreseeable impact to the consumer by not responding, taking into account applicable circumstances, such as the size of the business, service provider, contractor, or third party, the nature of the request, and the technical limitations impacting their ability to respond. For example, responding to a consumer request to know may require disproportionate effort when the personal information that is the subject of the request is not in a searchable or readily-accessible format, is maintained only for legal or compliance purposes, is not sold or used for any commercial purpose, and there is no reasonably foreseeable material impact to the consumer by not responding. By contrast, the impact to the consumer of denying a request to correct inaccurate information that the business uses and/or sells may outweigh the burden on the business, service provider, contractor, or third party in honoring the request when the reasonably foreseeable consequence of denying the request would be the denial of services or opportunities to the consumer. A business, service provider, contractor, or third party that has failed to put in place adequate processes and procedures to receive and process consumer requests in accordance with the CCPA and these regulations cannot claim that responding to a consumer's request requires disproportionate effort.
- (n) ~~(e)~~ ~~(i)~~ "Employment benefits" means retirement, health, and other benefit programs, services, or products to which consumers and their dependents or their beneficiaries receive access through the consumer's employer.
- (o) ~~(e)~~ ~~(k)~~ "Employment-related information" means personal information that is collected by the business about a natural person for the reasons identified in Civil Code section 1798.145, subdivision (m)(1). The collection of employment-related information, including for the purpose of administering employment benefits, shall be considered a business purpose.
- (p) ~~(e)~~ ~~(t)~~ "Financial incentive" means a program, benefit, or other offering, including payments to consumers, for the collection, retention, sale, or sharing of personal information. Price or service differences are types of financial incentives.
- (q) ~~(s)~~ ~~(m)~~ "First party" means a consumer-facing business with which the consumer intends and expects to interact.

- (r) ~~(t)~~ ~~(n)~~ "Frictionless manner" means a business's processing of an opt-out preference signal that complies with the requirements set forth in section 7025, subsection (f).
- (s) ~~(u)~~ ~~(e)~~ "Information practices" means practices regarding the collection, use, disclosure, sale, sharing, and retention of personal information.
- (t) ~~(w)~~ "Information system" means the resources (e.g., network, hardware, and software) organized for the processing of personal information or that can provide access to, ~~including the collection, use, disclosure, sale, sharing, and retention of~~ personal information. The business's information system includes the resources organized for the business's processing of personal information, regardless of whether the business owns those resources.
- (u) **"Intervening cybersecurity audit" means the risk-based cybersecurity audit accounting for any materially updated conditions that both affect the processing of personal information and present significant risk to consumer security as set forth in section 7120, subsection (b).**
- (v) ~~(w)~~ "Multi-factor authentication" means authentication through verification of at least two of the following types of authentication factors: (1) knowledge factors, such as a password; (2) possession factors, such as a token; or (3) inherence factors, such as a biometric characteristic.
- (w) ~~(x)~~ ~~(p)~~ "Nonbusiness" means a person or entity that does not meet the definition of a "business" as defined in Civil Code section 1798.140, subdivision (d). For example, ~~non-~~ ~~profits and~~ government entities and many non-profits are nonbusinesses because ~~one~~ ~~definition of "business" is defined, among other things, to include only required entities~~ ~~to be~~ they are not "organized or operated for the profit or financial benefit of its shareholders or other owners."
- (x) ~~(y)~~ ~~(q)~~ "Notice at Collection" means the notice given by a business to a consumer at or before the point at which a business collects personal information from the consumer as required by Civil Code section 1798.100, subdivisions (a) and (b), and specified in these regulations.
- (y) ~~(z)~~ ~~(r)~~ "Notice of Right to Limit" means the notice given by a business informing consumers of their right to limit the use or disclosure of the consumer's sensitive personal information as required by Civil Code sections 1798.121 and 1798.135 and specified in these regulations.
- (z) ~~(aa)~~ ~~(s)~~ "Notice of Right to Opt-out of Sale/Sharing" means the notice given by a business informing consumers of their right to opt-out of the sale or sharing of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in these regulations.

(aa) ~~(bb)~~ ~~(t)~~ "Notice of Financial Incentive" means the notice given by a business explaining each financial incentive or price or service difference as required by Civil Code section 1798.125, subdivision (b), and specified in these regulations.

(bb) ~~(ee)~~ ~~(u)~~ "Opt-out preference signal" means a signal that is sent by a platform, technology, or mechanism, on behalf of the consumer, that communicates the consumer choice to opt-out of the sale and sharing of personal information and that complies with the requirements set forth in section 7025, subsection (b).

(cc) ~~(dd)~~ "Penetration testing" means testing the security of an information system by attempting to circumvent or defeat its security features by authorizing attempted penetration of the information system.

~~(cc)~~ ~~(ee)~~ "Performance at work" means the performance of job duties for which the consumer has been hired or has applied to be hired. The following are not "performance at work": a consumer's union membership or interest in unionizing; a consumer's interest in seeking other employment opportunities; a consumer's location when off duty or on breaks; or a consumer's use of a personal account (e.g., email, text messages, or social media) unless solely to prevent or limit the use of these accounts on the business's information system or to prevent the disclosure of confidential information.

~~(dd)~~ ~~(ff)~~ "Performance in an educational program" means the performance of coursework in an educational program in which the consumer is enrolled or has applied to be enrolled. The following are not "performance in an educational program": a consumer's use of a personal account (e.g., email, text messages, or social media) unless solely to prevent or limit the use of these accounts on the educational program provider's information system, including to prevent the disclosure of confidential information or to prevent cheating; or a consumer's location when they are not performing coursework.

~~(ee)~~ ~~(gg)~~ "Physical or biological identification or profiling" means identifying or profiling a consumer using information that depicts or describes automated measurements or analysis of their physical or biological characteristics, or automated measurements or analysis of or relating to their body. This includes using biometric information, vocal intonation, facial expression, and gesture (e.g., to identify or infer emotion). This does not include processing physical or biological characteristics that do not identify, and cannot reasonably be linked with, a particular consumer.

(ff) ~~(hh)~~ ~~(v)~~ "Price or service difference" means (1) any difference in the price or rate charged for any goods or services to any consumer related to the collection, retention, sale, or sharing of personal information, or (2) any difference in the level or quality of any goods or services offered to any consumer related to the collection, retention, sale, or sharing of personal information, including the denial of goods or services to the consumer.

~~(gg)~~ ~~(ii)~~ ~~(w)~~ "Privacy policy," as referred to in Civil Code sections 1798.130, subdivision (a)(5), and 1798.135, subdivision (c)(2), means the statement that a business shall make available to consumers describing the business's online and offline information practices, and the rights of consumers regarding their own personal information.

~~(hh)~~ ~~(ii)~~ "Privileged account" means any authorized user account (i.e., an account designed to be used by an individual) or service account (i.e., an account designed to be used only by a service, not by an individual) that can be used to perform functions that other user accounts are not authorized to perform, including but not limited to the ability to add, change, or remove other accounts, or make configuration changes to an information system.

~~(ii)~~ ~~(kk)~~ "Profiling" means any form of **solely** 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,; healthy,; **(including mental health),;** personal preferences, interests, reliability, **predispositions,** behavior, location, or movements.

~~(ll)~~ "Publicly accessible place" means a place that is open to or serves the public. Examples of publicly accessible places include shopping malls, stores, restaurants, cafes, movie theaters, amusement parks, convention centers, stadiums, gymnasiums, hospitals, medical clinics or offices, transportation depots, transit, streets, or parks.

~~(jj)~~ ~~(mm)~~ "Request to access ADMT" means a consumer request that a business provide information to the consumer about the business's use of **automatic decisionmaking technology ADMT with respect to the consume to process personal information,** pursuant to Civil Code section 1798.185(a)(15) and Article 1144 **of these regulations.**

~~(kk)~~ ~~(nn)~~ "Request to appeal ADMT" means a consumer request to appeal the business's **use of automatic decisionmaking technology ADMT for a significant decision as set forth in section 7221, subsection (b)(2).**

~~(ll)~~ ~~(oo)~~ ~~(x)~~ "Request to correct" means a consumer request that a business correct inaccurate personal information that it maintains about the consumer, pursuant to Civil Code section 1798.106.

~~(mm)~~ ~~(pp)~~ ~~(y)~~ "Request to delete" means a consumer request that a business delete personal information about the consumer that the business has collected from the consumer, pursuant to Civil Code section 1798.105.

~~(nn)~~ ~~(qq)~~ ~~(z)~~ "Request to know" means a consumer request that a business disclose personal information that it has collected about the consumer pursuant to Civil Code sections 1798.110 or 1798.115. It includes a request for any or all of the following:

- (1) Specific pieces of personal information that a business has collected about the consumer;
- (2) Categories of personal information it has collected about the consumer;
- (3) Categories of sources from which the personal information is collected;
- (4) Categories of personal information that the business sold, shared, or disclosed for a business purpose about the consumer;
- (5) Categories of third parties to whom the personal information was sold, shared, or disclosed ~~for a business purpose~~; and
- (6) The business or commercial purpose for collecting, ~~or~~ selling, or sharing personal information.

(oo) ~~(ff)~~ ~~(aa)~~ "Request to limit" means a consumer request that a business limit the use and disclosure of the consumer's sensitive personal information, pursuant to Civil Code section 1798.121, subdivision (a).

(pp) ~~(ss)~~ ~~(bb)~~ "Request to opt-in to sale/sharing" means an action demonstrating that the consumer has consented to the business's sale or sharing of personal information about the consumer by a parent or guardian of a consumer less than 13 years of age or by a consumer at least 13 years of age.

(qq) ~~(tt)~~ "Request to opt-out of ADMT" means a consumer request that a business not use automated decisionmaking technology ADMT with respect to the consumer, pursuant to Civil Code section 1798.185(a)(15) and Article 11 of these regulations.

(rr) ~~(uu)~~ ~~(cc)~~ "Request to opt-out of sale/sharing" means a consumer request that a business neither sell nor share the consumer's personal information to third parties, pursuant to Civil Code section 1798.120, subdivision (a).

(ss) ~~(vv)~~ "Right to access ADMT" means a consumer's right to request that a business provide information to the consumer about the business's use of personal information for automated decisionmaking technology ADMT with respect to the consumer as set forth in Civil Code section 1798.185(a)(15) and Article 11 of these regulations.

(tt) ~~(ww)~~ ~~(dd)~~ "Right to correct" means the consumer's right to request that a business correct inaccurate personal information that it maintains about the consumer as set forth in Civil Code section 1798.106.

(uu) ~~(xx)~~ ~~(ee)~~ "Right to delete" means the consumer's right to request that a business delete any personal information about the consumer that the business has collected from the consumer as set forth in Civil Code section 1798.105.

(vv) ~~(yy)~~ ~~(ff)~~ "Right to know" means the consumer's right to request that a business disclose personal information that it has collected, sold, or shared about the consumer as set forth in Civil Code sections 1798.110 and 1798.115.

(ww) ~~(zz)~~ ~~(gg)~~ "Right to limit" means the consumer's right to request that a business limit the use and disclosure of a consumer's sensitive personal information as set forth in Civil Code section 1798.121.

(xx) ~~(aaa)~~ "Right to opt-out of ADMT" means a consumer's right to direct that a business not use ~~automated decisionmaking technology~~ ADMT with respect to the consumer as set forth in Civil Code section 1798.185(a)(15) and Article 11 ~~of these regulations~~.

(yy) ~~(bbb)~~ ~~(hh)~~ "Right to opt-out of sale/sharing" means the consumer's right to direct a business that sells or shares personal information about the consumer to third parties to stop doing so as set forth in Civil Code section 1798.120.

(zz) "Risk assessment report" means the document that every business that is required to conduct a risk assessment must create as part of its risk assessment. The risk assessment report includes the information set forth in section 7152, subsections (a)(1)-(3), (6)-(9).

~~(aaa)~~ "Sensitive location" means 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.

~~(bbb)~~ ~~(eee)~~ "Sensitive personal information" means:

(1) Personal information that reveals:

- (A) A consumer's social security, driver's license, state identification card, or passport number.
- (B) A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.
- (C) A consumer's precise geolocation.
- (D) A consumer's racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership.
- (E) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.

(F) A consumer's genetic data.

(G) A consumer's neural data, which means information that is generated by measuring the activity of a consumer's central or peripheral nervous system, and that is not inferred from nonneural information.

(2) The processing of biometric information for the purpose of uniquely identifying a consumer.

(3) Personal information collected and analyzed concerning a consumer's health, sex life, or sexual orientation.

(4) Personal information of consumers that the business has actual knowledge are less than 16 years of age. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age.

Sensitive personal information does not include information that is "publicly available" pursuant to Civil Code section 1798.140, subdivision (v)(2).

(ccc) ~~(ddd) (ii)~~ "Signed" means that the written attestation, declaration, or permission has either been physically signed or provided electronically in accordance with the Uniform Electronic Transactions Act, Civil Code section 1633.1 et seq.

(ddd) "Significant decision" means a **material legal** decision that results in the provision or denial **to a consumer** of financial or lending services, housing, education enrollment or opportunities, **employment or independent contracting opportunities or compensation**, or healthcare services **to a consumer**. For purposes of this definition:

(1) "Financial or lending services" means the extension of credit or a loan, transmitting or exchanging funds, the provision of deposit or checking accounts, check cashing, or installment payment plans.

(2) "Housing" means any building, structure, or portion thereof that is used or occupied as, or designed, arranged, or intended to be used or occupied as, a home, residence, or sleeping place by one or more consumers including for permanent or temporary occupancy. The use of ADMT that provides or denies housing to a consumer based solely on the availability or vacancy of the housing or the successful receipt of payment for housing from the consumer is not making a significant decision.

(3) "Education enrollment or opportunities" means:

(A) Admission or acceptance into academic or vocational programs;

(B) Educational credentials (e.g., a degree, diploma, or certificate); and

(C) Suspension and expulsion.

(4) "Employment or independent contracting opportunities or compensation" means:

(A) Hiring;

(B) Allocation or assignment of work for employees; or salary, hourly or per assignment compensation, incentive compensation such as a bonus, or another benefit ("allocation/assignment of work and compensation");

(C) Promotion; and

(D) Demotion, suspension, and termination.

(5) "Healthcare services" means services related to the diagnosis, prevention, or treatment of human disease or impairment, ~~or the assessment or care of an individual's health.~~

(6) Significant decision does not include advertising to a consumer.

(eee) "Systematic observation" means methodical and regular or continuous observation. This includes, for example, methodical and regular or continuous observation using Wi-Fi or Bluetooth tracking, radio frequency identification, drones, video or audio recording or live streaming, technologies that enable physical or biological identification or profiling; and geofencing, location trackers, or license plate recognition.

(fff) ~~"Train automated decisionmaking technology or artificial intelligence" for the purposes of sections 7150, subsection (b)(6), and 7153 means the process through which automated decisionmaking a technology or artificial intelligence discovers underlying patterns, learns a series of actions, or is taught to generate a desired output. Examples of training include adjusting the parameters of an algorithm used for ADMT-automated decisionmaking technology or artificial intelligence, improving the algorithm that determines how a machine learning model learns, and iterating the datasets fed into ADMT-automated decisionmaking technology or artificial intelligence.~~

(ggg) (jjj) "Third-party identity verification service" means a security process offered by an independent third party that verifies the identity of the consumer making a request to the business. Third-party identity verification services are subject to the requirements set forth in Article 5 regarding requests to delete, requests to correct, or requests to know.

~~(hhh)~~ ~~(kk)~~ "Unstructured" as it relates to personal information means personal information that is not organized in a pre-defined manner and could not be retrieved or organized in a pre-defined manner without disproportionate effort on behalf of the business, service provider, contractor, or third party.

~~(iii)~~ ~~(H)~~ "Value of the consumer's data" means the value provided to the business by the consumer's data as calculated under section 7081.

~~(iii)~~ (mm) "Verify" means to determine that the consumer making a request to delete, request to correct, ~~or~~ request to know, or request to access ADMT is the consumer about whom the business has collected information, or if that consumer is less than 13 years of age, the consumer's parent or legal guardian.

~~(kkk) "Zero trust architecture" means denying access to an information system and the information that it processes by default, and instead explicitly granting and enforcing only the minimal access required. Zero trust architecture is based upon the acknowledgment that threats exist both inside and outside of a business's information system, and it avoids~~

ARTICLE 8. TRAINING AND RECORD-KEEPING

§ 7102. Requirements for Businesses Collecting Large Amounts of Personal Information.

- (a) A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, shares, or otherwise makes available for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall:
- (1) Compile the following metrics for the previous calendar year:
- (A) The number of requests to delete that the business received, complied with in whole or in part, and denied;
 - (B) The number of requests to correct that the business received, complied with in whole or in part, and denied;
 - (C) The number of requests to know that the business received, complied with in whole or in part, and denied;
 - (D) ~~The number of requests to access ADMT that the business received, complied with in whole or in part, and denied;~~
 - (E) The number of requests to opt-out of sale/sharing that the business received, complied with in whole or in part, and denied;
 - (F) The number of requests to limit that the business received, complied with in whole or in part, and denied;
 - (G) ~~The number of requests to opt-out of ADMT that the business received, complied with in whole or in part, and denied; and~~
 - (H) The median or mean number of days within which the business substantively responded to requests to delete, requests to correct, requests to know, requests to opt-out of sale/sharing, and requests to limit.
- (2) Disclose, by July 1 of every calendar year, the information compiled in subsection (a)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy. In its disclosure, a business may choose to disclose the number of requests that it denied in whole or in part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds.
- (b) A business may choose to compile and disclose the information required by subsection (a)(1) for requests received from all individuals, rather than requests received from

consumers. The business shall state whether it has done so in its disclosure and shall, upon request, compile and provide to the Attorney General the information required by subsection (a)(1) for requests received from consumers.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135 and 1798.185, Civil Code.

Adopt all of the text in the following Article:

ARTICLE 9. CYBERSECURITY AUDITS

§ 7120. Requirement to Complete a Cybersecurity Audit **and Intervening Cybersecurity Audit.**

- (a) Every business whose processing of consumers' personal information presents significant risk to consumers' security as set forth in subsection (b) must complete a cybersecurity audit **or intervening cybersecurity audit.**
- (b) A business's processing of consumers' personal information presents significant risk to consumers' security if **any of** the following is true:
 - (1) **The processing involves sensitive personal information for purposes other than those in subsection 7027(m)(1)-(8); and The business meets the threshold set forth in Civil Code section 1798.140, subdivision (d)(1)(C), in the preceding calendar year; or**
 - (2) **The processing presents a significant risk of harm to consumers considering the following factors:**
 - (A) **The size of the business;**
 - (B) **The complexity of the business;**
 - (C) **The nature of the processing activities; and**
 - (D) **The scope of processing activities.**

~~The business meets the threshold set forth in Civil Code section 1798.140, subdivision (d)(1)(A); and~~

 - (E) **~~Processed the personal information of 250,000 or more consumers or households in the preceding calendar year; or~~**
 - (F) **~~Processed the sensitive personal information of 50,000 or more consumers in the preceding calendar year.~~**

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7121. Timing Requirements for Cybersecurity Audits.

- (a) Before April 1, 2030, a business must complete its first cybersecurity audit report no later than:
 - (1) April 1, 2028, if the business's annual gross revenue for 2026 was more than one hundred million dollars (\$100,000,000) as of January 1, 2027. The business's audit would cover the period

from January 1, 2027, through January 1, 2028.

- (2) April 1, 2029, if the business's annual gross revenue for 2027 was between fifty million dollars (\$50,000,000) and one hundred million dollars (\$100,000,000) as of January 1, 2028. The business's audit would cover the period from January 1, 2028, through January 1, 2029.
- (3) April 1, 2030, if the business's annual gross revenue for 2028 was less than fifty million dollars (\$50,000,000). The business's audit would cover the period from January 1, 2029, through January 1, 2030.

(b) **Every three years after the completion of the business's first cybersecurity audit report, the business must conduct a cybersecurity audit that satisfies the requirements of sections 7122 and 7123.**

(c) **For each of the two years that follows a cybersecurity audit, the business must conduct an intervening cybersecurity audit.**

~~(a) A business has 24 months from the effective date of these regulations to complete its first cybersecurity audit in compliance with the requirements in this Article.~~

~~(d) After the business completes its first cybersecurity audit pursuant to subsection (a), its subsequent cybersecurity audits must be completed every calendar years, and there must be no gap in the months covered by successive cybersecurity audits.~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7122. Thoroughness and Independence of Cybersecurity Audits.

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

(1) To be qualified, an auditor must have knowledge of cybersecurity and how to audit a business's cybersecurity program.

(2) The auditor may be internal or external to the business but must exercise objective and impartial judgment on all issues within the scope of the cybersecurity audit, must be free to make decisions and assessments without influence by the business being audited, including the business's owners, managers, or employees; and must not participate in activities that may compromise, ~~or appear to compromise,~~ the auditor's independence. For example, the auditor must not participate in the business activities that the auditor may assess in the current or subsequent cybersecurity audits, including

developing procedures, preparing the business's documents, ~~or~~ making recommendations regarding, the business's cybersecurity program (separate from articulating audit findings), or implementing, or maintaining the business's cybersecurity program.

- (3) If a business uses an internal auditor, to maintain the auditor's independence, the highest-ranking auditor must report ~~regarding cybersecurity audit issues~~ directly to ~~the business's board of directors or governing body, not to business management that has direct responsibility for the business's cybersecurity program. If no such board or equivalent body exists, the internal auditor must report to the business's highest ranking~~ a member of the business's executive management team who could include the business's Chief Information Security Officer that does not have direct responsibility for the business's cybersecurity program. A member of the business's executive management team who does not have direct responsibility for the business's cybersecurity program must conduct the highest-ranking auditor's performance evaluation, if any, and determine the auditor's compensation.
- (b) ~~To enable the auditor to determine the scope of the cybersecurity audit and the criteria the cybersecurity audit will evaluate, t~~ the business must make available to the auditor all information in the business's possession, custody, or control that the auditor requests as relevant to the cybersecurity audit (e.g., information about the business's cybersecurity program and information system and the business's use of service providers or contractors). For example, the auditor may request information to determine the scope of the cybersecurity audit and the criteria the cybersecurity audit will use.
- (c) The business must make good-faith efforts to disclose to the auditor all facts relevant to the cybersecurity audit and must not misrepresent ~~in any manner~~ any fact relevant to the cybersecurity audit.
- (d) ~~The cybersecurity audit must articulate its scope, articulate its criteria, and identify the specific evidence (including documents reviewed, sampling and testing performed, and interviews conducted) examined to make decisions and assessments, and explain why the scope of the cybersecurity audit, the criteria evaluated, and the evidence that the auditor examined are (1) appropriate for auditing the business's cybersecurity program, taking into account the business's size, complexity, and the nature and scope of its processing activities; and (2) why the specific evidence examined is sufficient to justify the auditor's findings.~~ No finding of any cybersecurity audit may rely primarily on assertions or attestations by the business's management. Cybersecurity audit findings must rely primarily upon the specific evidence (including documents reviewed, sampling and testing performed, and interviews conducted) that the auditor is deemed appropriate ~~by the auditor.~~
- (e) The cybersecurity audit report must include the information set forth in section 7123, subsection (e).

- ~~(1) Assess, document, and summarize each applicable component of the business's cybersecurity program set forth in section 7122;~~
 - ~~(2) Specifically identify any gaps or weaknesses in the business's cybersecurity program;~~
 - ~~(3) Specifically address the status of any gaps or weaknesses identified in any prior cybersecurity audit; and~~
 - ~~(4) Specifically identify any corrections or amendments to any prior cybersecurity audits.~~
- (f) ~~The cybersecurity audit must include the auditor's name, affiliation, and relevant qualifications.~~
 - (g) ~~The cybersecurity audit must include a statement that is signed and dated by each auditor that certifies that the auditor completed an independent review of the business's cybersecurity program and information system, exercised objective and impartial judgment on all issues within the scope of the cybersecurity audit, and did not rely primarily on assertions or attestations by the business's management.~~
 - (h) The cybersecurity audit report must be ~~reported~~ provided ~~to the business's board of directors or governing body, or if no such board or equivalent body exists, to the highest ranking to a member of the business's~~ executive management team who has direct responsibility ~~in the business responsible~~ for the business's cybersecurity program.
 - (i) ~~The cybersecurity audit must include a statement that is signed and dated by a member of the board or governing body, or if no such board or equivalent body exists, the business's highest ranking executive with authority to certify on behalf of the business and who is responsible for the business's cybersecurity program. The statement must include the signer's name and title, and must certify that the business has not influenced or made any attempt to influence the auditor's decisions or assessments regarding the cybersecurity audit. The statement also must certify that the signer has reviewed, and understands the findings of, the cybersecurity audit.~~
 - (j) The business and the auditor must retain all documents relevant to each the cybersecurity audit, intervening cybersecurity audit and cybersecurity audit report for a minimum of five (5) two (2) years after completion of the cybersecurity audit.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7123. Scope of Cybersecurity Audit and Audit Report.

- (a) The cybersecurity audit must assess ~~and document~~ how the business's cybersecurity program protects personal information from unauthorized access, destruction, use,

modification, or disclosure; and protects against unauthorized activity resulting in the loss of availability of personal information.

- (b) **Requirements under this Article apply only to activities involving the processing of personal information.**
- (c) The cybersecurity audit must **take into account the size and complexity of the business and the nature and scope of processing activities and assesses** ~~specifically identify, assess, and document:~~
 - (1) The business's establishment, implementation, and maintenance of its cybersecurity program, including the related written documentation thereof (e.g., policies and procedures), that is appropriate to the business's size and complexity and the nature and scope of its processing activities, **taking into account the state of the art and cost of implementing the components of a cybersecurity program,** ~~including the components set forth in this subsection and subsection (b)(2);~~ and
 - (2) Each of the ~~following~~ components of ~~a the business's~~ cybersecurity program listed in subsection (c) that the auditor deems, as applicable to the business's information system. ~~If not applicable, the cybersecurity audit must document and explain why the component is not necessary to the business's protection of personal information and how the safeguards that the business does have in place provide at least equivalent security;~~
 - (3) **How the business implements and enforces compliance with its cybersecurity program, as described in subsection (b)(1), the applicable components in subsection (c), and any additional components as set forth in subsection (d).**
- (d) The cybersecurity audit must assess the following components, if applicable:
 - (A) Authentication, including:
 - (i) Multi-factor authentication (including multi-factor authentication that is resistant to phishing attacks for employees, independent contractors, and any other personnel, ~~and~~ service providers, ~~and~~ and contractors); and
 - (ii) If the business uses passwords or passphrases, strong ~~Strong~~ unique passwords or passphrases (e.g., passwords that are at least eight characters in length, not on the business's disallowed list of commonly used passwords, and not reused).
 - (B) Encryption of personal information, at rest and in transit;

~~(C) Zero trust architecture (e.g., ensuring that connections within the business's information system are both encrypted and authenticated)~~

(D) Account management and access controls **used to protect personal information**, including:

(i) Restricting each person's account's, or application's privileges and access to personal information to what is necessary for that person account, or application to perform their duties. For example:

1. If the person is an employee, independent contractor, or any other personnel, restricting their privileges and access to personal information to what is necessary to perform the respective job functions of each individual, and revoking their privileges and access when their job functions no longer require them, including when their employment or contract is terminated;

2. If the person is a service provider or contractor, restricting their privileges and access to personal information to what is necessary for the specific business purpose(s) **for which it processes personal information set forth in, and in compliance with, the written contract between the business and the service provider or contractor required by the CCPA and section 7051; and**

3. Restricting the privileges and access of third parties to whom the business sells or shares personal information to the personal information that is necessary for the limited and specified purpose(s) **for which it processes personal information set forth in, and in compliance with, the written contract between the business and the service provider or contractor required by the CCPA and section 7051; and**

(ii) Restricting the number of privileged accounts, restricting those privileged accounts' access functions to only those necessary to perform the account-holder's job, restricting the use of privileged accounts to when they are necessary to perform functions, and using a privileged-access management solution (e.g., to ensure just-in-time temporary assignment of privileged access);

(iii) Restricting and monitoring the creation of new accounts for employees, independent contractors, or other personnel; service

providers or contractors; and privileged accounts, and ensuring that the accounts' access and privileges are limited as set forth in subsections (c)(3)(A) and (B) ~~(b)(2)(D)(i) (ii)~~; and

- (iv) Restricting and monitoring physical access to personal information (e.g., through the use of badges, secure physical file locations, and enforcement of clean-desk policies).

(E) ~~Inventory and management of personal information and the business's information system, including~~ This includes:

- ~~(i) Personal information inventories (e.g., maps and flows identifying where personal information is stored, and how it can be accessed) and the classification and tagging of personal information (e.g., how personal information is tagged and how those tags are used to control the use and disclosure of personal information);~~
- ~~(ii) Hardware and software inventories, and the use of allowlisting (i.e., discrete lists of authorized hardware and software to control what is permitted to connect to and execute on the business's information system); and~~
- ~~(iii) Hardware and software approval processes, and preventing the connection of unauthorized hardware and devices to the business's information system.~~

(F) Secure configuration of hardware and software used to protect personal information, including:

- (i) Software updates and upgrades;
- (ii) Securing on-premises and cloud-based environments;
- (iii) Masking (i.e., systematically removing or replacing with symbols such as asterisks or bullets) the sensitive personal information set forth in Civil Code section 1798.145, subdivisions (ae)(1)(A) and (B) and other personal information as appropriate by default in applications;
- (iv) Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and

- (v) Change management (i.e., processes and procedures to ensure that changes to information system(s) do not undermine existing safeguards).
- (G) Internal and external vulnerability scans, penetration testing, and vulnerability disclosure and reporting (e.g., bug bounty and ethical hacking programs) **used to protect personal information;**
- (H) Audit-log management, including the centralized storage, retention, and monitoring of logs **used to protect personal information;**
- (I) Network monitoring and defenses **used to protect personal information,** including the deployment of:
 - (i) Technologies, such as ~~Bot~~-detection and intrusion-detection and intrusion-prevention ~~systems,~~ which a business may use (e.g., to detect unsuccessful login attempts, monitor the activity of authorized users, and detect and prevent unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information); and
 - (ii) Data-loss-prevention systems (e.g., software to detect and prevent unauthorized access, use, or disclosure of personal information).
- (J) Antivirus and antimalware protections **to safeguard personal information;**
- (K) Segmentation of an information system **that involve personal information** (e.g., via properly configured firewalls, routers, switches);
- (L) **Limitation and control of ports, services, and protocols;**
- (M) Cybersecurity awareness, **which may include** including how the business maintains current knowledge of changing cybersecurity threats and countermeasures.
- (N) Cybersecurity education, and training, **including:**
 - (i) **Training for each employee, independent contractor, and any other personnel to whom the business provides access to its information system (e.g., when their employment or contract begins, annually thereafter, and after a personal information security breach, as described in Civil Code section 1798.150); and**

~~(ii) How the business maintains current knowledge of changing cybersecurity threats and countermeasures.~~

(O) Secure development and coding best practices, including code- reviews and testing;

(P) ~~Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053;~~

(Q) ~~Retention schedules and proper disposal of personal information no longer required to be retained, by (1) shredding, (2) erasing, or (3) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means;~~

(R) How the business manages its responses to security incidents (i.e.e.g., its incident response management);

(i) For the purposes of subsection (179), “security incident” has the same meanings as “breach of security of the system” in Section 1798.82, as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. ~~actually or potentially imminently jeopardizes the confidentiality, integrity, or availability of the business’s information system or the personal information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of the business’s cybersecurity program; Unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information is a security incident.~~

(ii) The business’s incident response management **could** includes:

1. The business’s documentation of predetermined instructions or procedures to detect, respond to, limit the consequences of, and recover from **a security incident malicious attacks against its information system (i.e., the business’s incident response plan)**; and

2. ~~How the business tests its incident response capabilities;~~ and

- (S) Business-continuity and disaster-recovery plans, including data- recovery capabilities and backups **as it relates to personal information for cybersecurity-related disruptions.**

~~(2) For each of the applicable components set forth in subsections (b)(1)–(2), including the safeguards the business identifies in its policies and procedures, the cybersecurity audit must describe, at a minimum, how the business implements and enforces compliance with them.~~

- (3) Nothing in this section prohibits an audit from assessing ~~and documenting~~ components of a cybersecurity program that are not set forth in subsections (b) or (c)(1)–(2).

(e) The cybersecurity audit report must:

- (1) Describe the business’s information system; and **identify** (A) the policies, procedures, and practices that the cybersecurity audit assessed; (B) the criteria used for the cybersecurity audit; and (C) the specific evidence examined to make decisions and assessments, such as documents reviewed, sampling and testing performed, and interviews conducted. The cybersecurity audit report must also explain why assessing those policies, procedures, and practices; using those criteria; and examining that specific evidence justify the auditor’s findings.
- (2) Identify the applicable components in subsection (c), and any additional component assessed in accordance with subsection (d); describe how the business implements and enforces compliance with the policies and procedures in subsections (b)(1), the applicable components in subsection (c), and any additional component assessed in accordance with subsection (d); and explain their effectiveness. ~~Assess and document the effectiveness of the components set forth in subsections (b)(1)–(2)~~ in preventing unauthorized access, destruction, use, modification, or disclosure of personal information; and preventing unauthorized activity resulting in the loss of availability of personal information;
- (3) Identify and describe in detail the status of any **material** gaps or weaknesses of the policies and procedures ~~components set forth~~ in subsections (b)(1)–~~(2)~~, the applicable components in subsection (c), and any additional component assessed in accordance with subsection (d), that the auditor deemed to increase the risk of unauthorized access, destruction, use, modification, or disclosure of consumers’ personal information; or increase the risk of unauthorized activity resulting in the loss of availability of personal information.
- (4) Document the business’s plan to address the **material** gaps and weaknesses identified and described pursuant to subsection ~~(e)(2)–(e)(3)~~, including the ~~resources it has allocated to resolve them and the~~ timeframe in which it will resolve them;

- (5) Identify any corrections or amendments to any prior cybersecurity audit reports.
 - (6) Include the title(s) of up to three ~~the~~ qualified individuals **primarily** responsible for the business's cybersecurity program; ~~and~~
 - (7) Include the auditor's name, affiliation, and relevant qualifications.
 - ~~(8) Include the date that the cybersecurity program and any evaluations thereof were presented to the business's board of directors or governing body or, if no such board or equivalent governing body exists, to the highest ranking executive of the business responsible for the business's cybersecurity program.~~
 - (9) Include a statement that is signed and dated by the highest-ranking auditor that certifies that they completed an independent review of the business's cybersecurity program and information system, exercised objective and impartial judgment on all issues within the scope of the cybersecurity audit, and did not rely primarily on assertions or attestations by the business's management.
 - (10) If the business provided notification to **the Attorney General affected consumer(s)** pursuant to Civil Code section 1798.82, subdivision (f)(a), **the cybersecurity audit must** ~~the cybersecurity audit must include~~ **assess** a **sample** copy of the notification(s), excluding any personal information; or a description of the notification(s), **as applicable.**
 - (11) If the business was required to notify any **California** agency with jurisdiction over privacy laws ~~or other data processing authority in California, other states, territories, or countries~~ **pursuant to Cal. Civ. Code 1798.82** unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information, **the cybersecurity audit must assess** ~~the cybersecurity audit must include~~ **the materials provided to that agency. a sample copy of the notification(s), excluding any personal information; or a description of the required notification(s) as well as the date(s) and details of the activity that gave rise to the required notification(s) and any related remediation measures taken by the business.**
- (f) ~~if the business has engaged in~~ A business may utilize a cybersecurity audit, assessment, or evaluation that it has prepared for another purpose, provided that it is reasonably in scope and effect as a cybersecurity audit that would otherwise be conducted under meets all of the requirements of this Article, either on its own or through supplement ~~the business is not required to complete a duplicative cybersecurity audit.~~ For example, a business may have engaged in an audit that uses **or is conducted to evaluate the business's implementation of** the National Institute of Standards and Technology Cybersecurity framework 2.0, SOC 2 Type 2, and ISO Certifications meets all of the requirements of this Article. ~~However, the business must specifically explain how the~~

~~cybersecurity audit, assessment, or evaluation that it has completed meets all of the requirements set forth in this Article. The business must specifically address subsections (a) – (e), including explaining how the cybersecurity audit, assessment, or evaluation addresses each component set forth in subsections (b)(1) – (2). If the cybersecurity audit, assessment, or evaluation completed for the purpose of compliance with another law or regulation or for another purpose does not meet all of the requirements of this Article, the business must supplement the cybersecurity audit with any additional information required to meet all of the requirements of this Article.~~

- (g) **A single cybersecurity audit that meets the requirements set forth in subsection (a) may address a comparable set of processing activities that includes similar activities.**

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7124. Certification of Completion.

- (a) Each calendar year that a business ~~that~~ is required to complete a cybersecurity audit **or intervening cybersecurity audit** pursuant to this Article, it must submit to the Agency ~~every calendar year~~ a written certification that the business completed the cybersecurity audit **or intervening cybersecurity audit** as required by ~~set forth in~~ this Article.
- ~~(b) The business must submit the certification no later than April 1 following any year that the business is required to complete a cybersecurity audit.~~
- ~~(c) The written certification must be completed by a member of the business's executive management team who:~~
- ~~(1) Is directly responsible for the business's cybersecurity audit compliance;~~
 - ~~(2) Has sufficient knowledge of the business's cybersecurity audit to provide accurate information; and~~
 - ~~(3) Has the authority to submit the business's certification to the Agency.~~
- (d) The written certification must be completed and submitted to the Agency ~~through the Agency's~~ via its website at <https://cppa.ca.gov/> ~~and must identify the 12 months that the audit covers.~~ The certification must include:
- The business's name and point of contact for the business, including the contact's name, phone number, and email address.
 - A statement that the business has completed the cybersecurity audit.
 - The time period covered by the audit, by month and year.

- (4) An electronically signed attestation to the following statement: "I attest that I meet the requirements of California Code of Regulations, Title 11, section 7124, subsection (c), to submit this certification. Under penalty of perjury under the laws of the state of California, I hereby declare that the information contained within and submitted with this certification is true and correct and that the business has not made any attempt to influence the auditor's decisions or assessments regarding the cybersecurity audit."
- (5) The name and business title of the person submitting the certification, and the date of the certification.
- (e) ~~The written certification must be signed and dated by a member of the board or governing body, or if no such board or equivalent body exists, the business's highest-ranking executive with authority to certify on behalf of the business and who is responsible for oversight of the business's cybersecurity audit compliance. It also must include a statement that certifies that the signer has reviewed and understands the findings of the cybersecurity audit. The signer must include their name and title.~~
- (f) The disclosure of a cybersecurity audit or written certification to the Agency or Attorney General shall not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.
- ~~(g)~~ Cybersecurity audits and written certifications shall be confidential and shall be exempt from disclosure under the California Public Records Act.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

Adopt all of the text in the following Article:

ARTICLE 10. RISK ASSESSMENTS

§ 7150. When a Business Must Conduct a Risk Assessment.

- (a) Every business whose processing of consumers' personal information presents significant risk to consumers' privacy as set forth in subsection (b) must conduct a risk assessment before initiating that processing.
- (b) Each of the following processing activities presents significant risk to consumers' privacy:
 - (1) Selling or sharing personal information.
 - (2) Processing sensitive personal information **for purposes other than those listed in subsection 7027(m)(1)-(8).**
 - (A) A business that processes the sensitive personal information of its employees or independent contractors solely and specifically for 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.
 - (3) Using ADMT ~~automated decisionmaking technology~~ **to process personal information** for a significant decision concerning a consumer **that presents a significant risk to consumer privacy** ~~or for extensive profiling.~~

~~(A) For purposes of this Article, "significant decision" means a decision using information that is not subject to the exceptions set forth in Civil Code sections 1798.145, subdivisions (c)-(g), or 1798.146, subdivisions (a)(1), (4), and (5), that results in access to, or the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice (e.g., posting of bail bonds), employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services (e.g., groceries, medicine, hygiene products, or fuel).~~

~~(i) Education enrollment or opportunity includes:~~

~~1. Admission or acceptance into academic or vocational programs;~~

~~2. Educational credentials (e.g., a degree, diploma, or certificate); and~~

~~3. Suspension and expulsion.~~

~~(ii) Employment or independent contracting opportunity or compensation includes:~~

~~1. Hiring;~~

~~2. Allocation or assignment of work, salary, hourly or per-assignment compensation, incentive compensation such as a bonus, or another benefit ("allocation/assignment of work and compensation");~~

~~3. Promotion; and~~

~~4. Demotion, suspension, and termination.~~

~~(B) For purposes of this Article, "extensive profiling" means:~~

~~(i) Profiling a consumer through systematic observation when they are acting in their capacity as an applicant to an educational program, job applicant, student, employee, or independent contractor ("work or educational profiling");~~

~~(ii) Profiling a consumer through systematic observation of a publicly accessible place ("public profiling"); or~~

~~(iii) Profiling a consumer for behavioral advertising.~~

(4) Using automated processing to infer or extrapolate a consumer's intelligence, ability, aptitude, performance at work, economic situation, health (including mental health), personal preferences, interests, reliability, predispositions, behavior, location, or movements, based upon systematic observation of that consumer when they are acting in their capacity as an educational program applicant, job applicant, student, employee, or independent contractor for the business.

(5) Using automated processing to infer or extrapolate a consumer's intelligence, ability, aptitude, performance at work, economic situation, health (including mental health), personal preferences, interests, reliability, predispositions, behavior, or movements, based upon that consumer's presence in a sensitive location. "Infer or extrapolate" does not include a business using a consumer's personal information solely to deliver goods to, or provide transportation for, that consumer at a sensitive location.

~~(6) Processing the personal information of consumers, which the business intends to use to train an ADMT automated decisionmaking technology for a significant~~

~~decision concerning a consumer; or train a facial recognition, emotion recognition, or other technology that verifies a consumer's identity, or conducts physical or biological identification or profiling of a consumer. For purposes of the paragraph, "intends to use" means the business is using, plans to use, permits to use, plans to permit others to use, is advertised or marking the use of, or plans to advertise or market the use of or artificial intelligence that is capable of being used for any of the following:~~

~~(A) For a significant decision concerning a consumer;~~

~~(B) To establish individual identity;~~

~~(C) For physical or biological identification or profiling;~~

~~(D) For the generation of a deepfake; or~~

~~(E) For the operation of generative models, such as large language models.~~

(c) Illustrative examples of when a business must conduct a risk assessment follow:

~~(1) Business A is a rideshare provider. Business A seeks to use automated decisionmaking technology to allocate rides and determine fares and bonuses for its drivers. Business A must conduct a risk assessment because it seeks to use automated decisionmaking technology for a significant decision concerning a consumer.~~

(2) Business A ~~is hiring a new employee. Business A plans to videotape job interviews then B seeks to use emotion recognition assessment technology without human involvement to decide as part of the job interview process who to hire. Business A-B must conduct a risk assessment because it plans seeks to use ADMT-automated decisionmaking technology (specifically, physical or biological identification or profiling) for a significant decision concerning a consumer.~~

(3) Business B ~~provides a mobile dating application. Business B plans C seeks to process disclose consumers' precise geolocation and the ethnicity and medical information the consumers provided in their dating profiles to Business B-C's analytics service provider. Business B-C must conduct a risk assessment because if it seeks to process sensitive personal information of consumers for purposes other than those listed in subsection 707(m)(1)-(8).~~

(4) Business C ~~provides a personal-budgeting application into which consumers enter their financial information, including income. Business C-D seeks to display advertisements to these consumers on different websites (through cross-context behavioral advertising) for payday loans that are based on evaluations of these consumers' personal preferences, interests, and reliability from their financial~~

information. Business D must conduct a risk assessment because it plans ~~seeks~~ to ~~conduct extensive profiling and~~ share personal information **for cross-context behavioral advertising**.

~~(5) Business E is a grocery store chain. Business E seeks to process consumers' device media access control (MAC) addresses via Wi-Fi tracking to observe consumers' shopping patterns within its grocery stores. Business E must conduct a risk assessment because it seeks to profile consumers through systematic observation of a publicly accessible place.~~

(6) Business D ~~F~~ is a technology provider. Business D ~~F~~ plans ~~seeks~~ to extract faceprints from consumers' photographs to train Business D ~~F~~'s facial-recognition technology. Business D ~~F~~ must conduct a risk assessment **because if** it seeks to process consumers' **sensitive** personal information **to train a facial recognition technology** ~~automated decisionmaking technology or artificial intelligence that is capable of being used to establish individual identity~~ **for purposes other than those listed in subsection 7027(m)(1)-(8).**

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7151. Stakeholder Involvement for Risk Assessments.

- (a) A business's primary employees whose job duties include participating in the processing of personal information that would be subject to a risk assessment must be included in business's risk assessment process for that processing activity. ~~The business must ensure that relevant individuals prepare, contribute to, or review the risk assessment, based upon their level of involvement in the processing activity that is subject to the risk assessment. Relevant individuals are those whose job duties pertain to the processing activity. For example, an individual who determines the method by which the business plans to collect consumers' personal information for one of the processing activities in section 7150, subsection (b), must provide that information to the individuals conducting the risk assessment. relevant individuals may be part of the business's product, fraud prevention, or compliance teams. These individuals must make good faith efforts to disclose all facts necessary to conduct the risk assessment and must not misrepresent in any manner any fact necessary to conduct the risk assessment.~~
- (b) In conducting the A-risk assessment, a business may include involve external parties in the process. ~~to identify, assess, and mitigate the risks to consumers' privacy. These external parties may include, f~~ For example, a business may utilize or gather information from service providers, contractors, experts in detecting and mitigating bias in ADMT ~~automated decisionmaking technology~~, a subset of the consumers whose personal information the business plans ~~seeks~~ to process, or stakeholders that represent consumers' or others' interests, including consumer advocacy organizations.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7152. Risk Assessment Requirements.

- (a) ~~A~~ The business must conduct a risk assessment to **inform its processing activities, including determine** whether the risks to consumers' privacy from the processing of personal information outweigh the benefits to the consumer, the business, other stakeholders, and the public from that same processing. The ~~business must conduct and document the~~ risk assessment **must may** ~~as set forth below:~~
- (1) ~~The business must specifically i~~ Identify and document in a risk assessment report the business's ~~its~~ purpose for processing consumers' personal information. **The purpose must not be identified or described in generic terms, such as "to improve our services" or for "security purposes." By contrast, if a business is "improving the service" by decreasing consumers' wait times when processing their privacy rights requests, the business may identify this decrease of wait times to process privacy rights requests as the relevant purpose.**
- (2) ~~The business must i~~ Identify and document in a risk assessment report identify the categories of personal information to be processed, ~~and whether they include~~ any categories of sensitive personal information. This must include:
- (A) The minimum personal information that is necessary to achieve the purpose of processing consumers' personal information.
- ~~(B) For uses of automated decisionmaking technology or artificial intelligence as set forth in section 7150, subsections (b)(3)(A)–(4), the business may must identify the actions the business has taken or any actions it plans to take to maintain the quality of personal information processed by the automated decisionmaking technology or artificial intelligence.~~
- ~~(i) "Quality of personal information" includes completeness, representativeness, timeliness, validity, accuracy, consistency, and reliability of the sources of the personal information for the business's proposed use of the automated decisionmaking technology or artificial intelligence.~~
- ~~(ii) Actions a business may take to ensure quality of personal information include: (1) identifying the source of the personal information and whether that source is reliable (or, if known, whether the original source of the personal information is reliable); (2) identifying how the personal information is relevant to the task being automated and how it is expected to be useful for the development, testing, and operation of the automated decisionmaking technology or artificial intelligence; (3) identifying whether the personal information contains sufficient breadth to address the range of real world inputs the automated~~

~~decisionmaking technology or artificial intelligence may encounter; and (4) identifying how errors from data entry, machine processing, or other sources are measured and limited.~~

- (3) ~~The business must~~ identify and document in a risk assessment report the following operational elements of the ~~its~~ processing:
- (A) The business's planned method for collecting, using, disclosing, retaining, or otherwise processing personal information, and the sources of the personal information.
 - (B) How long the business plans to will retain each category of personal information, or if unknown, the and any criteria the business plans to used to determine that retention period.
 - (C) The business's method of interacting with the consumers whose personal information the business plans to process. ~~The relationship between the consumer and the business, including whether the consumer interacts with the business, how they do so~~ (e.g., via websites, applications, or offline), and the purpose of the interaction ~~and the nature of the interaction~~ (e.g., to provide ~~obtain~~ a good or service ~~from the business~~).
 - (D) The approximate number of consumers whose personal information the business plans seeks to process.
 - (E) What disclosures the business has made or plans to make to the consumer about the processing of their personal information and, how these disclosures were or will be made (e.g., via a just-in-time notice); ~~and what actions the business has taken or plans to take to make these disclosures specific, explicit, prominent, and clear to the consumer.~~
 - ~~(F)~~ The names or categories of the service providers, contractors, or third parties to whom the business discloses or makes available the consumers' personal information for the processing; the purpose for which the business discloses or makes the consumers' personal information available to them; ~~and what actions the business has taken or plans to take to make consumers aware of the involvement of these entities in the processing.~~
 - (G) ~~The technology to be used in the processing.~~ For the uses of ADMT ~~automated decisionmaking technology~~ set forth in section 7150, subsections (b)(3), the business may must identify:
 - (i) The logic of the ADMT automated decisionmaking technology, including any assumptions or limitations of the logic; and

- (ii) The output of the ADMT ~~automated decisionmaking technology~~, and how the business will use the output to make a significant decision.
- (4) ~~The business must specifically i~~ Identify the benefits to the business, the consumer, other stakeholders, and the public from the processing of the personal information, as applicable. The benefits ~~For example, a business must not be identified in generic terms, such as a benefit as “improving our service.” By contrast, if a benefit of a processing activity is to reduce the response time to a consumer’s right to know request, a business may identify the relevant benefit as enabling consumers to receive the personal information they requested on a quicker timeline.~~

~~because this does not identify the specific improvements to the service nor by what means the benefit resulted from the processing. If the benefit resulting from the processing is that the business profits monetarily (e.g., from the sale or sharing of consumers’ personal information), the business must identify this benefit and, when possible, estimate the expected profit.~~

- (5) ~~The business must specifically i~~ Identify the negative impacts to consumers’ privacy associated with the processing. The business **may must** identify the sources and causes of these negative impacts, ~~and any criteria that the business used to make these determinations.~~

For example, n ~~A~~ Negative impacts to consumers’ privacy that a business may consider include the following:

- (A) Unauthorized access, destruction, use, modification, or disclosure of personal information; and unauthorized activity resulting in the loss of availability of personal information.
- (B) Discrimination upon the basis of protected classes characteristics that would violate federal or state antidiscrimination law.
- (C) Impairing consumers’ control over their personal information, such as by providing insufficient information for consumers to make an informed decision regarding the processing of their personal information, or by interfering with consumers’ ability to make choices consistent with their reasonable expectations.
- (D) Coercing or compelling consumers into allowing the processing of their personal information, such as by conditioning consumers’ acquisition or use of an online service upon their disclosure of personal information that is unnecessary to the expected functionality of the service, or requiring consumers to consent to processing when such consent

cannot be freely given (e.g., because it was obtained through the use of a dark pattern).

- ~~(E) Disclosing a consumer's media consumption (e.g., books they have read or videos they have watched) in a manner that chills or deters their speech, expression, or exploration of ideas.~~
 - (F) **Economic harms, including limiting or depriving consumers of economic opportunities; charging consumers higher prices, or compensating consumers at lower rates based on profiling; or imposing additional costs upon consumers, including costs associated with the unauthorized access to consumers' personal information.**
 - (G) **Physical harms to consumers or to property, including processing that creates the opportunity for physical or sexual violence.**
 - (H) **Reputational harms, including stigmatization, that would negatively impact an average consumer, such as stigmatization of a consumer as a result of. Examples of processing activities that result in such harms include a mobile dating application's disclosure of a consumer's sexual or other preferences in a partner; a business stating or implying that a consumer has committed a crime without verifying this information; or a business processing consumers' biometric information to create a deepfake of them.**
 - (I) **Psychological harms, including emotional distress, stress, anxiety, embarrassment, fear, frustration, shame, and feelings of violation, that would negatively impact an average consumer. Examples of such harms include emotional distress resulting from disclosure of nonconsensual intimate imagery; stress and anxiety from regularly targeting a consumer who visits websites for substance abuse resources with advertisements for alcohol; or emotional distress from disclosing or a disclosure of a consumer's purchase of pregnancy tests or emergency contraception for non-medical purposes.**
- (6) ~~The business must specifically identify and document in a risk assessment report any the safeguards that the business # plans to implement for the processing, such as safeguards to address the negative impacts identified in subsection (a)(5). The business must specifically identify how these safeguards address the negative impacts identified in subsection (a)(5), including to what extent they eliminate or reduce the negative impacts; and identify any safeguards the business will implement to maintain knowledge of emergent risks and countermeasures.~~

(A) For example, Safeguards that a business may consider include the following:

- (i) Encryption, segmentation of information systems, physical and logical access controls, change management, network monitoring and defenses, and data and integrity monitoring;
- (ii) Use of privacy-enhancing technologies, such as trusted execution environments, federated learning, homomorphic encryption, and differential privacy;
- (iii) Consulting external parties, such as those described in section 7151, subsection (b), to ensure that the business maintains current knowledge of emergent privacy risks and countermeasures; and using that knowledge to identify, assess, and mitigate risks to consumers' privacy; and

~~(iv) Evaluating the need for human involvement as part of the business's use of automated decisionmaking technology, and implementing policies, procedures, and training to address the degree and details of human involvement identified as necessary in that evaluation.~~

~~(B) For uses of automated decisionmaking technology set forth in section 7150, subsection (b)(3)(A), the business may must identify the following:~~

~~(i) Whether it evaluated the automated decisionmaking technology to ensure it works as intended for the business's proposed use and does not discriminate based upon protected classes ("evaluation of the automated decisionmaking technology"); and~~

(ii) **The implementing policies, procedures, and training the business has implemented or plans to implement to ensure that the business's ADMT automated decisionmaking technology works as intended for the business's purpose proposed use and does not unlawfully discriminate based upon protected classes characteristics.** ~~("accuracy and nondiscrimination safeguards"). For example, if a business determines that the use of low quality enrollment images creates a high risk of false positive matches in its proposed use of facial recognition technology, the business must identify the policies, procedures, and training it has implemented or plans to implement to ensure that it is using only sufficiently high quality enrollment images to mitigate that risk.~~

- (iii) ~~Where a business obtains the automated decisionmaking technology from another person, the business must identify the following:~~
- ~~1. Whether it reviewed that person's evaluation of the automated decisionmaking technology, and whether that person's evaluation included any requirements or limitations relevant to the business's proposed use of the automated decisionmaking technology.~~
 - ~~2. Any accuracy and nondiscrimination safeguards that it implemented or plans to implement.~~
- (7) ~~The business must specifically i~~ Identify and document in a risk assessment report whether it will initiate the processing subject to the risk assessment.
- (8) ~~The business must specifically i~~ Identify and document in a risk assessment report the contributors to individuals who provided the information for the risk assessment, except for legal counsel who provided legal advice. ~~In the risk assessment or in a separate document maintained by the business, the business must identify the individuals within the business and the external parties that contributed to the risk assessment.~~
- (9) ~~The business must specifically i~~ Identify and document in a risk assessment report the date the assessment was reviewed and approved, and the names and positions of the individuals who reviewed or approved the assessment, except for legal counsel who provided legal advice responsible for the review and approval. An individual who has the authority to participate in deciding ~~The individuals responsible for the review and approval may must include the individual who decides whether the business will initiate the processing that is the subject of to the risk assessment. If the business presented or summarized its risk assessment to the business's board of directors or governing body for review, or if no such board or equivalent body exists, to the business's highest ranking executive who is responsible for oversight of risk assessment compliance for review, the business must include the date of that review.~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7153. Additional Requirements for Businesses that Process Personal Information to Train Automated Decisionmaking Technology or Artificial Intelligence:

- (a) ~~A business that makes ADMT automated decisionmaking technology or artificial intelligence available to another business ("recipient business") for any processing activity to make a significant decision as~~ set forth in section 7150, subsection (b), must

~~provide to the recipient business all facts necessary to the recipient business for the recipient business to conduct its own risk assessment.~~

- (b) ~~A business that trains automated decisionmaking technology or artificial intelligence as set forth in section 7150, subsection (b)(4) and permits another person to use that automated decisionmaking technology or artificial intelligence, must provide to the person a plain language explanation of any requirements or limitations that the business identified as relevant to the permitted use of automated decisionmaking technology or artificial intelligence.~~
- (c) ~~The requirements of this section apply only to ADMT-automated decisionmaking technology or artificial intelligence trained using personal information.~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7154. Goal of a Risk Assessment. ~~Prohibition Against Processing If Risks to Consumers' Privacy Outweigh Benefits.~~

- (a) The goal of a risk assessment is **not initiating** ~~restricting or prohibiting the processing of personal information~~ business must not process personal information for any processing activity identified in section 7150, subsection (b), if the risks to ~~consumers' privacy~~ of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public ~~from the processing.~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7155. Timing and Retention Requirements for Risk Assessments.

- (a) A business must comply with the following timing requirements for conducting and updating its risk assessments:
- (1) A business must conduct and document a risk assessment in accordance with the requirements of this Article **before initiating any processing activity identified in section 7150, subsection (b).**
 - (2) **At least once every three years, a A** business must review, and update as necessary, its risk assessments to ensure that they remain accurate in accordance with the requirements of this Article.
 - (3) Notwithstanding subsection (a)(2) of this section, a business must ~~immediately~~ update a risk assessment whenever there is a material change relating to the processing activity, as soon as feasibly possible, but no later than 45 calendar days from the date of the material change. **A material change is one that is likely to affect whether a reasonable consumer would interact with the product or service based on the change in processing activity. A change relating to the processing activity is material if it diminishes the benefits of the processing**

~~activity as set forth in section 7152, subsection (a)(4), creates new negative impacts or increases the magnitude or likelihood of previously identified negative impacts as set forth in section 7152, subsection (a)(5), or diminishes the effectiveness of the safeguards as set forth in section 7152, subsection (a)(6).~~

Material changes may include, for example, changes to the purpose of the processing; the minimum personal information necessary to achieve the purpose of the processing; or the risks to consumers' privacy raised by consumers (e.g., numerous consumers complain to a business about the risks that the business's processing poses to their privacy).

(b) ~~A business must retain its risk assessments, including original and updated versions, for as long as the processing continues or for five years after the completion of the risk assessment, whichever is later.~~

(c) Requirements under this Article apply only to activities involving the processing of personal information.

(d) Requirements under this Article apply only to processing activities initiated after this Article enters effect.

~~(e)~~ For any processing activity identified in section 7150, subsection (b), ~~that the business initiated prior to [OAL to fill in] the effective date of these regulations and that begins~~ continues after [OAL to fill in] the effective date of these regulations, the business must conduct and document as set forth in section 7152, a risk assessment in accordance with the requirements of this Article within 24 months of the effective date of these regulations. no later than 24 months after the regulations enter into effect. December 31, 2027. The business must comply with the submission requirements set forth in section 7157, subsection (a)(1).

~~(f) A business must retain its risk assessments, including original and updated versions, for as long as the processing continues or for five years after the completion of the risk assessment, whichever is later.~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7156. Conducting Risk Assessments for a Comparable Set of Processing Activities or in Compliance with Other Laws or Regulations.

(a) A business may conduct a single risk assessment for a comparable set of processing activities. A "comparable set of processing activities" that can be addressed by a single risk assessment is a set of similar processing activities that present similar risks to consumers' privacy.

- (1) For example, Business E sells toys to children and is considering using in-store paper forms to collect names, mailing addresses, and birthdays from children that visit their stores, and to use that information to mail a coupon and list of age-appropriate toys to each child during the child's birth month and every November. Business E uses the same service providers and technology for each category of mailings across all stores. Business E must conduct ~~and document~~ a risk assessment, including documenting required information in its risk assessment report, because if it is processing sensitive personal information for purposes other than those listed in subsection 7027(m)(1)-(8). Business E may use a single risk assessment for processing the personal information for the birthday mailing and November mailing across all stores because in each case it is collecting the same personal information in the same way for the purpose of sending coupons and age-appropriate toy lists to children, and this processing presents similar risks to consumers' privacy.

~~(b) 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 and effect to the data protection assessment that would otherwise be conducted pursuant to contains the information that must be included in, or is paired with the outstanding information necessary for, compliance with section 7152. If the business has conducted and documented a risk assessment for the purpose of complying with another law or regulation that meets all the requirements of this Article, the business is not required to conduct a duplicative risk assessment. If the risk assessment conducted and documented for the purpose of compliance with another law or regulation does not meet all of the requirements of this Article, the business must supplement the risk assessment with any additional information required to meet all of the requirements of this Article.~~

- (1) For example, Business F plans to sell consumers' personal information. Business F conducts a risk assessment for that processing activity using a data protection assessment that is compliant with another state law. That state law requires the information that must be in section 7152, but does not explicitly require makes optional as relevant for the processing activity some of the information in subsections (a)(2)-(3), (7), or require the name and position of the individual who has the authority to participate in deciding whether the business will initiate the processing that is subject to the risk assessment. That risk assessment satisfies requirements under this article because it is reasonably similar in scope and effect as the risk assessment required under these regulations. Business F must also include this information in its risk assessment to meet the requirements in section 7152.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7157. Submission of Risk Assessments to the Agency.

(a) Timing of Risk Assessment-Submissions.

- (1) For risk assessments conducted in 2028⁸⁶ and 2029⁹⁷, the business must submit to the Agency the information required by section (b) no later than April 1, 2030²⁸.
~~First Submission. A business has 24 months from the effective date of these regulations to submit the risk assessment materials regarding the risk assessments that it has conducted from the effective date of these regulations to the date of submission ("first submission"). The risk assessment materials are set forth in subsection (b) and must be submitted to the Agency as set forth in subsection (c).~~
- (2) For risk assessments conducted after 2029⁹⁷, the business must submit to the Agency the information required by section (b) no later than April 1 following any year during which the business conducted the risk assessments. For example, for risk assessments conducted in 2029⁹⁸, the business must submit to the Agency the information required by subsection (b) no later than April 1, 2030²⁹.
~~Annual Submission. After the business completes its first submission to the Agency as set forth in subsection (a)(1), its subsequent certification of conduct risk assessment materials must be submitted every calendar year to the Agency, and there must be no gap in the months covered by successive submissions of risk assessment materials ("subsequent annual submissions").~~

(b) A business must submit to the Agency the following risk assessment information.
~~Risk Assessment Materials to Be Submitted. The first submission and subsequent annual submissions of the risk assessment materials to the Agency must include the Certification of Conduct following:~~

- (1) The business's name and a point of contact for the business, including the contact's name, phone number, and email address.
- (2) The time period covered by the submission, by month and year.
- (3) The number of risk assessments conducted or updated by the business during the time period covered by the submission, in total and for each of the processing activities identified in section 7150, subsection (b).
- (4) Whether the risk assessments conducted or updated by the business during the time period covered by the submission involved the processing of each of the categories of personal information and sensitive personal information identified in Civil Code section 1798.140, subdivisions (v)(1)(A)-(L), (ae)(1)(A)-(G), and (ae)(2)(A)-(C).
- (5) 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."

(6) The name and business title of the person submitting the risk assessment information, and the date of the certification.

~~(7) Certification of Conduct. The business must submit a written certification that the business conducted its risk assessment as set forth in this Article during the months covered by the first submission and subsequent annual submissions to the Agency on a form provided by the Agency;~~

~~(A) The business must designate a qualified individual with authority to certify the conduct of the risk assessment on behalf of the business. This individual must be the business's highest ranking executive who is responsible for oversight of the business's risk assessment compliance in accordance with this Article ("designated executive");~~

~~(B) The written certification must include:~~

~~(i) Identification of the months covered by the submission period for which the business is certifying its conduct of the risk assessment and the number of risk assessments that the business conducted and documented during that submission period;~~

~~(ii) An attestation Confirmation that the designated executive has reviewed, understood, and approved the business's risk assessments that were conducted and documented as set forth in this Article;~~

~~(iii) An attestation that the business initiated any of the processing set forth in section 7150, subsection (b), only after the business conducted and documented a risk assessment as set forth in this Article; and~~

~~(iv) The designated executive's name, title, and signature, and the date of certification;~~

~~(8) Risk Assessments in Abridged Form. For each risk assessment conducted and documented or updated by the business during the submission period, the business must submit an abridged version of the new or updated risk assessment to the Agency in response to the Agency's request on a form provided by the Agency that includes:~~

- ~~(A) Identification of the processing activity in section 7150, subsection (b), that triggered the risk assessment;~~
- ~~(B) A plain language explanation of its purpose for processing consumers' personal information;~~
- ~~(C) The categories of personal information processed, and whether they include sensitive personal information; and~~
- ~~(D) A plain language explanation of the safeguards that the business has implemented or plans to implement as set forth in section 7152, subsection (a)(6). A business is not required to provide information that would compromise its ability to prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information; resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions; or ensure the physical safety of natural persons. A business is not required to provide information that would be business sensitive, confidential, or subject to privilege or other protection.~~

~~(9) Risk Assessments in Unabridged Form. A business also may include in its submission to the Agency a hyperlink that, if clicked, will lead to a public webpage that contains its unabridged risk assessment.~~

~~(10) Exemptions.~~

- ~~(A) A business is not required to submit a Certification of Conduct risk assessment to the Agency if the business does not initiate the processing activity subject to the risk assessment.~~
- ~~(B) If a business previously conducted a risk assessment for a processing activity in compliance with this Article and submitted an abridged risk assessment to the Agency, and there were no material changes to that processing during a subsequent submission period, the business is not required to submit an updated risk assessment to the Agency. The business must still submit a certification of the conduct of its risk assessment to the Agency.~~

(c) The individual submitting the information set forth in subsection (b) must be a member of the business's executive management team who:

- (1) Is directly responsible for the business's risk assessment compliance;
- (2) Has sufficient knowledge of the business's risk assessment to provide accurate information; and

(3) ~~Has the authority to submit the risk assessment information to the Agency.~~

(d) ~~Method of Submission.~~ The risk assessment information materials must be submitted to the Agency via ~~through~~ the Agency's website at <https://cppa.ca.gov/>.

(e) ~~Risk Assessments Must Be Provided to the Agency or to the Attorney General Upon Request.~~ The Agency or the Attorney General may require a business to submit ~~provide~~ its ~~unabridged~~ risk assessments reports to the Agency or to the Attorney General at any time. A business must submit ~~provide~~ its ~~unabridged~~ risk assessment reports within 30 calendar ~~10 business~~ days of the Agency's or the Attorney General's request.

(1) The disclosure of a risk assessment to the Agency or Attorney General shall not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

(2) Risk assessments shall be confidential and shall be exempt from disclosure under the California Public Records Act.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

Adopt all of the text in the following Article:

ARTICLE 11. AUTOMATED DECISIONMAKING TECHNOLOGY

§ 7200. When a Business’s Use of Automated Decision making Technology is Subject to the Requirements of This Article.

- (a) A business that uses ~~automated decision-making technology~~ ADMT to make a significant decision concerning a consumer that results in a significant risk to consumer privacy in any of the following ways must comply with the requirements of this Article:

~~(1) For a significant decision concerning a consumer. For purposes of this Article, “significant decision” means a decision using information that is not subject to the exceptions set forth in Civil Code sections 1798.145, subdivisions (c) (g), or 1798.146, subdivisions (a)(1), (4), and (5), that results in access to, or the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice (e.g., posting of bail bonds), employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services (e.g., groceries, medicine, hygiene products, or fuel).~~

~~(A) Education enrollment or opportunity includes:~~

- ~~(i) Admission or acceptance into academic or vocational programs;~~
- ~~(ii) Educational credentials (e.g., a degree, diploma, or certificate); and~~
- ~~(iii) Suspension and expulsion.~~

~~(B) Employment or independent contracting opportunities or compensation includes:~~

- ~~(i) Hiring;~~
- ~~(ii) Allocation or assignment of work, salaries, hourly or per-assignment compensation, incentive compensation such as bonuses, or other benefits (“allocation/assignment of work and compensation”);~~
- ~~(iii) Promotion; and~~
- ~~(iv) Demotion, suspension, and termination.~~

~~(2) For extensive profiling of a consumer. For purposes of this Article, “extensive profiling” means:~~

~~(A) Profiling a consumer through systematic observation when they are acting in their capacity as an applicant to an educational program, job applicant, student, employee, or independent contractor (“work or educational profiling”);~~

~~(B) Profiling a consumer through systematic observation of a publicly accessible place (“public profiling”); or~~

~~(C) Profiling a consumer for behavioral advertising;~~

~~(3) For training uses of automated decisionmaking technology, which are processing consumers’ personal information to train automated decisionmaking technology that is capable of being used for any of the following:~~

~~(A) For a significant decision concerning a consumer;~~

~~(B) To establish individual identity;~~

~~(C) For physical or biological identification or profiling; or~~

~~(D) For the generation of a deepfake.~~

(b) A business that uses ADMT in any of the ways described in section 7200, subsection (a) is not required to comply with this Article where it processes personal information for self-testing to identify, mitigate, or prevent discrimination or otherwise ensure compliance with federal and state law.

(c) A business that uses ADMT in any of the ways described in section 7200, subsection (a) is not required to comply with this Article where it processes personal information for internal research and development.

(d) A business has 24 months from the effective date of these regulations to comply with requirements related to the use of ADMT.

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

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

~~§ 7201. Requirement for Physical or Biological Identification or Profiling.~~

(a) ~~A business that uses physical or biological identification or profiling for a significant decision concerning a consumer as set forth in section 7200, subsection (a)(1), or for~~

~~extensive profiling of a consumer as set forth in section 7200, subsection (a)(2), must comply with subsections (1) and (2) below:~~

~~(1) The business must conduct an evaluation of the physical or biological identification or profiling to ensure that it works as intended for the business's proposed use and does not discriminate based upon protected classes ("evaluation of the physical or biological identification or profiling technology"). For example, a business that uses emotion assessment technology on its customer service calls to analyze the customer service employees' performance at work must conduct an evaluation to ensure that it works as intended for this use and does not discriminate based upon protected classes.~~

~~(A) Alternatively, where a business obtains the physical or biological identification or profiling technology from another person, the business must review that person's evaluation of the physical or biological identification or profiling technology, including any requirements or limitations relevant to the business's proposed use of the physical or biological identification or profiling technology.~~

~~(2) The business must implement policies, procedures, and training to ensure that the physical or biological identification or profiling works as intended for the business's proposed use and does not discriminate based upon protected classes.~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7220. Pre-use Notice Requirements.

~~(a) A business that uses ADMT **automated decisionmaking technology** as set forth in section 7200, subsection (a), may must provide consumers with a Pre-use Notice. The Pre-use Notice must inform consumers about the business's use of ADMT **automated decisionmaking technology** and consumers' rights to opt-out of ADMT and to access ADMT, as set forth in this section. A business may provide a Pre-use Notice in its Notice at Collection, provided that the Notice at Collection complies with, and includes the information required by, subsections (b) and (c).~~

~~(b) The Pre-use Notice must:~~

~~(1) Comply with section 7003, subsections (a)-(b);~~

~~(2) Be presented prominently and conspicuously to the consumer at or before the point when the business collects **processes** the consumer's personal information that the business plans to process using ADMT **automated decisionmaking technology**. If a business has already collected the consumer's personal information for a different purpose and subsequently plans to process it using ADMT for the purpose set forth in section 7200, subsection (a), the~~

business must provide a Pre-use Notice before processing the consumer's personal information for that purpose.

- (3) Be presented in the manner in which the business primarily interacts with the consumer;

(c) The Pre-use Notice must include the following:

~~(1)~~ A plain language explanation of the specific purpose for which the business plans ~~proposes~~ to use the ADMT ~~automated decisionmaking technology~~. The business must not describe the purpose in generic terms, such as "to make a significant decision" without further information because this does not describe to the consumer the specific decision for which the business plans to use ADMT with respect to them. ~~to improve our services."~~

(A) ~~For training uses of automated decisionmaking technology set forth in section 7200, subsection (a)(3), the business must identify for which specific uses the automated decisionmaking technology is capable of being used, as set forth in section 7200, subsections (a)(3)(A)–(D). The business also must identify the categories of the consumer's personal information, including any sensitive personal information, that the business proposes to process for these training uses.~~

- (2) A description of the consumer's right to opt out of ADMT and how the consumer can submit a request to opt out of ADMT.

(A) If the business is not required to provide the ability to opt out because it is relying upon the human appeal exception set forth in section 7221, subsection (b) ~~(1)(2)~~, the business must instead inform the consumer of their ability to appeal the decision and provide instructions to the consumer on how to submit their appeal.

(B) If the business is not required to provide the ability to opt out because it is relying upon another exception set forth in section 7221, subsection (b), the business must identify the specific exception it is relying upon.

- (3) A description of the consumer's right to access ADMT with respect to the consumer and how the consumer can submit their request to access ADMT to the business.

~~(A)~~ ~~If the business proposes to use automated decisionmaking technology solely for training uses of automated decisionmaking technology as set forth in section 7200, subsection (a)(3), the business is not required to include a description about the right to access ADMT, nor how the~~

~~consumer could submit their request to access ADMT to the business, as set forth in this subsection.~~

(4) ~~That the business is prohibited from retaliating against consumers for exercising their CCPA rights.~~

(5) ~~Additional information about how the ADMT automated decisionmaking technology works to make a significant decision about consumers, and how the significant decision would be made if the consumer opts out. The business may provide this information via a simple and easy to use method (e.g., a layered notice or hyperlink). The additional information must include a plain language explanation of the following:~~

~~(A) How the ADMT processes personal information to make a significant decision about consumers, including the categories of personal information that affect the output generated by the ADMT. The logic used in the automated decisionmaking technology, including the key parameters that affect the output of the automated decisionmaking technology; and~~

~~(i) For purposes of this Article, An “output” may includes predictions, decisions, content, and recommendations (e.g., numerical scores of compatibility).~~

~~(B) The type of intended output generated by of the automated decisionmaking technology ADMT and how that output is used to make a significant decision. For example, this may include whether the output is the sole factor in the decisionmaking process or what the other factors are in that decisionmaking process; and to the extent that a human is part of the decisionmaking process in a manner that does not meet the requirements of “human involvement” in section 7001, subsection (e)(1), what that human’s role is in the decisionmaking process the business plans to use the output, including the role of any human involvement. Illustrative examples follow:~~

~~(i) If the business proposes to use the automated decisionmaking technology to make a significant decision concerning a consumer, the intended output may be a numerical score of compatibility, which a human may use as a key factor to make a hiring decision.~~

~~(ii) If the business proposes to use the automated decisionmaking technology for profiling for behavioral advertising, the intended output may be the placement of a consumer into a profile~~

~~segment or category, which the business may use to determine which advertisements it will display to a consumer.~~

~~(C) What the alternative process for making a significant decision is for consumers who opt out, unless an exception to providing the opt out of ADMT set forth in section 7221, subsection (b), applies. A business relying upon the security, fraud prevention, and safety exception to providing a consumer with the ability to opt out as set forth in section 7221, subsection (b)(1), is not required to provide information that would compromise its use of automated decisionmaking technology for these security, fraud prevention, or safety purposes when complying with this subsection.~~

~~(D) If the business proposes to use automated decisionmaking technology solely for training uses of automated decisionmaking technology as set forth in section 7200, subsection (a)(3), the business is not required to include the additional information set forth in this subsection.~~

~~(d) In providing the information required by subsection (c)(5), a business's Pre-use Notice is not required to include:~~

~~(1) Trade secrets, as defined in Civil Code section 3426.1, subdivision (d); or~~

~~(2) Information that would compromise the business's ability to:~~

~~(A) Prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information;~~

~~(B) Resist malicious, deceptive, fraudulent, or illegal actions directed at the business or at consumers, or to prosecute those responsible for those actions; or~~

~~(C) Ensure the physical safety of natural persons.~~

~~(e) A business may provide a consolidated Pre-use Notice as set forth below, provided that the consolidated Pre-use Notice includes the information required by this Article for each of the business's proposed uses of ADMT automated decisionmaking technology:~~

~~(1) The business's use of a single ADMT automated decisionmaking technology for multiple purposes. For example, an employer may provide a consolidated Pre-use Notice to an employee that addresses the employer's proposed use of productivity monitoring software, which the employer also intends to use as a primary factor in to determining the employee's allocation/assignment of~~

~~work and compensation, and to determine which employees will be demoted as set forth in section 7200, subsection (a)(1)(B)(iii).~~

- (2) The business's use of multiple ADMT ~~automated decisionmaking technology~~ for a single purpose. For example, a business may provide a consolidated Pre-use Notice to a job applicant ~~consumer~~ that addresses the business's proposed use of: (1) software to screen applicants' resumes to determine which applicants it will hire, and (2) software to evaluate applicants' vocal intonation, facial expression, and gestures to determine which applicants to hire. ~~public profiling as set forth in section 7200, subsection (a)(2)(B). The consolidated Pre-use Notice may address the business's proposed use of location trackers and facial recognition technology to ensure the physical safety of natural persons.~~
- (3) The business's use of multiple ADMT ~~automated decisionmaking technology~~ for multiple purposes. For example, an educational provider may provide a consolidated Pre-use Notice to a new student that addresses the educational provider's proposed use of: (1) facial recognition technology to authenticate the student and grant them access to a secured classroom, and (2) software that automatically screens a student's work for plagiarism to determine whether they will be suspended, and (2) software that automatically assesses students' exams to determine whether to grant them a diploma or certificate.
- (4) The systematic use of a single ADMT ~~automated decisionmaking technology~~. For example, a business may provide a consolidated Pre-use Notice to an employee ~~independent contractor~~ that addresses the business's methodical and regular use of ADMT ~~automated decisionmaking technology~~ to allocate work to its employees ~~independent contractors~~, rather than the business providing a Pre-use Notice to the same employee each time it proposes to use the same ADMT ~~automated decisionmaking technology~~ to the same consumers for the same purpose.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7221. Requests to Opt-Out of ADMT.

- (a) ~~Consumers have a right to opt out of ADMT as set forth in section 7200, subsection (a).~~ A business must provide consumers with the ability to opt-out of the uses of ADMT to make a significant decision concerning the consumer that results in a significant risk to consumer privacy ~~automated decisionmaking technology, except as set forth in subsection (b).~~
- (b) A business is not required to comply with requirements as set forth in section 7200 and 7222, provide consumers with the ability to opt-out of a business's use of automated decisionmaking technology ADMT to make for a significant decision concerning a consumer as set forth in section 7200, subsection (a)(1), for work or educational

~~profiling as set forth in section 7200, subsection (a)(2)(A), or for public profiling as set forth in section 7200 (a)(2)(B),~~ in the following circumstances:

- ~~(1) The business's use of that automated decisionmaking technology is necessary to achieve, and is used solely for, the security, fraud prevention, or safety purposes listed below ("security, fraud prevention, and safety exception"):~~
 - ~~(A) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information;~~
 - ~~(B) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions; or~~
 - ~~(C) To ensure the physical safety of natural persons.~~
- (2) ~~For any significant decision concerning a consumer as set forth in section 7200, subsection (a)(1), if the business provides the consumer with a method to appeal the decision to a qualified human reviewer who has the authority to overturn the decision ("human appeal exception"). To qualify for this the human appeal exception, the business must do the following:~~
 - (A) ~~The business must d~~ Designate a human reviewer to review and analyze the output of the ADMT and any other information that is relevant to change the significant decision at issue ~~who is qualified to understand the significant decision being appealed and the consequences of the decision for the consumer.~~ This human reviewer must consider the ~~relevant~~ information provided by the consumer in support of their appeal and may consider any other sources of information about the significant decision. The human reviewer must know how to interpret and use the output of the ADMT that made the significant decision being appealed and must have the authority to change the decision based on their analysis.
 - (B) ~~The business must e~~ Clearly describe to the consumer how to submit an appeal and enable the consumer to provide information to ~~for~~ the human reviewer ~~to consider as part~~ in support of their ir appeal. The method of appeal ~~also~~ must be easy for the consumers to execute, require minimal steps, and comply with section 7004. Disclosures and communications with consumers concerning the appeal must comply with section 7003, subsections (a)–(b). The timeline for requests to appeal ADMT must comply with section 7021. Businesses must comply with the verification requirements ~~verify the consumer submitting the appeal~~ as set forth in Article 5 when a consumer submits an appeal.

- (3) For admission, acceptance, or hiring decisions as set forth in section 7001, subsections (ddd)(3)(A) and (ddd)(4)(A) ~~7200, subsections (a)(1)(A)(i), (a)(1)(B)(i)~~, if the following are true:

- (A) The business uses ~~The automated decisionmaking technology is necessary to achieve, and is used~~ solely for the business's assessment of the consumer's ability to perform at work or in an educational program to determine whether to admit, accept, or hire them; and
- (B) ~~The business has conducted an evaluation of the automated decisionmaking technology to ensure it works as intended for the business's proposed use and does not discriminate based upon protected classes ("evaluation of the automated decisionmaking technology"), and has implemented policies, procedures, and training to ensure that~~ The ADMT automated decisionmaking technology works for the business's purpose as intended for the business's proposed use and does not unlawfully discriminate based upon protected classes characteristics ("accuracy and nondiscrimination safeguards").
- ~~(i) Alternatively, where a business obtained the automated decisionmaking technology from another person, the business has reviewed that person's evaluation of the automated decisionmaking technology, including any requirements or limitations relevant to the business's proposed use of the automated decisionmaking technology, and has implemented accuracy and nondiscrimination safeguards.~~

For allocation/assignment of work and compensation decisions as set forth in section 7001, subsection (ddd)(4)(B) ~~7200, subdivision (a)(1)(B)(ii)~~, if the following are true:

- (C) The business uses ~~The ADMT automated decisionmaking technology is necessary to achieve, and is used~~ solely for the business's allocation/assignment of work or compensation; and
- ~~(D) The ADMT works for the business's purpose and does not unlawfully discriminate based upon protected characteristics.~~ The business has conducted an evaluation of the automated decisionmaking technology and has implemented accuracy and nondiscrimination safeguards.
- ~~(i) Alternatively, where a business obtained the automated decisionmaking technology from another person, the business has reviewed that person's evaluation of the automated decisionmaking technology, including any requirements or limitations relevant to the business's proposed use of the~~

~~automated decisionmaking technology; and has implemented accuracy and nondiscrimination safeguards.~~

~~(4) For work or educational profiling as set forth in section 7200, subsections (a)(2)(A), if the following are true:~~

~~(A) The automated decisionmaking technology is necessary to achieve, and is used solely for, an assessment of the consumer's ability to perform at work or in an educational program, or their actual performance at work or in an educational program; and~~

~~(B) The business has conducted an evaluation of the automated decisionmaking technology and has implemented accuracy and nondiscrimination safeguards.~~

~~(i) Alternatively, where a business obtained the automated decisionmaking technology from another person, the business has reviewed that person's evaluation of the automated decisionmaking technology, including any requirements or limitations relevant to the business's proposed use of the automated decisionmaking technology; and has implemented accuracy and nondiscrimination safeguards.~~

~~(5) The exceptions in this subsection do not apply to profiling for behavioral advertising as set forth in section 7200, subsection (a)(2)(C), or to training uses of automated decisionmaking technology as set forth in section 7200, subsection (a)(3). A business must provide the ability to opt-out of these uses of automated decisionmaking technology in all circumstances.~~

(c) A business that uses ADMT ~~automated decisionmaking technology~~ as set forth in subsection (a) must provide two or more designated methods for submitting requests to opt-out of ADMT. A business must consider the methods by which it interacts with consumers, the manner in which the business uses the ADMT ~~automated decisionmaking technology~~, and the ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of the business's use of the ADMT ~~automated decisionmaking technology~~. At least one method offered must reflect the manner in which the business primarily interacts with the consumer. Illustrative examples and requirements follow.

(1) A business that interacts with consumers online **may must, at a minimum,** allow consumers to submit requests to opt-out through an interactive form accessible via an opt-out link that is provided **on their website or** in the **Privacy Policy Pre-use Notice. The link title must state what the consumer is opting out of, such as be titled "Opt out of Automated Decisionmaking Technology."**

- (2) A business that interacts with consumers in person and online may provide an in-person method for submitting requests to opt-out in addition to the online form.
- (3) Other methods for submitting requests to opt-out include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, and a form submitted through the mail.
- ~~(4) A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to opt-out of the business's use of ADMT automated decisionmaking technology because cookies concern the collection of personal information and not necessarily the use of ADMT automated decisionmaking technology. An acceptable method for submitting requests to opt out must be specific to the right to opt out of the business's use of the ADMT automated decisionmaking technology.~~
- (d) **In lieu of posting an opt-out link, a business may include this additional opt-out on the webpage of the Alternative Opt-out Link in accordance with Section 7015.**
- (e) A business's methods for submitting requests to opt-out of ADMT must be easy for consumers to execute, must require minimal steps, and must comply with section 7004.
- (f) A business must not require a consumer submitting a request to opt-out of ADMT automated decisionmaking technology to create an account or provide additional information beyond what is necessary to direct the business to opt-out the consumer.
- (g) A business must not require a verifiable consumer request for a request to opt-out of ADMT set forth in subsection (a). A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer whose information is subject to the business's use of automated decisionmaking technology. However, to the extent that the business can comply with a request to opt-out of ADMT without additional information, it must do so.
- (h) If a business has a good-faith, reasonable, and documented belief that a request to opt-out of ADMT is fraudulent, the business may deny the request. The business must inform the requestor that it will not comply with the request and must provide to the requestor an explanation why it believes the request is fraudulent.
- ~~(i) A business must provide a means by which the consumer can confirm that the business has processed their request to opt out of ADMT automated decisionmaking technology.~~
- (j) In responding to a request to opt-out of ADMT, a business may present the consumer with the choice to allow specific uses of automated decisionmaking technology **as long**

~~as the business also offers a single option to opt out of all of the business's uses of ADMT-automated decisionmaking technology set forth in subsection (a)~~

- (k) A consumer may use an authorized agent to submit a request to opt-out of ADMT as set forth in subsection (a) on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf.
- (l) Except as allowed by these regulations, a business must wait at least 12 months from the date the business receives the consumer's request to opt-out of ADMT before asking a consumer who has exercised their right to opt-out of ADMT, to consent to the business's use of the ADMT ~~automated decisionmaking technology~~ for which the consumer previously opted out.
- (m) A business must not retaliate against a consumer because the consumer exercised their opt-out right as set forth in Civil Code section 1798.125 and Article 7 ~~of these regulations~~.
- (n) If the consumer submits a request to opt-out of ADMT before the business has initiated that processing, the business must not initiate processing of the consumer's personal information using that ADMT ~~automated decisionmaking technology~~.
- (o) If the consumer did not opt-out **prior to the commencement of processing in response to the Pre-use Notice**, and submitted a request to opt-out of ADMT after the business initiated the processing, the business must comply with the consumer's opt-out request by:
 - (1) Ceasing to **engage in such ADMT in connection with such consumer using the consumer's personal information-process the consumer's personal information using that ADMT** ~~automated decisionmaking technology~~ as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. ~~For personal information previously processed by that automated decisionmaking technology, the business must neither use nor retain that information;~~ and
 - (2) Notifying all the business's service providers, contractors, or other persons to whom the business has disclosed or made personal information available to process the consumer's personal information using that ADMT ~~automated decisionmaking technology~~, that the consumer has made a request to opt-out of that ADMT and instructing them to comply with the consumer's request to opt-out of that ADMT within the same time frame.

(a) In honoring a business's ADMT opt-out request, a business shall not be required to include:

(1) Trade secrets, as defined in Civil Code section 3426.1, subdivision (d); or

(A) Prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information;

(B) Resist malicious, deceptive, fraudulent, or illegal actions directed at the business or at consumers, or to prosecute those responsible for those actions; or

(C) Ensure the physical safety of natural persons.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125 and 1798.185, Civil Code.

§ 7222. Requests to Access ADMT Used to Process Personal Information.

(a) ~~Consumers have a right to access ADMT when a business uses automated decisionmaking technology as set forth in section 7200, subsections (a)(1)–(2).~~ A business that uses ADMT automated decisionmaking technology to make a significant decision ~~for these purposes~~ must provide a consumer with information about this use ~~these uses~~ when responding to a consumer's request to access ADMT, ~~except as set forth in subsection (a)(1).~~

~~(1) A business that uses automated decisionmaking technology solely for training uses of automated decisionmaking technology, as set forth in section 7200, subsection (a)(3), is not required to provide a response to a consumer's request to access ADMT. The business must still comply with section 7024.~~

(b) When responding to a consumer's request to access ADMT, a business must provide plain language **explanations of with** the following information to the consumer:

(1) The **statement of the specific purpose for which the business used** ~~for which the business used~~ ADMT to process the consumer's personal information to reach a significant decision that presented a significant risk to consumer privacy ~~automated decisionmaking technology with respect to the consumer.~~ **The business must not describe the purpose in generic terms, such as "to improve our services."**

~~(2)~~ Information about the logic of the ADMT, where logic means: Such information must enable a consumer to understand how the ADMT processed their personal information to generate an output with respect to them, which may include the parameters that generated the output as well as the specific ~~The~~

~~output of the automated decisionmaking technology with respect to the consumer. If the business has multiple outputs with respect to the consumer, the business may provide a simple and easy to use method by which the consumer can access all of the outputs.~~

- (A) The personal characteristics or attributes that the ADMT will measure or assess.
- (B) The method by which the ADMT measures or assesses those attributes or characteristics.
- (C) How those attributes or characteristics contribute to the significant decision.
- (D) The format and structure of the ADMT's outputs.
- (E) How those outputs are used to make, be a substantial factor in making, a significant decision.
- (F) A summary of the most recent impact assessment performed on the ADMT.

(3) ~~The outcome of the decisionmaking process for the consumer, including how the business used the output of the ADMT to make a significant decision with respect to the consumer. For example, this may include information about whether the output was the sole factor to make the decision; and if it was not the sole factor, which other factors played a role in making the decision; and to the extent that a human was part of the decisionmaking process in a manner that does not meet the requirements of "human involvement" in section 7001, subsection (e)(1), what that human's role was in the decisionmaking process.~~

- ~~(A) If the business also plans to use the output to make an additional significant decision concerning the consumer in the future, the business's explanation must include how the business plans to use that output to make a significant decision about the consumer in the future. For example, this may include whether the output will be the sole factor in the decisionmaking process or what the other factors will be in that decisionmaking process; and to the extent that a human will be part of the decisionmaking process in a manner that does not meet the requirements of "human involvement" in section 7001, subsection (e)(1), what that human's role will be in the decisionmaking process.~~
~~used the output of the automated decisionmaking technology to make a significant decision concerning the consumer as set forth in section 7200, subsection (a)(1), this explanation must include the role the output played in the business's decision and the role of any human involvement.~~

- ~~(i) If the business also plans to use the output to make a significant decision concerning the consumer as set forth in section 7200, subsection (a)(1), the business's explanation may additionally include how the business plans to use the output to make a decision, and the role of any human involvement.~~
- ~~(B) If the business used automated decisionmaking technology to engage in extensive profiling of the consumer as set forth in section 7200, subsection (a)(2), this explanation must include the role the output played in the evaluation that the business made with respect to the consumer.~~
- ~~(i) If the business also plans to use the output to evaluate the consumer as set forth in section 7200, subsection (a)(2), the business's explanation must additionally include how the business plans to use the output to evaluate the consumer.~~
- ~~(4) How the automated decisionmaking technology worked with respect to the consumer. At a minimum, this explanation must include subsections and (B):~~
 - ~~(A) How the logic, including its assumptions and limitations, was applied to the consumer; and~~
 - ~~(B) The key parameters that affected the output of the automated decisionmaking technology with respect to the consumer, and how those parameters applied to the consumer.~~
 - ~~(C) A business also may provide possible outputs the range of possible outputs or aggregate output statistics to help a consumer understand how they compare to other consumers. For example, a business may provide the five most common outputs of the automated decisionmaking technology, and the percentage of consumers that received each of those outputs during the preceding calendar year.~~
 - ~~(D) A business relying upon the security, fraud prevention, and safety exception to providing a consumer with the ability to opt out as set forth in section 7221, subsection (b)(1), is not required to provide information that would compromise its use of automated decisionmaking technology for these security, fraud prevention, or safety purposes.~~
- (5) That the business is prohibited from retaliating against consumers for exercising their CCPA rights, and instructions for how the consumer can exercise their other CCPA rights. These instructions must include any links to an online request form or portal for making such a request, if offered by the business.

- (A) ~~The business may comply with the instructions requirement by providing a link that takes the consumer directly to the specific section of the business's privacy policy that contains these instructions. Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain these instructions, so that the consumer is required to scroll through other information in order to find the instructions, does not satisfy the instructions requirement.~~
- (c) In providing the information required by subsections (b)(2)–(3), a business's response to a consumer's request to access ADMT is not required to include:
- (1) Trade secrets, as defined in Civil Code section 3426.1, subdivision (d); or
- (A) Prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information;
- (B) Resist malicious, deceptive, fraudulent, or illegal actions directed at the business or at consumers, or to prosecute those responsible for those actions; or
- (C) Ensure the physical safety of natural persons.
- (d) A business's methods for consumers to submit requests to access ADMT must be easy to use and must ~~not use dark patterns~~ **comply with Section 7004**. A business may use its existing methods to submit requests to know, delete, or correct as set forth in section 7020 for requests to access ADMT.
- (e) A business must comply with the verification requirements ~~verify the identity of the person making the request to access ADMT as~~ set forth in Article 5 for requests to access ADMT. If a business cannot verify the identity of the person making the request to access ADMT, the business must inform the requestor that it cannot verify their identity.
- (f) If a business denies a consumer's verified request to exercise their right to access ADMT, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business must inform the requestor and explain the basis for the denial, unless prohibited from doing so by law. If the request is denied only in part, the business must disclose the other information sought by the consumer.
- (g) A business must use reasonable security measures when transmitting the requested information to the consumer.
- (h) If a business maintains a password-protected account with the consumer, it may comply with a request to access ADMT by using a secure self-service portal for consumers to access, view, and receive a portable copy of their requested information if the portal

fully discloses the requested information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 5.

- (i) A service provider or contractor must provide assistance to the business in responding to a verifiable consumer request to access ADMT, including by providing the business with the consumer's personal information it has in its possession that it collected pursuant to their written contract with the business, or by enabling the business to access that personal information.
- (j) A business that used an ~~ADMT-automated decisionmaking technology~~ **with respect to a consumer** more than ~~two~~ **four** times within a 12-month period may provide an aggregate-level response to the consumer's request to access ADMT. Specifically, for the information required by subsection ~~(b)(2)-(4)~~, the business may provide a summary of the outputs **with respect to the consumer** over the preceding 12 months; ~~the key parameters that, on average over the preceding 12 months, affected the outputs with respect to the consumer; and a summary of how those parameters generally applied to the consumer.~~
- (k) A business must not retaliate against a consumer because the consumer exercised their right to access ADMT as set forth in Civil Code section 1798.125 and Article ~~7 of these regulations.~~
- (l) Nothing in this section prohibits a business from providing additional information to enable a consumer to understand how the ADMT was used to make a significant decision with respect to them. For example, a business may provide the range of possible outputs or aggregate output statistics to help a consumer understand how they compare to other consumers, such as the five most common outputs of the ADMT and the percentage of consumers that received each of those outputs during the preceding calendar year.
- (m) ~~Additional notice requirement regarding the right to access ADMT when a business used automated decisionmaking technology for certain significant decisions. A business that used automated decisionmaking technology to make certain significant decisions that were adverse to the consumer ("adverse significant decision"), as set forth in subsection (1) below, must provide the consumer with notice of their right to access ADMT as set forth in subsection (2) below, as soon as feasibly possible but no later than 15 business days from the date of the adverse significant decision.~~
 - ~~(1) A significant decision concerning a consumer that was adverse to the consumer is a significant decision that:~~
 - ~~(A) Resulted in a consumer who was acting in their capacity as a student, employee, or independent contractor being denied an educational~~

~~credential; having their compensation decreased; or being suspended, demoted, terminated, or expelled; or~~

~~(B) Resulted in a consumer being denied financial or lending services, housing, insurance, criminal justice, healthcare services, or essential goods or services.~~

~~(2) The information that a business must provide to the consumer in this notice of their right to access ADMT must include:~~

~~(A) That the business used automated decisionmaking technology to make the significant decision with respect to the consumer;~~

~~(B) That the business is prohibited from retaliating against consumers for exercising their CCPA rights;~~

~~(C) That the consumer has a right to access ADMT and how the consumer can exercise their access right; and~~

~~(D) If the business is relying upon the human appeal exception set forth in section 7221, subsection (b)(2), that the consumer can appeal the decision and how the consumer can submit their appeal and any supporting documentation.~~

~~(3) If a business provides notice to consumers of adverse significant decisions in its ordinary course (e.g., a business ordinarily notifies consumers of termination decisions via email), the business may include the information required by subsection (2) in that notice, provided that the notice overall complies with the requirements of section 7003, subsections (a) (b). Alternatively, a business may provide a separate contemporaneous notice of the consumer's right to access ADMT that includes the information set forth in subsection (2).~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125 and 1798.185, Civil Code.

Grenda, Rianna@CPPA

From: Safchuk, Sherry <ssafchuk@orrick.com>
Sent: Monday, June 2, 2025 4:53 PM
To: Regulations@CPPA
Cc: Susan Milazzo
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: Comment Letter to Modified Proposed Regulations (6.2.pdf)

This Message Is From an External Sender

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

Report Suspicious

To Whom it May Concern,

Please see attached for comments from California Mortgage Bankers Association ("California MBA") and Mortgage Bankers Association ("MBA"). Please do not hesitate to reach out with any questions or comments.

Many thanks,

Sherry

Sherry-Maria Safchuk

Partner

Pronouns: she/her/hers

Orrick

Santa Monica

T 310-424-3917

ssafchuk@orrick.com



NOTICE TO RECIPIENT | This e-mail is meant for only the intended recipient of the transmission, and may be a communication privileged by law. If you received this e-mail in error, any review, use, dissemination, distribution, or copying of this e-mail is strictly prohibited. Please notify us immediately of the error by return e-mail and please delete this message from your system. Thank you in advance for your cooperation.

For more information about Orrick, please visit <http://www.orrick.com>.

In the course of our business relationship, we may collect, store and transfer information about you. Please see our privacy policy at <https://www.orrick.com/Privacy-Policy> to learn about how we use this information.

NOTICE TO RECIPIENT | This e-mail is meant for only the intended recipient of the transmission, and may be a communication privileged by law. If you received this e-mail in error, any review, use, dissemination, distribution, or copying of this e-mail is strictly prohibited. Please notify us immediately of the error by return e-mail and please delete this message from your system. Thank you in advance for your cooperation.

For more information about Orrick, please visit <http://www.orrick.com>.

In the course of our business relationship, we may collect, store and transfer information about you. Please see our privacy policy at <https://www.orrick.com/Privacy-Policy> to learn about how we use this information.



VIA E-Mail: regulations@coppa.ca.gov

June 2, 2025

California Privacy Protection Agency

Attn: Legal Division – Regulations Public Comment

2101 Arena Blvd.

Sacramento, CA 95834

RE: Comments on Modified Text of the Proposed CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations

To Whom It May Concern:

California Mortgage Bankers Association (“California MBA”) and Mortgage Bankers Association (“MBA”) (together the “Associations”) appreciate the opportunity to provide comments to the California Privacy Protection Agency’s (“CPPA”) modified “Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology [(“ADMT”)], and Insurance Companies” (“Modified Proposed Regulations”).¹ Please see the end of this letter for more information on each Association.

The Associations appreciate and support the CPPA’s goal of strengthening consumer privacy. In furtherance of that goal, it is incumbent upon us to point out that if the Proposed Modified Regulations are finalized and implemented in their current proposed form, financial institutions would face substantial operational difficulties, with minimal, if any, benefit to consumers.

First, the new definition of “significant decision” identifies “financial or lending services” as a type of significant decision, which conflicts with the express exemption the California Legislature included in the statute for information collected, processed, or disclosed pursuant to the Gramm-Leach-Bliley Act (“GLBA”)², the California Financial Information Privacy Act (“CFIPA”)³, and the Fair Credit Reporting Act (“FCRA”).⁴ California courts have consistently held that when regulations conflict with the statute authorizing an agency to engage in rulemaking, such regulations are invalid and/or void. Here, the Modified Proposed Regulations expressly conflict with the statute and, therefore, such regulations similarly would be rendered void.

¹ Cal. Privacy Prot. Agency, Modified text of Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies (proposed May 9, 2025), https://coppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_mod_txt_pro_reg.pdf (last visited May 27, 2025).

² 15 U.S.C. §§ 6801–6809.

³ Cal. Fin. Code §§ 4050–4060.

⁴ 15 U.S.C. § 1681 *et seq.*

Second, if the definition of “significant decision” includes the definition for “financial or lending services,” then certain underwriting technologies overseen by a human reviewer could be considered ADMT. This mischaracterization may require lenders to use older manual underwriting and fraud review methods that have not been frequently used to ensure they are not considered ADMTs, which would impair the cost of credit more generally.

Lastly, because real-time underwriting and fraud detection effectively requires the use of ADMT technology,⁵ ADMT requirements in the Proposed Modified Regulations are not feasible in the financial services space. As such, the Associations respectfully request omission of the reference to “financial or lending services” from the final version of the Modified Proposed Regulations.

I. Financial institutions collect information subject to the GLBA/CFIPA and FCRA to offer financial or lending services, and such information is expressly exempt from the CCPA.

The Proposed Modified Regulations attempt to regulate information that the California Legislature expressly exempted from the scope of the CCPA. In similar instances, where agencies attempt to issue regulations expressly prohibited by statute, California courts have uniformly deemed the conflicting proposed regulations void.

The California Legislature expressly exempted⁶ the following categories of information from the CCPA’s coverage:

1. Personal information collected, processed, sold, or disclosed pursuant to the GLBA and CFIPA (collectively, “GLBA exemption”); and
2. Any activity involving the collection, maintenance, disclosure, sale, or use of personal information bearing on a consumer’s creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by consumer-reporting agencies, furnishers, and users of consumer reports subject to the FCRA (“FCRA exemption”).⁷

Based on these exemptions, most information a company obtains in connection with a financial product or service is expressly exempt from the CCPA. Specifically, the GLBA and its implementing Regulation P (as well as the California equivalent – CFIPA) apply to “nonpublic personal information” (“NPI”), which includes any information:

- Provided by a consumer to obtain a financial product or service;
- Resulting from any transaction involving a financial product or service; or

⁵ See Board of Governors of the Federal Reserve System, et al., *Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing* (Dec. 3, 2018), <https://www.occ.treas.gov/news-issuances/news-releases/2018/nr-occ-2018-130a.pdf>.

⁶ Apart from the data breach private right of action, which is not discussed further herein. See Cal. Civ. Code § 1798.150(c).

⁷ Cal. Civ. Code § 1798.145(d), (e).

- Otherwise obtained in connection with providing a financial product or service to that consumer.⁸

Similarly, the FCRA applies to information contained in “consumer reports,”⁹ which includes any communication of information used or expected to be used in establishing a consumer’s eligibility for credit, among other things. The FCRA also applies to entities that offer consumer report information about individuals and sell such reports to third parties.¹⁰ Thus, activities involving loan applications, mortgage origination, servicing, default management, and secondary-market transactions, among others, all require the routine exchange of both NPI and FCRA data, and are therefore expressly exempt from the CCPA.

The GLBA and other federal law broadly define the term “financial product or service” to cover “any product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity.”¹¹ In other words, any product or service a financial institution offers to a consumer likely would be considered a “financial product or service,” such that any information obtained in connection with any product or service provided by a financial institution would be considered NPI subject to GLBA/CFIPA/FCRA, and accordingly exempt from the CCPA.

The Proposed Modified Regulations attempt to regulate information expressly exempt from the CCPA in direct conflict with the California Legislature’s mandate in the CCPA. The Proposed Modified Regulations set forth requirements that apply to ADMTs used to make significant decisions, including “the provision or denial of financial or lending services.” This phrase is further defined to mean “the extension of credit or a loan, transmitting or exchanging funds, the provision of deposit or checking accounts, check cashing, or installment payment plans.”¹² However, any information collected and used to approve or deny a financial or lending service is inherently NPI and subject to the GLBA and/or FCRA, and accordingly, expressly exempt from the CCPA.¹³ As a result, this provision of the Proposed Modified Regulations directly conflicts with the CCPA.

California law is clear that “[e]ach regulation adopted, to be effective, shall be *within the scope of authority* conferred and in accordance with standards prescribed by other provisions of law.”¹⁴ Consistent with this mandate and the Constitutional separation of powers between the legislative and executive branches in California,¹⁵ state courts have consistently held that regulations that conflict with a statute providing rulemaking authority are void or invalid. In other words, “[a] valid regulation must fit ‘within the scope of authority conferred’ by the Legislature.”¹⁶ In *Fipke v. California Horse Racing Board*, 55 Cal. App. 5th 505, 516 (2020), the court prohibited

⁸ 12 C.F.R. § 1016.3(q)(1); Cal. Fin. Code § 4050 *et seq.*

⁹ 15 U.S.C. § 1681a(d); Cal. Fin. Code § 4050 *et seq.*

¹⁰ 15 U.S.C. § 1681a(d).

¹¹ 12 U.S.C. 1843(k); 12 C.F.R. § 1016.3(m)(1).

¹² Cal. Privacy Prot. Agency, Proposed Modified Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (“ADMT”), and Insurance Companies (May 9, 2025), https://cippa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_mod_txt_pro_reg.pdf (last visited May 27, 2025).

¹³ See 15 U.S.C. § 6801 *et seq.* (2018) (GLBA); 15 U.S.C. § 1681 *et seq.* (FCRA)

¹⁴ Cal. Gov. Code § 11342.1 (emphasis added).

¹⁵ Cal. Const. art. III, § 3.

¹⁶ See *id.*; *Ass’n of Cal. Ins. Cos. v. Jones*, 2 Cal. 5th 376, 406 (2017).

a California agency from awarding a specific fee because the fee conflicted with the statute, and therefore, “exceeded the scope of the stewards’ authority and is void.” Courts have also found this to be the case when a California agency creates additional exemptions beyond those expressly excluded from the statute.¹⁷ The *Bearden* court summarized the relevant law as follows:

The authority of an administrative agency to adopt regulations is limited by the enabling legislation. “[A]n administrative regulation must ‘be within the scope of authority conferred and in accordance with standards prescribed by other provisions of law.’ (Gov.Code, § 11342.1.) ‘Whenever by the express or implied terms of any statute a state agency has authority to adopt regulations to implement, interpret, make specific or otherwise carry out the provisions of the statute, no regulation adopted is valid or effective unless consistent and not in conflict with the statute and reasonably necessary to effectuate the purpose of the statute.’ (Gov.Code, § 11342.2.)” (*Agnew v. State Bd. of Equalization* (1999) 21 Cal.4th 310, 321, 87 Cal.Rptr.2d 423, 981 P.2d 52 (*Agnew*).)

“Even apart from these statutory limits, it is well established that the rulemaking power of an administrative agency does not permit the agency to exceed the scope of authority conferred on the agency by the Legislature. (California Emp. Com. v. Kovacevich (1946) 27 Cal.2d 546 [165 P.2d 917].) ‘A ministerial officer may not ... under the guise of a rule or regulation vary or enlarge the terms of a legislative enactment or compel that to be done which lies without the scope of the statute and which cannot be said to be reasonably necessary or appropriate to subserving or promoting the interests and purposes of the statute.’ (First Industrial Loan Co. v. Daugherty (1945) 26 Cal.2d 545, 550 [159 P.2d 921].) And, a regulation which impairs the scope of a statute must be declared void. (Association For Retarded Citizens v. Department of Developmental Services (1985) 38 Cal.3d 384, 391 [211 Cal.Rptr. 758, 696 P.2d 150]; Morris v. Williams (1967) 67 Cal.2d 733, 748 [63 Cal.Rptr. 689, 433 P.2d 697].)” (Agnew, supra, 21 Cal.4th at p. 321, 87 Cal.Rptr.2d 423, 981 P.2d 52; Colmenares v. Braemar Country Club, Inc. (2003) 29 Cal.4th 1019, 1029, 130 Cal.Rptr.2d 662, 63 P.3d 220.)

Id. (emphasis added). The opposite is also true (*i.e.*, removing an exemption), such that this principle should apply in this scenario as well.

The CPPA does not have authority to remove exemptions other than those necessary to implement the requirements imposed by the California Legislature, which is not the case here.¹⁸ Thus, if the CCPA finalizes a definition of “significant decision” that includes “lending and financial services,” such definition would directly conflict with the CCPA exemption for NPI subject to GLBA and FCRA-data, and would be invalidated because it exceeds the scope of authority the California Legislature conferred upon the CPPA. Given that the statute sets forth the express exemption for GLBA and FCRA data, the only way for the CPPA to change the exemption is through a statutory amendment by the California Legislature.¹⁹

¹⁷ See *Bearden v. U.S. Borax, Inc.*, 138 Cal. App. 4th 429, 436 (2006).

¹⁸ See Cal. Civ. Code § 1798.185 (enumerating the CPPA’s rulemaking authority under the CCPA).

¹⁹ See Cal. Civ. Code § 1798.145(d)–(e).

II. If the term “significant decision” continues to reference “financial or lending services,” then certain financial/lending tools may be considered ADMTs, which would require lenders to use older manual underwriting or fraud review methods that have not been frequently used, may be inaccurate, and impair the cost of credit.

If the definition of “significant decision” references “financial or lending services,” then some application, underwriting, and fraud review systems—including systems that have been used for decades— may be considered ADMTs²⁰ subject to Modified Proposed Regulations. As expressly defined in the Modified Proposed Regulations, the CCPA would apply to any ADMT that provides for “the extension of credit or a loan, transmitting or exchanging funds, the provision of deposit or checking accounts, check cashing, or installment payment plans.”²¹ This would include core activities by financial institutions such as preapproving consumers for an offer of credit, approving an application for credit, setting the terms of a financial product or service (for example, the downpayment amount on a mortgage), and identifying and combatting fraud—activities that plainly use NPI obtained under the GLBA and CFIPA, as well as information obtained under the FCRA, which is exempt from the CCPA’s scope. Applying the CCPA to these processes would have ramifications in the financial or lending service space and may impair the cost of credit as discussed further below.

If offering financial or lending services is included in the definition of “significant decision,” then the following types of technology may be considered ADMTs:

- **BSA/AML/KYC Reviews:** Financial institutions regularly use ADMT-type technology to identify and combat fraud and comply with the Bank Secrecy Act, Anti-Money Laundering requirements, and Know Your Customer (“KYC”) reviews. Indeed, federal banking regulators have evaluated ADMT-type technology and “welcome these types of innovative approaches to further efforts to protect the financial system against illicit financial activity.”²²
- **Online Mortgage Lenders and Other Lending Platforms:** Many financial institutions use technology to streamline the loan application process and enhance the customer experience. These technologies rely on applying algorithms to applicants’ financial information to facilitate the mortgage origination process, without the need for human intervention—a process that is likely to be considered an ADMT.

²⁰ The Proposed Modified Regulations broadly define “automated decisionmaking technology” or “ADMT” as “any technology that processes personal information and uses computation to replace human decisionmaking, or substantially replace human decisionmaking.” “Substantially replace human decisionmaking” means a business uses the technology’s output to make a decision without human involvement. *See* Cal. Privacy Prot. Agency, Proposed Text of Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Regulations § 7001(e)(1) (May 9, 2025), https://coppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_mod_txt_pro_reg.pdf. “Human involvement” requires the human reviewer to: (A) know how to interpret and use the technology’s output to make the decision; (B) review and analyze the output of the technology, and any other information that is relevant to make or change the decision; and (C) have the authority to make or change the decision based on their analysis in subsection (B). *Id.*

²¹ *See id.*

²² *See* Board of Governors of the Federal Reserve System et al., *Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing* (Dec. 3, 2018), <https://www.occ.treas.gov/news-issuances/news-releases/2018/nr-occ-2018-130a.pdf>.

- **Automated Loan Underwriting:** There are technologies that originate consumer loans using automated underwriting processes that are required to be used for a mortgage loan to be eligible for securitization or an agency guarantee. Automated underwriting systems analyze financial metrics to facilitate lending decisions.
- **Automated Credit Scoring and Microfinance Platforms:** There are financial institutions that use consumer data to determine credit risk for individuals. These can rely on non-traditional data sources to make lending decisions. Some financial institutions use machine learning algorithms to evaluate credit risk based on personal data, instead of using traditional human-based credit scoring methods. These types of technologies expand access to credit.

The foregoing is only a couple of examples of the types of technology in the lending space that may be considered ADMTs. If the CCPA applies to such technology, many lenders will not be able to offer products to California consumers in a cost-effective manner. This would result in less accessible credit and/or higher costs for obtaining credit, which directly impacts California residents.

III. The ADMT requirements in the Modified Proposed Regulations are not feasible to implement.

The Proposed Modified Regulations set forth several requirements that would apply to “significant decisions” made by ADMTs, many of which are not feasible when offering financial or lending services or products. If finalized, a business that uses ADMTs to make a “significant decision” concerning a consumer would be required to provide consumers with the following:

- **Pre-Use Notice:** A Pre-use Notice that informs consumers about the business’s use of ADMT, a consumer’s rights to opt-out of ADMT, and the ability to access information regarding the ADMT (discussed further below) (“Pre-use Notice”). Implementing a Pre-use Notice in the lending and financial space does not provide any additional consumer benefit. The relationship between an individual and a financial institution is unique in the sense that customers willingly provide personal information to financial institutions to obtain a mortgage, *e.g.*, applicant-supplied information, as opposed to collecting personal information that the customer is unaware of. In these instances, the customer knows how the financial institution will use their personal information – *i.e.*, to obtain a mortgage. In addition, when a customer files an application, they receive numerous disclosures regarding the financial product and service, including the information on the NPI that will be processed in connection with an application, such that providing customers with another disclosure may be repetitive. Further, if a customer is already receiving numerous disclosures in connection with the product or service, one more notice would be lost in all the paper and not have much impact.
- **Right to Opt-out or Appeal:** The ability to opt-out of the use of ADMT to make significant decisions regarding the consumer and providing a method to appeal the decision for manual review by a human reviewer is very difficult to implement in the financial or lending space.

Implementing a manual process to handle decisions is costly, inefficient, and may make a loan ineligible for securitization or guarantee. Creating a manual process would require relying on a human-led process, which would lead to inconsistent and subjective outcomes. This requirement would drastically slow down the lending processes, impacting the institution's ability to provide timely services and a customer's ability to use the funds from the loan. Further, if individuals are able to opt-out of AML, BSA, and fraud reviews, all consumers would be impacted by the increase in fraud that may have been otherwise identified by ADMTs. Moreover, if the number of appeals is elevated, human reviewers may not be able to handle the sheer volume of appeals, leading to delays and increased costs, and may hinder access to credit, and result in upset and frustrated customers.

- **Right to Access:** Information about the use of the ADMT to make a significant decision, such as the specific purposes of the use, information about the logic of the ADMT, and the outcome of the decision-making process for the consumer, among other disclosure requirements. Providing consumers with detailed information about the use of ADMT, including the logic behind decisions and the specific purposes for the use of ADMT, does not provide a significant consumer benefit for the costs of compliance. Further, if financial institutions are required to describe how a “significant decision” would be made without ADMT, then such institutions will face complexity outlining alternative manual processes that may not exist or be practical. Manual decision-making is inherently slower and more prone to human error, which results in inconsistent outcomes and undermines the efficiency and accuracy that ADMT may provide. Furthermore, explaining algorithmic processes in a way that is understandable to consumers would require significant effort and expertise, and may ultimately confuse the consumer. The requirement to disclose such detailed information could lead to frustration (especially with receiving another disclosure) and misinterpretation, potentially undermining consumer trust rather than enhancing it. In addition, financial algorithms are often unique, proprietary, and complex, and designed to analyze vast amounts of data. Disclosing the logic of these algorithms could compromise intellectual property and expose institutions to security risks. Moreover, revealing detailed information about the system could enable bad actors to better understand and potentially circumvent the institution's review processes, increasing the risk of fraud for all financial institutions.

For consumer lenders in particular, the right to access is redundant and unnecessary, as the federal Equal Credit Opportunity Act (“ECOA”) requires creditors to provide applicants with notice of adverse action and the specific principal reasons for any adverse action.²³ Similarly, when a company uses a credit report obtained under FCRA and declines a consumer's request for credit, employment, housing or otherwise based upon the information in that credit report, the company must provide a similar adverse action notice regarding credit scores and the right to obtain a free copy of the consumer report, when applicable, under the Equal Credit Opportunity Act and the FCRA. These requirements apply equally to decisions made using complex algorithms or ADMTs, are duplicative of the CCPA's requirements, and create confusion for consumers and companies alike.

²³ 12 C.F.R. 1002.9.

IV. Conclusion and Recommended Revisions

For the reasons set forth above, we respectfully request that the CPPA remove reference to “financial or lending services” from the definition of “significant decision.”

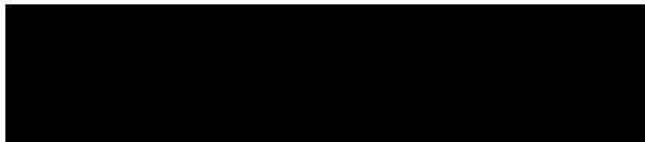
We appreciate the CPPA’s thoughtful engagement with stakeholders and its willingness to refine the draft rules. By aligning the modified regulations with the statutory text and the comprehensive federal and California framework governing financial institutions, the CPPA will avoid duplicative requirements, preserve consumer protections already in place, and ensure consistent application of privacy principles across industries.

Should you have any questions regarding these comments, or if we may provide further information, please contact the undersigned.

Respectfully submitted,



Susan Milazzo
California Mortgage Bankers Association
susan@cmba.com



William Kooper, MPA
Mortgage Bankers Association
WKooper@mba.org

Background on Associations

California MBA has been a leading trade association for the California mortgage banking industry for the past 60 years, and has been an active advocate for real estate finance in California during that time. California MBA has actively participated in, and supported, efforts to ensure adequate and effective regulation of the mortgage industry, and protection for California consumers, including by working with lawmakers to enact the existing California

Residential Mortgage Lending Act (CRMLA), and participating in the debate over Proposition 13, the California Homeowner's Bill of Rights, and implementation of the SAFE Act, among others. In addition to its advocacy efforts, California MBA provides its members with education and analysis to facilitate the use of best practices, and to ensure members remain up to date on industry trends and regulatory requirements. For additional information, visit California MBA's website: <https://cmba.com/>.

The Mortgage Bankers Association (MBA) is the national association representing the real estate finance industry, an industry that employs more than 390,000 people in virtually every community in the country. Headquartered in Washington, D.C., the association works to ensure the continued strength of the nation's residential and commercial real estate markets, to expand homeownership, and to extend access to affordable housing to all Americans. MBA promotes fair and ethical lending practices and fosters professional excellence among real estate finance employees through a wide range of educational programs and a variety of publications. Its membership of more than 2,100 companies includes all elements of real estate finance: independent mortgage banks, mortgage brokers, commercial banks, thrifts, REITs, Wall Street conduits, life insurance companies, credit unions, and others in the mortgage lending field. For additional information, visit MBA's website: www.mba.org.

Grenda, Rianna@CPPA

From: Jacob Brint <jacob@calretailers.com>
Sent: Monday, June 2, 2025 10:41 AM
To: Regulations@CPPA
Cc: Sarah Pollo
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT and Insurance Regulations
Attachments: Cal Retailers Comments Letter on CPPA Updates, Cyber, Risk, ADMT, and Insurance Regulations_6.2.25.pdf

This Message Is From an External Sender

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

[Report Suspicious](#)

Hello,

Attached are the California Retailers Association's comments regarding the CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations, based on the May 1st CPPA hearing.

For your reference, our comments from the February meeting are also included at the end of the letter.

Best,

Jacob Brint

Legislative and Regulatory Manager

California Retailers Association

1121 L Street, Suite 607

Sacramento, CA 95814

O: (916) 443-1975

C: [REDACTED]

jacob@calretailers.com





June 2, 2025

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

VIA Email: regulations@coppa.ca.gov

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

Dear Members of the Committee:

The California Retailers Association (Cal Retailers) is submitting the following concerns we have on the modified regulatory text, which is based on the May 1 CCPA hearing, regarding Automated Decision-making Technology (“ADMT”), risk assessments, and cybersecurity. We have also attached our original letter submitted to the CCPA in February for reference.

§ 7001(e) – ADMT Definition:

Request to revise as follows:

- On 1(b), revise: “information that is relevant necessary to make . . .” As currently framed, it is unclear what info would be relevant and may be impossible for a human reviewer to consider all such factors. If a business has a protocol on what info is needed to make a decision or exception, then that should be sufficient.
- On (3), remove “provided that they do not replace human decision making,” as it otherwise removes the purpose of the exception. And if a company were to make a decision based solely on a calculator, while perhaps not advisable, it should not be within scope.
- On (3), add “search term software” to exclude when recruiters or employers conduct manual searches using terms to narrow the scope of a recruitment pool.

§ 7001(ddd) – Significant Decision:

Request to revise as follows:

- Under the Significant Decision definition “employment or independent contracting opportunities or compensation” should be removed.
- Under (4), Cal Retailers requests that employment related decisions be limited to hiring or firing—not decisions related to allocation or assignment of work, compensation, bonuses, etc.

§ 7010 (d):

Cal Retailers seeks the removal of this provision. A persistent option for opt-out through a link, versus a just-in-time option, is not as consumer friendly. Consumers are unlikely to have the context needed to know to access the link. The business should determine the appropriate interaction based on its relationship with the consumer and nature of the processing.

The ideal approach would give business flexibility to determine how to offer opt-out; specifically, where PI is being processed for a significant decision, a business should be able to offer the opt-out as part of the user experience that leads to that decision.

§ 7150(b):

Cal Retailers would like the removal of this provision. If this does not prove possible, we have included some feedback along with revisions below.

Feedback:

The rules still regulate the use of ADMT to process publicly available information, as a consumer's presence on a college campus or a grocery store with a pharmacy is not private information. The CPRA otherwise regulates the use of data collected from geo-trackers that identify a consumer's precise geolocation, regardless of the location. As sensitive data, a controller must still conduct a risk assessment (per these regs) and provide an opt out. The overbreadth would capture low risk activities such as providing discounts for (i) prescriptions at specific pharmacies based on a consumer's prior use or (ii) college merchandise based on a student's residence at a specific college.

Potential Revisions:

- (3) – Seek the below revisions to this provision:
 - Using ADMT for a significant decision concerning a consumer that presents a reasonably foreseeable risk of (A) unfair or deceptive treatment of, or unlawful disparate impact on, consumers, (B) financial, physical or reputational injury to consumers, (C) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person, or (D) other substantial injury to consumers.
- (4) – Seek removal of this provision.
- (5) – Profiling Sensitive Location – Seek removal of this provision.
- (7) - Seek the creation of a new provision utilizing the below text:
 - A risk assessment completed under another law that is substantially similar to the assessment required under this Article will satisfy the requirements of this Article.

§ 7152(a)(3) – Risk Assessment Requirements:

The purpose of the risk assessment is to make sure the business considers and weighs the privacy harms resulting from certain high-risk processing activities. As businesses continue to innovate, the nature of in-scope processing activities will change. Businesses should retain flexibility in how to approach assessments to make sure that they identify and weigh the right factors. However, the approach in the proposed rules under § 7152 is overly prescriptive and may force businesses to view assessments as a check-the-box exercise rather than focusing on the factors that ultimately matter for the assessment.

The cost of this approach to business and innovation outweighs the privacy benefits to consumers. California companies operate nationally and internationally. Under almost all other privacy laws including GDPR, a business will prepare risk assessments tailored to the processing activity rather than follow the CPPA's formulaic approach. Yet since the proposed rules do not permit a business to rely entirely on an assessment prepared to meet the requirements for another jurisdiction, a business will need to prepare a California-specific supplement for the same processing activity. The CPPA has not explained how this approach will provide incremental benefits to consumer privacy. See § 7156 below for more info.

§ 7156 Interoperability of Risk Assessments:

The modified regulatory text continues to require a California risk assessment to include all the specific requirements under this regulation. Instead, it should follow the approach of all other state privacy laws and permit businesses to rely on assessments prepared for other laws that are reasonably similar in scope and effect. For instance, Colorado requires data protection assessments for (1) processing personal data for targeted advertising (defined as equivalent to “*cross-context behavioral advertising*,” not “*behavioral advertising*”) and profiling if the profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial or physical injury to consumers; (iii) physical or other intrusion on the solitude, seclusion, or private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or (iv) other substantial injury; (2) selling personal data; and (3) processing sensitive data.

Moreover, other state privacy laws that require “*risk assessments*” (i.e. “*data protection assessments*”) for high-risk activity limit the scope of activities requiring such assessments in similar circumstances to (1) the processing of “*sensitive data*,” which could include location information ***but only when such data is precise geolocation information***, and (2) profiling, ***but only when it presents a reasonably foreseeable risk of the following***: unfair or deceptive treatment of (or unlawful disparate impact on) consumers, financial or physical injury, physical or other intrusion on the solitude or seclusion – or private affairs or concerns – of consumers if it would be offensive to a reasonable person (***hardly the case in a publicly available space, where consumers do not have a reasonable expectation of privacy***), or other substantial injury.

As currently written, the draft rules contemplate interoperability only between similar “*risk assessments*” and do not contemplate “*data protection assessments*.” Further, the draft rules are rather stringent in requiring that a company may only forego a risk assessment if (1) the other “*risk assessment*” created for the purpose of complying with another law or regulation “*meets all the requirements of this Article*,” and (2) if it covers a “*comparable set of processing activities*,” defined as processing activities that “*present similar risks to consumers’ privacy*.” Of course, an entity would not know if an activity presented similar risks until it conducts the risk assessment, thereby the purpose of this provision.

(F): This is an example of how the rule leans more toward the prescriptive rather than functional. Section (a)(1) already requires an assessment to identify the processing purpose, and then (a)(3)(F) requiring mapping those purposes to specific third parties. A business should consider in its assessment both processing purposes and sharing, but this mapping will not always be necessary—especially when a business already discloses categories of data sharing in its privacy notice and the purpose of processing in its agreements with service providers.

(G)(1) [limited to significant decisions]: As described below at § 7220(c)(5), research is still ongoing in how to explain the logic of ADMT models. Moreover, the focus on methodology is not tethered to the risk to the consumer—privacy or otherwise. Instead, the risks are related to an adverse impact of a significant decision and whether a data subject can exercise rights. These are sufficiently addressed by other RA provisions.

§ 7157 Submission of Risk Assessments to the Agency:

The draft rules require companies to submit abridged forms of their risk assessments on an annual basis to the CPPA. Routine submission is not only burdensome, but inconsistent with other state privacy laws and may result in reduced privacy protections as businesses may prepare assessments in a way that is legally protective rather than focused on the right risk-benefit balancing.

However, the CPRA statute mandates that the CPPA issue regulations that require submission at a regular cadence. For instance, the statute does not preclude the CPPA from setting separate standards for what processing activities trigger a risk assessment vs what activities are sufficiently risky to trigger a submission. This would allow the CPPA to focus on those assessments that are highest risk, such as those involving the sale of sensitive data.

Further, the rules require companies to submit risk assessments in the employment context to the regulator, but in most instances, any decisions in the employment context are confidential and not available to competitors. We'd likely need an exception to not require the submission of information that is confidential business/trade secret information.

§ 7157(b):

It is still unclear what the CPPA plans to do with this information. Per our prior points, consider limiting the requirement to certain processing activities only—e.g., sales of sensitive data. Alternatively, seek to limit the substance to metrics, i.e. the number of assessments, and drop (4). Companies are otherwise required to disclose in their privacy notice the types of personal data that they collect, process, and share. Unclear how adding this to the submissions will produce any greater benefit for the Agency.

§ 7150(a)(1) – Significant Decision:

This should be limited in the same manner and for the same reasons above at § 7150(b)(3)(A). § 7200(a)(1) extends application to all uses of ADMTs for decisions regarding provision of, denial of, or access to, employment and employment compensation. Per the regulation, this includes almost all activity within the scope of the employment lifecycle: hiring, promotion/demotion; suspension/termination; and, during employment, allocation/assignment of work; setting of base and incentive compensation; and decisions regarding “other benefits.” This also includes “independent contracting opportunities,” i.e., the same activities in the IC, gig-economy, and other emerging work contexts.

§ 7150(b)(6) – AI/ADMT Training:

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

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

§ 7200(a)(1) – Significant Decision:

See above at 7001(ddd)

The first sentence of 7200(b) should be removed—a business should not have to provide a risk assessment where ADMT was used prior to effective date and is not used on or after the effective date.

§ 7200(a)(2)(A) - Extensive Profiling (Profiling of Employees):

This should be limited in scope.

§ 7200(a)(2)(B) - Extensive Profiling (Publicly Accessible Spaces):

This should be limited in scope.

§ 7200(a)(2)(C) - Extensive Profiling (Behavioral Advertising):

This should be limited in scope.

§ 7150(a)(3) - AI/ADMT Training:

This should be limited in scope.

§ 7220(a) – When Required:

As a threshold matter, the CPRA does not permit regulations on pre-use notice of ADMT—instead, CPRA § 1798.185 calls for regulations “*governing access and opt-out rights*,” with respect to ADMT. The access right (addressed below) covers the information that a business needs to provide about its ADMT, and so CPPA should not issue separate and overlapping rules on notice.

At minimum, pre-use notice should be limited to where the ADMT processing is otherwise subject to access and opt-out rights. To the extent that one of these customer rights does not apply (e.g., relying on security or fraud prevention exception), then the business should not have an obligation to post this notice. In other words, section 7220(a) should apply subject to the exceptions in § 7221(b) and § 7222(a)(1).

This makes practical sense as forcing a business to make disclosures on how it uses ADMT to perform these functions would undermine the safety and security of consumers and businesses. The notice must provide extensive details about the use of the ADMT, which will be difficult to draft and likely not useful to the consumer, particularly where a business uses ADMT in multiple ways and must provide several notices. Consumers may not be well-equipped to evaluate information about how ADMT works and the logic behind the ADMT.

Suggested Revision:

CPPA did not revise the regulations to 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. Amend § 7220(a) as follows:

- A business that uses automated decision-making technology as set forth in section § 7200, subsection (a), and subject to the exceptions in section § 7221(b) and section § 7222(a)(1), must provide consumers with a Pre-Use Notice.

§ 7220(c)(5):

Our preference is to delete pre-use notice entirely. If pre-use notice is required, it should be limited to manageable information.

Suggested Revisions:

- Amend § 7220(c)(5)(A) as follows: The categories of personal information processed by the ADMT.
- Strike § 7220(c)(5)(B)

§ 7220 – Notices:

While the updated rules include the appropriate carveouts (§ 7200(d)), it still requires the notice to include a significant amount of information. The most problematic are (A) and (B), which requires disclosing the type of outputs generated and how the output is used to make a significant decision. Per our original concerns, the CPPA should consider whether this helps the consumer and whether risks are better mitigated through an assessment that requires rigorous testing.

On (A), unclear how it relates to 7222(b)(2) re access right, as one requires disclosing how ADMT processes personal info to decide and other the ADMT logic.

§ 7221(a) – Opt-out of ADMT:

Our preference is to delete the right to opt-out entirely, as this is administratively difficult to implement without significant consumer benefit unless there is an adverse decision. If the right cannot be deleted, it should only apply as a right to appeal in the event of an adverse decision, like the Colorado AI Act and other similar laws, as per the below.

An exception for cybersecurity uses previously included in the regulations should be re-inserted as this type of safe harbor is critical to allowing businesses to safely protect consumer data from unauthorized uses.

Suggested Revisions:

- Amend § 7221(a) to read as follows: In the event of an adverse significant decision having legal or similarly significant effect, a business must provide consumers with the ability to appeal the decision and in that appeal opt-out of the use of ADMT to make a significant decision concerning the consumer, except as set forth in subsection (b).
- Amend § 7221(b) to add the following sections and text:
 - (1) The business’s use of that automated decision-making technology is necessary to achieve, and is used solely for, the security, fraud prevention, or safety purposes listed below (“security, fraud prevention, and safety exception”):
 - (A) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information.
 - (B) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions.
 - (C) To ensure the physical safety of natural persons; or
 - (D) To protect property or rights or defend against legal claims.

§ 7221(b)(4) & (5) – Employee Exceptions: Cal Retailers requests that the CPPA remove the limiters “solely” in both exceptions—so long as the ADMT is not used to make another type of significant decision, then the opt out should not apply. As written, it suggests that the exception would not apply to ADMT that is used for both assignment of work and how the business manages its products and services—even though the latter is not a significant decision.

The standard “ensures” sets an unreasonably high bar. Propose revising to say that a business must take reasonable measures to ensure. Also, an ADMT deployer should be able to rely on an assessment or instructions from developer rather than conduct an independent assessment.

§ 7221(f)

Request to Amend entire section to the following text only:

- A business may require a verifiable consumer request for a request to opt-out of ADMT set forth in subsection (a). A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer whose information is subject to the business's use of ADMT.

§ 7222 (a) – When Access Right Applies:

This provision in the modified text still requires that business's responses be specific to the specific consumer making the request (see previous Cal retailers letter attached).

At a minimum, the access right should be limited to an adverse decision. A company should not be required to explain details about when and how it uses technology when no harm is involved, such as where a consumer is pre-approved for credit. This follows the approach of FCRA and the Equal Credit Opportunity Act. We are not aware of any other regulatory regime that requires a company to disclose how it made a non-adverse decision to a consumer. We request the removal of section § 7222 (a)(b)(2).

The same opt-out exceptions for employment uses (under § 7221(b)) should be added here. If the terms ADMT and significant decisions are broadly interpreted to include interim hiring decisions or filtering tools, then it will be impractical to require a business to respond to consumer-specific access requests on how the ADMT was applied to them, regardless of whether it was adverse. This will eliminate the advantages of using automated tools in the first place.

§ 7222(b) – Response to Access Request:

We propose limiting the right to access to situations in which the consumer has actually been subjected to an adverse significant decision. Perhaps including a Pre-Use Notice as a baseline disclosure, and then only upon an adverse decision could a consumer potentially obtain more individualized info.

Suggested Revisions:

- On (1), per above, this should be limited at minimum to where the ADMT use resulted in an adverse decision.
- On (2), this language should be removed, even if limited to were used for an adverse decision. Other regulatory regimes that require a business to explain an (adverse) decision do not require disclosing methodology (eg, under FCRA, the notice when taking an adverse action based on a consumer report must explain that an adverse action occurred, identify the consumer rights, and provide contact info of consumer reporting agency—but not the methodology of the decision making). It does not relate to any privacy risk to the consumer but instead creates a moral hazard in that the primary benefit to consumers of accessing a methodology is to either copy it for their own business needs or use it to game the system, defeating the purpose of the technology and harming all consumers.
- On (3), this is inconsistent with the definition of ADMT, which is limited to technologies that fully replace or substantially replace human decision-making. As framed, it suggests that this requirement applies to interim automated tools. To the extent the rule is seeking to inform consumers about the purpose of the decision, then that is already covered under (1). Again, the outcome at most should be limited to adverse decisions, per 7222(a) above.

§ 7222(k) – Adverse Significant Decisions:

In the employment context, the rules give companies too little time to effectively provide detailed, and in parts, data specific to each individual decision—a bar too burdensome given the broad applicability. In the case of an “*adverse significant decision*” (suspension, demotion, termination, or reduction in compensation), the business must provide notice of the right to access within 15 days of the adverse decision, and with detailed information within 45 days. Upon request, the business must provide “*a plain language explanations*” — requiring interpretation — of the purpose of the ADMT, and more concerningly, (a) the specific outputs the ADMT produced after processing the individual’s data; (b) the way in which the business used (and plans to use) the ADMT output and human assessment in making decisions regarding that individual; (c) the “*extensive profiling*”, if any, performed by the business using an ADMT; and (d) the precise “*logic*”, “*key parameters*”, and “*range of possible outputs or aggregate output statistics*” of the ADMT, so the individual can understand the workings of the tool and how the specific decision came to be. Little of this information will be helpful to the individual and will require extensive interpretation on behalf of a company to produce this information in “*plain language*” to an individual—often in each specific “*adverse significant decision*.”

Behavioral Advertising – Fallback:

The scope of covered ADMT under § 7200 should not include profiling of a consumer, or at minimum, should exclude behavioral advertising. If not, then the draft should at minimum not apply the access right to this type of ADMT processing.

Suggested Revisions:

See previous comments to strike “*behavioral advertising*.”

We also have concerns with the way § 7123(f) is currently drafted. As written, it is effectively useless as it says another audit can only be used if another audit has all the same requirements as the CCPA audit. No other audit regime looks like the CCPA audit, so businesses will always be required to conduct a separate audit for CCPA. Most businesses already conduct annual audits for ISO certification. We suggest the regulations include common security audit frameworks that will be accepted as compliant with these regulations without requiring businesses to make the determination whether they meet all the requirements the agency requires.

Related to this, the specific controls outlined in § 7123(b) risk becoming outdated quickly. Most current cybersecurity audit standards focus on assessing how organizations achieve security outcomes. For example, NIST recommends controls such as: “The confidentiality, integrity, and availability of data-at-rest are protected.” In contrast, the proposed regulations mandate specific technical controls to achieve these outcomes—for instance, requiring assessment of “Encryption of personal information, at rest.” As an example, § 7123(b)(2)(A) emphasizes multi-factor authentication (MFA) and password requirements, even though many companies are now transitioning to passkeys and other modern authentication methods. We recommend removing subsections (E) and (P), which we believe are overly prescriptive. Additionally, we request that subsection (O) be revised to exclude third parties, as this could result in businesses being required to audit their peers—raising concerns around feasibility and confidentiality.

We also believe the definition of a “security incident” in § 7123(b)(2)(Q) is overly broad. Specifically, including violations of a business’s internal program—rather than focusing on unauthorized access—does not align with industry standards for incidents that may require reporting. This could conflate internal compliance issues with actual security events.

Finally, we recommend the following:

- A limitation on the requirement to submit full audit reports,
- The ability to redact sensitive security and proprietary information, and

- A requirement that the CPPA maintain strict confidentiality and security of submitted reports.

Additional Issues:

In addition to the concerns outlined above, we respectfully raise the following issues with the proposed regulations, which may create unintended consequences or conflict with existing statutory frameworks:

1. Over-Inclusive Deletion Threshold:

The proposed regulations would require data brokers to honor deletion requests submitted through the DROP if more than 50% of the unique identifiers provided match a single consumer record. This threshold is overly broad and could result in the deletion of personal information for individuals who did not actually submit a request. Additionally, this approach conflicts with existing CPPA regulations, which require verification of deletion requests to a “reasonable” or “reasonably high degree of certainty,” depending on the sensitivity of the data. For more sensitive information, verification typically requires at least three matching data points before a business is obligated to act.

2. Lack of Verification for Authorized Agents:

The proposed DROP regulations lack sufficient safeguards to verify that authorized agents are legitimately acting on behalf of consumers. This omission conflicts with existing CCPA regulations, which require agents to provide signed authorization from the consumer and allow businesses to verify the consumer’s identity directly or confirm the authorization. Without similar verification requirements in the DROP process, a significant loophole is created that could be exploited by unauthorized agents.

3. Insufficient Consumer Verification Requirements:

The proposed regulations do not mandate adequate verification to confirm that a deletion request is being made by the actual consumer. While there are limited guidelines for verifying residency, there is no requirement to confirm that the individual is a California resident. Moreover, although the regulations allow for verification of specific data elements, they do not require it. This is inconsistent with existing CCPA rules, which obligate businesses to establish reasonable methods for verifying the identity of the requestor and to assess whether the personal information provided is robust enough to prevent fraudulent or spoofed requests.

4. Mandated Data Standardization Raises Concerns:

The proposed rules would require all registered data brokers to reformat their databases to conform to a standardized format prescribed by the CPPA—such as removing capital letters, extraneous characters, and special symbols. This requirement could introduce data security risks by enforcing uniform formatting across systems and may also raise First Amendment concerns by compelling how business’s structure and maintain their data.

5. Improper Expansion of the “Data Broker” Definition:

The proposed expansion of the “data broker” definition through the revised interpretation of “direct relationship” exceeds the CPPA’s regulatory authority. By including entities that have a first-party relationship with consumers—such as those that sell personal information but also directly interact with consumers—the CPPA is contradicting legislative intent. The California Legislature clearly intended to limit data broker registration and compliance obligations to entities that do not have a direct relationship with consumers.

Again, we appreciate the opportunity to provide comments on the modified regulatory text but continue to urge a thoughtful reconsideration of these regulations to ensure they protect consumers without

unduly burdening businesses or stifling innovation. California's position as a global leader in AI research and development is at stake, and a balanced, well-deliberated approach is crucial for maintaining our competitive edge while safeguarding consumer interests.

If you have any questions or need additional information on our comments included in this letter, please do not hesitate to contact me directly.

Sincerely,

A handwritten signature in black ink, appearing to read "J. Brint". The signature is fluid and cursive, with a large initial "J" and a stylized "Brint".

Jacob Brint
Policy Advocate

Original Cal Retailers letter included on following pages.



February 19, 2025

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

VIA Email: regulations@coppa.ca.gov.

Cal Retailers Comments on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations

Dear Members of the Committee:

The California Retailers Association respectfully urges reconsideration of the proposed regulations regarding Automated Decision-making Technology (“ADMT”), risk assessments, and cybersecurity, as they may inadvertently hinder California's economic growth and innovation while potentially falling short of their intended consumer protection goals. We believe a more balanced approach is necessary to safeguard both consumer privacy and the state's economic vitality.

The Standardized Impact Assessment (SRIA) reveals concerning projections: over 52,000 California businesses could face compliance costs, resulting in a \$3.5 billion economic impact. This burden may disproportionately affect small businesses, forcing them to divert resources from growth and innovation to legal and compliance needs. The SRIA also forecasts significant job losses, peaking at 126,000 in 2030, and state revenue losses of up to \$2.8 billion annually by 2028.

We appreciate the importance of consumer privacy but believe the proposed regulations may exceed the scope of the California Consumer Privacy Act (CCPA). Even Alastair Mactaggart, author of the California Privacy Rights Act, has expressed concerns about the rules' scope. We suggest that AI regulations be developed through a more inclusive process led by the Legislature and the Newsom Administration, ensuring a thorough evaluation of costs, benefits, and budget impacts.

The proposed regulations, particularly those concerning Automated Decision-Making Technology (ADMT), may unintentionally impede online transactions and research. Multiple pop-up notifications could frustrate consumers and hinder their online experiences, potentially harming small and local businesses that rely heavily on e-commerce. We recommend simplifying notice requirements to focus on high-risk activities, benefiting both consumer privacy and business efficiency. Furthermore, the regulations may inadvertently discourage the use of AI technologies that could enhance efficiency, productivity, and growth across various sectors. By treating low-risk AI applications similarly to high-stakes decisions, we risk losing valuable opportunities for innovation and economic advancement.

We respectfully suggest that the California Privacy Protection Agency (CPPA) collaborate closely with Governor Newsom and the Legislature to develop a risk-based approach that addresses genuine consumer risks while fostering innovation. This approach would align with the Governor's Executive Order on AI, which aims to harness AI's benefits for Californians while avoiding a patchwork of conflicting regulations.

We would also like to share very specific examples within the proposed regulations to illustrate why we encourage the board to take time to collaborate with the Governor and the Legislature on this important issue.

EXAMPLE #1 - The draft regulations inappropriately attempt to limit first party advertising: The draft regulations are overly broad and exceed the California Privacy Protection Agency's (CPPA) authority to regulate beyond what was expressly included in the California Consumer Protection Act (CCPA) and the amendments voters approved in the California Privacy Rights Act (CPRA). CCPA clearly exempted information a business acquires through its own interaction with consumers while CPRA amended CCPA to restrict **cross-contextual behavioral advertising** by requiring a business to obtain a consumer's consent before it could share the consumer's personal information with **third parties**. Instead of providing businesses with implementation guidance, the draft regulations inappropriately attempt to broaden the scope of the CPPA's authority by granting consumers a right to opt-out of ADMT and restrict businesses' use of **first party data**. Many consumers expect businesses to provide relevant product recommendations and personalized ads that correspond to items they have previously purchased or considered purchasing to be able to take advantage of special offers and competitive pricing of goods and services. Many businesses also provide customers with opportunities to restrict how a business can use personal information it has collected about them if they choose. The draft regulations inappropriately violate the First Amendment by restricting businesses' free speech right to advertise their products and services without government interference. The draft regulations provide no compelling state interest for restricting speech, and they do not set forth a narrowly tailored solution to achieve their desired outcome.

EXAMPLE #2: The draft regulations inappropriately attempt to regulate Automated Decision-Making Technologies (ADMT): It is inappropriate for CPPA to use its authority to regulate data privacy as justification for regulating ADMTs and apply a data privacy protection framework when this type of technology was not clearly contemplated by CCPA or CPRA. Last year, the California Legislature considered, but did not pass legislation to regulate ADMTs. The Legislature and Governor continue to consider the appropriate restrictions on AI technology. The Governor signed AB 2013 imposing training data transparency requirements, but vetoed other bills attempting to regulate AI. The Governor has noted the importance of striking the appropriate balance between providing industry incentives to innovate without enacting arbitrary restrictions on technology that will stifle competition and has invited continued conversation on this topic with the Legislature. CPPA is encroaching upon the power of the Legislature to legislate with its attempt to usurp authority to regulate ADMTs.

EXAMPLE #3: The draft regulations do not appropriately distinguish between significant decisions and non-significant decisions: Effective AI laws regulate conduct, not the technology itself; otherwise, continued technological advancement renders them obsolete. For example, Colorado's AI law distinguishes between consequential and non-consequential uses of generative AI and grants consumers the right to appeal consequential decisions to ensure that human review is part of any decision pertaining to a consumer's access to education, employment, financial services, housing, health care, or legal services. Individuals are afforded analogous protection under the EU AI Act. The CPPA's draft regulations do not recognize or describe what would be considered a "significant harm" under existing California law, nor do they refer to any examples that would point to these areas of existing law. As a result, the draft regulations do not provide enough clarity on what would be considered a "significant decision" for businesses to meaningfully rely upon to ensure their compliance with California law.

EXAMPLE #4: The draft regulations interfere with regular business operations under existing law: The draft regulations' requirements for cybersecurity audits force a business' board of directors to perform managerial tasks instead of delegating those tasks to business leaders who are better qualified to execute them. For example, the draft regulations require a board member to sign a written statement they have reviewed stating they understand the findings of the cybersecurity audit. This is not an appropriate requirement given the role of a board of directors is to provide strategic planning, leadership,

and guidance, not to weigh in on day-to-day business decisions for which the board member may or may not have the appropriate level of experience or expertise to meaningfully evaluate.

EXAMPLE #5: The draft regulations impose burdensome compliance requirements without

appropriate justification: The purpose of cybersecurity audits is to ensure that businesses who process significant amounts of sensitive personal information have appropriate safeguards in place to protect consumers from the risk of harm of this information becoming public. The draft regulations provide no threshold to evaluate the significance of the risk of harm to consumers before imposing additional costly and burdensome cybersecurity requirements upon the organization. As directed in CCPA and as amended by CPRA, the draft regulations should have provided a methodology to consider the complexity of the business and the type of information it processes before imposing additional cybersecurity requirements.

EXAMPLE #6: The draft rules include several concerning provisions that may mandate businesses to compromise their proprietary info and IP (e.g., how the logic operates and the key parameters that affect the output).

The rules should clarify that no provision shall be construed to require the disclosure of trade secrets or confidential or proprietary information about the design or use of an automated system. Also, per § 1798.185(a)(3), the CPPA must issue rules to clarify that companies are not required to disclose trade secrets or proprietary information.

We also have concerns with specific sections of the proposed regulations.

§ 7001(f) – ADMT Definition - The definition of ADMT is overbroad. Including technology that “*substantially facilitates human decision making*” (i.e., “*using the output of the technology as a key factor in a human’s decision making*”, as when “*a human reviewer uses [an output] as a primary factor to make a significant decision about them*”) will require an impossible line-drawing exercise (what is a “key/primary factor”? when are other factors considered by the reviewing human “key/primary” when they produce the same result recommended by the ADMT?), and will chill use of innovative technologies in California. An ADMT should not “*substantially facilitate human decision-making*” when it (i) performs a narrow procedural task, (ii) improves the result of a previously completed human activity, (iii) detects decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment without proper human review, or (iv) performs a preparatory task to an assessment relevant to a significant decision.

§ 7150(b)(3)(A) – Significant Decision - In every other US State law that defines “*profiling*,” such profiling is tied to a legal or similarly significant decision. And in those states, a decision that produces legal or similarly significant effects is a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services or basic necessities, such as food and water. Providing consumers with the right to opt-out of profiling (and any other associated rights) is not an easy feat. As such, to the extent California will provide consumers with the right to opt-out of profiling (and other similar rights), those rights should be available only when they will significantly impact consumers.

Suggested Revision: Revise as follows – “For purposes of this Article, “*significant decision*” means a decision using information that is not subject to the exceptions set forth in Civil Code sections 1798.145, subdivisions I-(g), or 1798.146, subdivisions (a)(1), (4), and (5), ~~that results in access to, or~~ the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice (e.g., posting of bail bonds), employment ~~or independent contracting opportunities or compensation~~, healthcare services, or essential goods or services (e.g., groceries, medicine, hygiene products, or fuel).”

§ 7150(b)(3)(B)(i) – Extensive Profiling (Profiling of Employees) - It is not clear what the “*extensive profiling*” concept accomplishes that would not be addressed by the privacy risk assessment requirement for “significant decisions” concerning a consumer, which include decisions about provision or denial of educational or employment opportunities. The statute defines **profiling** as automated processing “*to evaluate certain personal aspects concerning that natural person,*” and therefore, it seems extensive “*profiling*” would be encompassed by the privacy risk assessment requirement for significant decisions. The CCPA should avoid duplicative requirements that are likely to confuse California businesses and consumers.

Suggested Revision: Strike § 7150(b)(3)(B), or at minimum, subpart (i).

§ 7150(b)(3)(B)(ii) – Extensive Profiling (Publicly Accessible Spaces) - The requirement to undertake risk assessments for extensive profiling is fundamentally in tension with the statutory text, which explicitly exempts “*publicly available information*” (i.e., information made available to the consumer to the public or from widely distributed media or if the consumer has not restricted the information to a specific audience). When a consumer is in public spaces, they have made a deliberate decision not to restrict the information to a specific audience, and moreover, have no reasonable expectation of privacy.

Accordingly, the CCPA makes clear that requirements for businesses, processors, and contractors, including the creation of risk assessments, do not apply to publicly available information, which includes information collected and processed in public spaces.

The definition of publicly available spaces is also unworkably broad and suggests that it encompasses not only parks and sidewalks, but also shopping areas, stadiums, and other places of congregation. The breadth of this definition would be extremely onerous for California businesses, especially small businesses, without a countervailing benefit to consumers.

Suggested Revision: Strike § 7150(b)(3)(B). If any part of this subpart (ii) remains, it would be helpful to clarify that “*publicly accessible place*” excludes the “*internet*” (similar to the EU AI Act), by clarifying that it refers to a **physical** place that is open to or serves the public.

§ 7150(b)(3)(B)(iii) – Extensive Profiling (Behavioral Advertising) - While other state privacy laws require a risk assessment for “*targeted ads*,” the draft rules significantly expand and alter what would be required—(i) it would extend to all behavioral ads rather than only CCBA (the focus of the statute) and (ii) impose detailed requirements that are not calibrated to the potential risk, since no consumer data is being shared with third parties or combined with other third-party data.

Suggested Revision: Strike § 7150(b)(3)(B), or at minimum, subpart (iii).

§ 7150(b)(4) – AI/ADMT Training - ADMT/model training should not be a category subject to heightened obligations (risk assessments, notice, opt out).

(1) Training a model is not “*automated decision-making*” in its core—because the “*training*” does not involve a decision that has an impact on a specific consumer—and so should be out of scope for these rules. The rules aim to cover certain high-risk AI/ADMT applications, such as when used to make a significant decision. But here, the rules would also cover developing tools that could provide lots of low-risk processing, but would still be in scope because they could one day be used for a higher risk application.

The actual use of ADMT/AI systems for these higher-risk applications would still be covered under these rules, and so extending obligations to the training of such tools is both misplaced and unnecessary. In other words, this training category expands the type of technologies that are subject to these obligations because many if not all models “*could*” be used to make a significant decision.

This "*theoretical*" approach is inconsistent with other risk-based frameworks focused on automated decision-making used to make a significant decision. This is a different issue because training a model on personal data is different from making a decision about that person (or otherwise creating any risk for them).

(2) This also exceeds the subject matter of what the CCPA contemplates, i.e., the privacy risk that may result from the processing of personal data. The statute and rules already provide ways for consumers to control how their data is used for training—they can opt out of ADMT that results in legal or similarly significant effects, access the data that a business processes about them, correct their data, and delete their data. The CPPA should not use this rulemaking to impose risk assessments that regulate AI training more broadly, when untethered to the privacy risk.

(3) The CPPA significantly departs from the approach taken in other state privacy frameworks, which neither mention nor provide heightened requirements for the use of personal information for model training. It also differs from the one other AI law (CO), where model training is not considered a high-risk decision. Also, California passed AB 2013 this year, which already imposes disclosure requirements on training data.

Suggested Revision: Strike §7150(b)(4)

§ 7154(a) – Prohibition of Certain Activities: The draft rules will prohibit processing of personal info for any covered activity if the risks outweigh the benefits. This is an extreme prohibition, and goes far beyond other AI regulations (e.g., the EU AI Act bans very limited categories of uses). It will also discourage innovation since the balance between benefits and risks is highly subjective and may be close depending on what perspective is applied (e.g., what qualifies as a risk or benefit varies wildly among experts). As an alternative, consider formulation used for unfairness under other legal regimes is the processing likely to cause substantial harm to consumers that is not reasonably avoidable (e.g., an opt out after reasonable notice and option for human review), and the injury is not outweighed by the benefit to consumers. This formulation limits the restriction to only processing that causes “substantial harm” rather than where there is only a non-material impact, and acknowledges that through the opt out, consumers can make their own choice about whether to permit the activity (rather than regulators making the choice for them).

Suggested Edit: Strike § 7154(a).

§ 7156 Interoperability of Risk Assessments: The rules governing “*risk assessments*” should align and be interoperable with the requirements for data protection assessments in other states. For instance, Colorado requires data protection assessments for (1) processing personal data for **targeted advertising** (defined as equivalent to “*cross-context behavioral advertising*,” not “*behavioral advertising*”) and **profiling** if the profiling presents a reasonably foreseeable risk of (i) unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial or physical injury to consumers; (iii) physical or other intrusion on the solitude, seclusion, or private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or (iv) other substantial injury; (2) **selling** personal data; and (3) processing **sensitive data**.

Moreover, other state privacy laws that require “*risk assessments*” (i.e. “*data protection assessments*”) for high-risk activity limit the scope of activities requiring such assessments in similar circumstances to (1) the processing of “*sensitive data*,” which could include location information **but only when such data is precise geolocation information**, and (2) profiling, **but only when it presents a reasonably foreseeable risk of the following:** unfair or deceptive treatment of (or unlawful disparate impact on) consumers, financial or physical injury, physical or other intrusion on the solitude or seclusion – or private affairs or concerns – of consumers if it would be offensive to a reasonable person (**hardly the case in a publicly available space, where consumers do not have a reasonable expectation of**

privacy), or other substantial injury.

As currently written, the draft rules contemplate interoperability only between similar “*risk assessments*” and do not contemplate “*data protection assessments*.” Further, the draft rules are rather stringent in requiring that a company may only forego a risk assessment if (1) the other “*risk assessment*” created for the purpose of complying with another law or regulation “*meets all the requirements of this Article,*” and (2) if it covers a “*comparable set of processing activities,*” defined as processing activities that “*present similar risks to consumers’ privacy.*” Of course, an entity would not know if an activity presented similar risks until it conducts the risk assessment, thereby the purpose of this provision.

§ 7157 Submission of Risk Assessments to the Agency: The draft rules require companies to submit abridged forms of their risk assessments on an annual basis to the CPPA. Routine submission is not only burdensome, but inconsistent with other state privacy laws and may result in reduced privacy protections as businesses may prepare assessments in a way that is legally protective rather than focused on the right risk-benefit balancing.

However, the CPRA statute mandates that the CPPA issue regulations that require submission at a regular cadence. For instance, the statute does not preclude the CPPA from setting separate standards for what processing activities trigger a risk assessment vs what activities are sufficiently risky to trigger a submission. This would allow the CPPA to focus on those assessments that are highest risk, such as those involving the sale of sensitive data.

Further, the rules require companies to submit risk assessments in the employment context to the regulator, but in most instances, any decisions in the employment context are confidential and not available to competitors. We’d likely need an exception to not require the submission of information that is confidential business/trade secret information.

§ 7150(a)(1) – Significant Decision: This should be limited in the same manner and for the same reasons above at § 7150(b)(3)(A). § 7200(a)(1) extends application to all uses of ADMTs for decisions regarding provision of, denial of, or access to, employment and employment compensation. Per the regulation, this includes almost all activity within the scope of the employment lifecycle: hiring, promotion/demotion; suspension/termination; and, during employment, allocation/assignment of work; setting of base and incentive compensation; and decisions regarding “other benefits.” This also includes “independent contracting opportunities,” i.e., the same activities in the IC, gig-economy, and other emerging work contexts.

§ 7200(a)(2)(A) - Extensive Profiling (Profiling of Employees): This should be limited in scope.

§ 7200(a)(2)(B) - Extensive Profiling (Publicly Accessible Spaces): This should be limited in scope.

§ 7200(a)(2)(C) - Extensive Profiling (Behavioral Advertising): This should be limited in scope.

§ 7150(a)(3) - AI/ADMT Training: This should be limited in scope.

§ 7220(a) – When Required: As a threshold matter, the CPRA does not permit regulations on pre-use notice of ADMT—instead, CPRA § 1798.185 calls for regulations “*governing access and opt-out rights,*” with respect to ADMT. The access right (addressed below) covers the information that a business needs to provide about its ADMT, and so CPPA should not issue separate and overlapping rules on notice.

At minimum, pre-use notice should be limited to where the ADMT processing is otherwise subject to access and opt-out rights. To the extent that one of these customer rights does not apply (e.g., relying on

security or fraud prevention exception), then the business should not have an obligation to post this notice. In other words, section 7220(a) should apply subject to the exceptions in § 7221(b) and § 7222(a)(1).

This makes practical sense as forcing a business to make disclosures on how it uses ADMT to perform these functions would undermine the safety and security of consumers and businesses.

Suggested Revision: Amend § 7220(a) as follows: *A business that uses automated decision-making technology as set forth in section § 7200, subsection (a), and subject to the exceptions in section § 7221(b) and section § 7222(a)(1), must provide consumers with a Pre-Use Notice.*

§ 7220(c)(5) – Explainability: The draft requires businesses to explain, in plain language, the logic used in the automated decision-making technology, including the key parameters that affect the output of the automated decision-making technology. We recommend deletion of this provision as it is effectively an explainability requirement. Research in the field of explainable ADMT is progressing rapidly, but many complex AI models (which tend to be the most useful ones) are not yet fully explainable. Indeed, requiring an explanation now could result in consumer confusion. CCPA should therefore consider whether it would benefit California to impose this requirement, or whether there are other better methods to mitigate risk such as human review and rigorous testing.

The draft rules are also in tension with the statute's explicit recognition that the CCPA's requirements do not require the business to disclose trade secrets (Cal. Civ. Code 1798.100(f)). The exception under § 7220(c)(5)(C) is too narrow. This is particularly important in the HR context, because HR deals with not only employee confidential data, but also beta and pilots for products that should be excluded as confidential business/trade secret information.

Suggested Revision: Strike § 7220(c)(5).

Behavioral Advertising – Fallback: For reasons stated above, the scope of covered ADMT under § 7200 should not include profiling of a consumer, or at minimum, should exclude behavioral advertising. If that is not excluded, then any notice requirements should be tailored to the reduced risk and different circumstances of advertising. For instance, as drafted, the rules would impose more detailed disclosures than required for higher-risk cross-context behavioral ads under § 7013.

AI/ADMT Training – Fallback: For reasons stated above, the scope of covered ADMT under § 7200 should not include the use of ADMT for training. If that is not excluded, then at minimum such processing should not trigger pre-use notice. It will contribute to notice fatigue without reducing risk as consumers will struggle to understand this notice. Instead, the draft rules already require AI/ADMT deployers (i.e., “users”) to conduct risk assessments and companies may invest in accuracy/testing safeguards that better demonstrate trustworthiness.

§ 7221(b) – Exceptions General: Expand the set of exceptions under § 7221(b) to include conducting internal research, fixing technical errors, effectuating product recalls, and performing internal operations consistent with the consumer’s expectations (like other privacy laws).

§ 7221(b)(1) - Security and Fraud Prevention: The fraud and security exception should be unencumbered by whether ADMT is “necessary” for the purposes of security, fraud prevention, or safety. Businesses should be free to choose the most effective and reasonable method of security, fraud prevention, or safety without regard for whether a particular method is “necessary.”

Suggested Revision: Amend § 7221(b)(1) as follows: (b)(1) The business’s uses of that automated decision-making technology ~~is necessary solely~~ to achieve, ~~and is used solely for~~, the security, fraud prevention, or safety purposes listed below...

§ 7221(i) – Single ADMT Opt Out: The draft rules would require a business to offer a single option to opt-out of all covered ADMT, although businesses may present consumers with a choice to allow specific uses. Consumers will struggle to comprehend the impact of a general opt out in the abstract or to analyze a vast range of potential use cases (e.g., behavioral advertising vs screening for health risks). This will likely result in consumers making opt-out elections to avoid certain high-risk use cases, and then losing out on significant beneficial opportunities that would likely approve when presented with the specific use case. Instead, business should be required to surface an opt out that is targeted to the specific use case so the consumer can decide in real time and in context rather than in the abstract. Also, mandating a single opt out presumes that the use of ADMT is generally harmful to consumers or lacks benefits, and is antithetical to California’s support for innovation, efficiency, and tools that reduce human error and bias.

Suggested Revision: Amend § 7221(i) as follows: In responding to a request to opt-out of ADMT, a business may present the consumer with the choice to allow specific uses of automated decision-making technology ~~as long as the business also offers a single option to opt-out of all of the business’s use of automated decision-making technology set forth in subsection (a).~~

§ 7221(b)(4) & (5) – Employee Exceptions: The draft rules provide some exceptions to the ADMT Opt-Out for “*allocation/assignment of work and compensation decisions*” and “*work or educational profiling*.” However, these exceptions require companies to conduct “*an evaluation*” and implement expensive and burdensome “*accuracy and nondiscrimination safeguards*.” Employers generally are allowed flexibility to ensure employees are working and productive. This would stifle employers’ ability to ensure employees are properly working or the company is properly staffed. It can also affect customer service where companies look at these tools to identify when to route calls to employees to ensure 1) they are working and 2) ensure they are not overwhelmed with the volume of calls. Moreover, it is not clear what “*work or educational profiling*” means. The proposed rules refer to “*extensive profiling*,” not “*work or educational profiling*.”

Behavioral Advertising – Fallback: The scope of covered ADMT, under § 7200, should not include profiling of a consumer, or at minimum, should exclude behavioral advertising. If not, then the draft should at minimum not apply an opt-out right to all behavioral ads as it conflicts with the statutory opt-out framework that is limited to CCBA. As a final fallback, the rules should be clear that any opt out that applies to behavioral ads is limited to targeting ads based on inference preferences from consumers based on their personal data. The draft rules potentially sweep in contextual ads since the definition of behavioral ads is not limited to activity “*over time*.”

Additionally, the proviso in the “*behavioral advertising*” definition makes it seem like measurement (e.g., attribution) could be covered as well. It unhelpfully copies some CPRA language, but without the additional context from the CPRA that clarifies that measurement is not in scope.

AI/ADMT Training – Fallback: § 7221(b) provides a limited set of exceptions to the opt-out right, but does not extend them to AI/ADMT training. For reasons stated above, the scope of covered ADMT under § 7200 should exclude ADMT training uses. If that is not excluded, then the exceptions should apply to this use, in particular, the fraud and security exception under (b)(1) and the evaluation exception under (b)(3), (4), and (5). Businesses should be encouraged to evaluate whether the ADMT is discriminatory or working as intended and the best way to do that is to train on representative samples of data.

If AI/ADMT training is not excluded entirely from Article 11, then another fallback should exclude or limit the right to opt out. Generally, model training (especially for the largest models trained on internet-scale data) personal data included in the training corpus is incidental. Requiring implementation of an opt out process runs counter to data minimization best practices, as it may require individual identification.

Suggested Revisions: The preferred option would be to strike § 7150(b)(4) – AI/ADMT Training altogether. If not, amend § 7221(b) by striking (b)(6).

§ 7222 Requests to Access ADMT: General concerns - CPRA § 1798.185 instructs the CPPA to issue regulations on access rights with respect to a business’s use of ADMT, and requiring responses to include “*meaningful information about the logic involved in those decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer.*” It does not call for separate notice. Based on these statutory requirements, the CPPA should consider a single set of rules about how businesses need to provide meaningful information about their use of ADMT.

Businesses should have the option to provide this information in a notice (rather than a response to a specific request). The rules should not require businesses to provide consumer-specific responses, as this (i) is not required under the statute, (ii) is not practical or feasible in many cases, and (iii) would be difficult to comply without disclosing confidential information or allowing consumers to game the process, which would have dangerous implications where the ADMT is used to make a significant decision. Consumers already have separate access rights under the CPRA, and so can obtain any personal information processed by the company, including ADMT inputs and outputs containing their personal information.

§ 7222 (a) – When Access Right Applies: The draft rules create a right to access ADMT when a business uses ADMT for significant decisions (§ 7200(a)(1)) or extensive profiling (§ 7200(a)(2)). It does not apply to AI/ADMT training. This right should be limited to where ADMT is used to make a significant decision. The access right serves to allow consumers to understand whether they want to exercise their opt-out right, and to allow them to correct any inaccurate input concerning their personal information. This may assist consumers when presented with an ADMT offering that will assist in making a significant decision, but does not apply to “extensive profiling” such as profiling for behavioral advertising. For those uses, the consumer can decide whether to opt out regardless of how technology works. Businesses should not be required to publicly disclose confidential information about their technological processes absent any direct consumer benefit.

Suggested Revisions: Amend § 7222(a) as follows: *Consumers have a right to access ADMT when a business uses automated decision-making technology as set forth in § 7200, subsections (a)(1)-(2)* Strike § 7222(b)(3)(B).

§ 7222(b) – Response to Access Request: Per above, the responses should not be tailored to specific consumers. At minimum:

(b)(2) should be modified so that the business must provide only the range of potential outputs and not the specific output as it relates to the consumer. If the output itself contains personal information related to the consumer, then it would be subject to the separate, broader access right under the CPRA.

(b)(4) should be clarified to not require the business to explain how the ADMT operated with respect to a specific consumer.

§ 7222(k) – Adverse Significant Decisions: In the employment context, the rules give companies too little time to effectively provide detailed, and in parts, data specific to each individual decision—a bar too burdensome given the broad applicability. In the case of an “*adverse significant decision*” (suspension, demotion, termination, or reduction in compensation), the business must provide notice of the right to access within 15 days of the adverse decision, and with detailed information within 45 days. Upon request, the business must provide “*a plain language explanations*” — requiring interpretation — of the purpose of the ADMT, and more concerning, (a) the specific outputs the ADMT produced after processing the individual’s data; (b) the way in which the business used (and plans to use) the ADMT output and human assessment in making decisions regarding that individual; (c) the “*extensive profiling*”,

if any, performed by the business using an ADMT; and (d) the precise “*logic*”, “*key parameters*”, and “*range of possible outputs or aggregate output statistics*” of the ADMT, so the individual can understand the workings of the tool and how the specific decision came to be. Little of this information will be helpful to the individual and will require extensive interpretation on behalf of a company to produce this information in “*plain language*” to an individual—often in each specific “*adverse significant decision*.”

Behavioral Advertising – Fallback: The scope of covered ADMT under § 7200 should not include profiling of a consumer, or at minimum, should exclude behavioral advertising. If not, then the draft should at minimum not apply the access right to this type of ADMT processing.

Suggested Revisions: See previous comments to strike “*behavioral advertising*.”

We also have concerns with the way § 7123(f) is currently drafted. As written, it is effectively useless as it says another audit can only be used if another audit has all the same requirements as the CCPA audit. No other audit regime looks like the CCPA audit, so businesses will always be required to conduct a separate audit for CCPA. Most businesses already conduct annual audits for ISO certification. We suggest the regulations include common security audit frameworks that will be accepted as compliant with these regulations without requiring businesses to make the determination whether they meet all the requirements the agency requires.

Related to this, the specific controls in § 7123(b) run the risk of quickly becoming outdated. Most existing cybersecurity audit standards call for the assessment of how organizations achieve outcomes (e.g., NIST recommends as a security control, “*The confidentiality, integrity, and availability of data-at-rest are protected.*”). The proposed regulations instead require specific security controls to achieve certain outcomes (e.g., requiring assessment of “*Encryption of personal information, at rest*”). For example, (b)(2)(A) focuses on MFA and passwords when most companies are increasingly moving to passkeys.

Finally, we suggest a limitation on the submission of full audits, allowance for redaction of sensitive security information and other information, and a requirement that the CPPA keep the reports secure and confidential.


General Comments and Concerns on AI/Privacy Regulations Impact on Emergencies

Weave in how these regulations will negatively impact the supply chain or small business recovery for those who are trying to rebuild after emergencies like the recent wildfires in Los Angeles County.

Again, we appreciate the opportunity to provide comments on the proposed regulations, but urge a thoughtful reconsideration of these regulations to ensure they protect consumers without unduly burdening businesses or stifling innovation. California's position as a global leader in AI research and development is at stake, and a balanced, well-deliberated approach is crucial for maintaining our competitive edge while safeguarding consumer interests.

If you have any questions or need additional information on our comments included in this letter, please do not hesitate to contact me directly.

Sincerely,



Sarah Pollo Moo
Policy Advocate

Grenda, Rianna@CPPA

From: Jesse Lieberfeld <jlieberfeld@ccianet.org>
Sent: Friday, May 30, 2025 4:12 AM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: CPPA ADMT Comments for submission.pdf

This Message Is From an Untrusted Sender

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

[Report Suspicious](#)

To the California Privacy Protection Agency Legal Division:

The Computer & Communications Industry Association (CCIA) is pleased to respond to the California Privacy Protection Agency's Notice of Proposed Rulemaking on the proposed CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations. CCIA's comments are attached. We appreciate CPPA's consideration, and look forward to continuing to participate in the CPPA's ongoing regulatory process.

Best,

Jesse Lieberfeld

Policy Counsel

jlieberfeld@ccianet.org

O: 202-517-1536 M: [REDACTED]



Computer & Communications
Industry Association
Open Markets. Open Systems. Open Networks.

ccianet.org | [@CCIANet](https://twitter.com/CCIANet)



May 30, 2025

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

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

The Computer & Communications Industry Association (CCIA)¹ is pleased to respond to the California Privacy Protection Agency’s Notice of Proposed Rulemaking on the proposed CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations (“the proposed Rules”).² As CPPA weighs potential modifications to the proposed Rules, CCIA offers the following proposals to guide deliberation, which are grouped by section of the proposed Rules below. CCIA’s suggested amendments to the draft Rules are set forth in **Attachment A**.

DEFINITIONS

Section 7001(e) – “Automated Decisionmaking Technology”

While CCIA appreciates the removal of subjective language from this definition, the standards for “human involvement” still create uncertainty. To have “human involvement,” a human reviewer must “Review and analyze the output of the technology, and any other information that is relevant to make or change the decision.” Assessing what information is “relevant” to a decision is often quite difficult to do objectively. Such assessments could be more objective if the “relevant” standard were changed to “necessary.” It should suffice for businesses to have protocols in place listing the factors that their human reviewers consider when reviewing technological outputs.

Subsection 3 of this definition lists various exceptions, such as firewalls, anti-malware, and robocall filtering, “provided that they do not replace human decisionmaking.” This qualification should be removed, as it defeats the purpose of these exceptions. The exceptions listed are integral features of businesses that do not cause automated decisions to be made about consumers. Businesses can therefore safely automate these technologies without undermining consumers or jeopardizing their data.

Section 7001(ddd) – “Significant decision”

Subsection 4 of this definition rightly extends to the hiring and firing of employees. However, businesses regularly establish preset formulas for work distribution, compensation, and

¹ CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than \$100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. For more, visit www.ccianet.org.

² *Proposed Text (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations)*, Cal. Privacy Protection Agency (May 1, 2025), https://cppa.ca.gov/meetings/materials/20250501_item4_draft_text.pdf.

bonuses, and should be able to continue to do so. CCIA therefore recommends limiting subsection 4 to the hiring and firing of employees.

ARTICLE 10 – RISK ASSESSMENTS

Section 7150(b)(5) – Profiling – Sensitive Location

CCIA recommends removing this provision. A “sensitive location,” like all other locations, can nonetheless be publicly available. The California Privacy Rights Act (CPRA) already regulates precise geolocation data from geo-trackers, regardless of the location’s sensitivity. If the location is sensitive, these regulations already require controllers to perform risk assessments and provide opt-outs. This provision therefore does not grant consumers additional data protection and may deny some local businesses the opportunities to offer their customers certain benefits, such as discounts at specific stores a customer has previously visited.

Section 7150(b)(6) – AI / ADMT Training

The scope of this section should be narrowed. This section provides that “Processing the personal information of consumers, which the business intends to use to train an automated decisionmaking technology” constitutes “significant risk to consumer privacy.” However, the definition of “intends to use” includes personal information that a business “permits others to use, plans to permit others to use, is advertising or marketing the use of, or plans to advertise or market the use of.” This definition extends to information that businesses never intend to use for training automated decisionmaking technology (ADMT) or any other high-risk purpose, and therefore should be restricted to cases where the business actually intends to use the information. Note that the proposed rules already regulate cases where developers use ADMT models to make significant decisions regarding consumers or modify such models with supplemental training using ADMT.

CCIA also suggests eliminating the automatic categorization of training models used for ID verification data and biological identification as sensitive information. Models may be trained for such purposes without identifying any specific person if, for instance, they are trained on anonymized data. If the models do identify specific persons, CPRA’s existing regulations for sensitive data will apply and risk assessments will still be required, as CPRA designates biometric data as a form of sensitive data. These categorizations therefore do not enhance user privacy and in fact undermine businesses’ ability to use privacy-preserving techniques in their training models.

Section 7152(a)(3) – Risk Assessment Requirements

CCIA recommends allowing a risk assessment that satisfies another jurisdiction’s requirements to be substituted for the list of requirements in this section. The purpose of risk assessment requirements is to ensure that no high-risk harm outweighs the benefits of processing data. Most privacy laws allow companies to tailor their risk assessments to the specific product or service provided, rather than follow a checklist like the one in this section.³ Consumers would

³ See, e.g., Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1-580.C (2025) (requiring that data protection assessments “identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential

benefit from more holistic evaluations of the risks and benefits of their data use, while companies doing business in California would avoid the burden of duplicative requirements that they would not face elsewhere.

In particular, the requirements in subsection (F) are unnecessarily burdensome. Section 7152(a)(1) already requires risk assessments to identify the purpose for which data is processed. As long as the risk assessment specifies which categories of data are processed, listing each third party recipient of the data will likely be unnecessary to determine the risk this processing possesses (unless sharing with a particular third party poses a special risk). Again, a more holistic approach would benefit consumers and businesses by allowing businesses to focus their assessments on the most pertinent privacy risks to their consumers.

Furthermore, the logic underlying ADMT is not necessarily related to any consumer privacy risk unless it is used to make a significant decision regarding a consumer. CCIA therefore recommends amending subsection (G)(i) to only require risk assessments to evaluate the logic underlying ADMT if the logic is used for a significant decision regarding a consumer.

Section 7156(b) – Conducting Risk Assessments for a Comparable Set of Processing Activities or in Compliance with Other Laws or Regulations

As noted above, CCIA recommends allowing a risk assessment that satisfies another jurisdiction’s requirements to be substituted for the list of requirements in this section, even if they do not meet every requirement listed in section 7152(a)(3). Additionally, other state privacy laws require risk assessments only when “sensitive data” is processed (e.g. precise geolocation data rather than all geolocation, or profiling resulting in specific consumer harms, rather than profiling in general).⁴

Section 7157(b) – Risk Assessment Materials to be Submitted

While CCIA appreciates the revisions to this section, it remains unclear how CPPA intends to use the information collected, and the proposed Rules should specify how the agency may use the data. Moreover, to minimize the burden on both CPPA and businesses, risk assessments should be required only when sensitive data is processed. This will enable both CPPA and the businesses it regulates to prioritize the most substantial threats to consumer privacy.

ARTICLE 11 – AUTOMATED DECISIONMAKING TECHNOLOGY

Section 7200(a)(1) – Significant Decision

CCIA recommends the same revisions to this provision as to section 7001(ddd), for the reasons described in the section 7001(ddd) comments.

risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks”).

⁴ See, e.g., Texas Data Privacy and Security Act, Tex. Bus. & Com. Code § 541.105(a) (2024).

Section 7200(b) – Effective Date

CCIA recommends removing the first sentence of this subsection. Businesses should not be required to submit risk assessments for ADMT that is used prior to the effective date but is not used on or after the effective date.

Section 7220(a) – Pre-Use Notice Requirements

CCPA does not allow regulations of pre-use notice of ADMT—instead, CCPA § 1798.185 calls for regulations “governing access and opt-out rights” regarding ADMT.⁵ The access right covers the required information from businesses about ADMT use. CCPA should therefore not issue rules on pre-use notice, or at minimum, limit pre-use notice requirements to cases where ADMT use is already subject to access and opt-out rights. Should one of these customer rights not apply (e.g., relying on a security or fraud prevention exception), then businesses should not need to post this notice. In essence, section 7220(a) should apply subject to the exceptions in sections 7221(b) and 7222(a)(1). Forcing businesses to disclose how they use ADMT to perform the specified functions risks undermining the security of consumers and businesses, and requirements to make such disclosures should be minimized.

Section 7220(c)(5) – Explainability

CCIA welcomes the carveouts to this subsection in section 7200(d). However, Sections 7220(c)(5)(A)-(B) still contain impracticable requirements. Many complex AI models (which tend to be the most useful ones) are not yet fully explainable. CCPA should consider whether California would benefit from this requirement, or whether human review and rigorous testing will better mitigate risk.

Sections 7221(b)(2)-(3) – Requests to Opt-Out of ADMT: Employee Exceptions

In sections 7221(b)(2)(A) and (b)(3)(A), the word “solely” should be removed. The opt-out provided in this section should be required only if the business uses the data described in these subsections for another significant decision regarding consumers, not if it merely uses the data for another low-risk activity. For instance, as written, a business using ADMT that both tracked workflow and performed routine website maintenance would have to provide the stated opt-out, even though the latter function does not involve any significant decision regarding a consumer.

In sections 7221(b)(2)(B) and (b)(3)(B), “Ensures” should be changed to “Takes reasonable measures to ensure.” As written, a compliant ADMT system could be rendered noncompliant because of a temporary malfunction. This revision would set a more realistic standard for businesses.

Section 7221(i) – Requests to Opt-Out of ADMT: Single Opt-Out

The draft rules would force businesses to offer a single opt-out for all covered ADMT, although businesses may let consumers allow specific uses. Businesses should instead be required to

⁵ California Consumer Privacy Act, Cal. Civ. Code § 1798.185(a)(15) (2018).

offer opt-outs targeting the specific use cases applicable to a consumer's data. A general opt-out does not give consumers information about how a given consumer activity leads to a given ADMT use. Requiring context-specific opt-outs will give consumers more autonomy and insight regarding the use of their data.

Section 7222(a) – Requests to Access ADMT

CCPA § 1798.185 instructs the CPPA to regulate access rights with respect to businesses' ADMT use, and requires responses to include “meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer.”⁶ It does not mandate separate notice to consumers. CCPA should implement a single set of rules about how businesses must provide meaningful information about their ADMT use. Businesses should be able to provide such information in a notice rather than responses to specific requests. Consumer-specific responses are not required under the statute, and are often impractical or infeasible. They can also be hard to answer without disclosing confidential information, which may harm consumers subject to “significant decisions” using ADMT. Consumers already have separate access rights under CCPA, allowing them to obtain any personal information companies process, including ADMT inputs and outputs containing their personal information.

Furthermore, the exceptions for employment uses in section 7221(b) should also apply to this section. Extending the terms “Automated decisionmaking technology” and “significant decision” to cover interim hiring decisions and filtering tools would make it impractical for businesses to respond to consumer-specific access requests on how the ADMT processed their data, regardless of whether it made an adverse decision regarding them. The entire point of using ADMT is to avoid having to respond to large numbers of such requests individually.

Sections 7222(b)(1) – Requests to Access ADMT: Specific Purpose

For the reasons described in the preceding paragraph, CCIA advocates limiting this right to cases in which the ADMT has made an adverse decision regarding the consumer.

Section 7222(b)(2) – ADMT Logic

This subsection should be removed. Other regulatory frameworks that require businesses to explain decisions adverse to consumers do not require disclosing methodology. For instance, the Fair Credit Reporting Act (FCRA) only requires that businesses taking adverse actions based on consumer reports explain that an adverse action occurred, state the consumer rights, and provide a means of contacting the reporting agency — it lacks any requirement to disclose decisionmaking methodologies.⁷ Requiring such disclosures provides no meaningful benefit to consumer privacy, but does allow a backdoor means for competitors to access and copy a business's proprietary methodologies.

Section 7222(b)(3) – ADMT Logic

⁶ *Id.* § 1798.185.

⁷ See Fair Credit Reporting Act, 15 U.S.C. § 1681g(f) (2010).



This subsection should also be removed. Section 7222(b)(1) already covers cases where ADMT was the sole factor in the decision. If the decision was reached through a combination of automated outputs and human decisionmaking, it does not fall within the proposed Rules' definition of ADMT, which only applies where the technology substantially or fully replaces human decisionmaking.

*

*

*

*

*

We appreciate CPPA's consideration of these comments. CCIA looks forward to continuing to participate in the CPPA's ongoing regulatory process, including reviewing and providing feedback on the series of proposed Rules. We hope CPPA will consider CCIA a resource as these discussions progress.

Sincerely,

Jesse Lieberfeld
Policy Counsel– Privacy, Security, and Emerging Technologies
Computer & Communications Industry Association

ATTACHMENT A

Suggested Amendments to Revised Draft Rules

This Attachment contains CCIA's suggestions for specific modifications to the Revised Draft Rules. The text below is the draft Rules text after the Department of Law's revisions. CCIA's proposed deletions are in **red** and proposed new language is in **green**.

§ 7001(e) – “Automated Decisionmaking Technology”: “Automated decisionmaking technology” means any technology that processes personal information and uses computation to replace human decisionmaking, or substantially replace human decisionmaking.

1. For purposes of this definition, to “substantially replace human decisionmaking” means a business uses the technology’s output to make a decision without human involvement. Human involvement requires the human reviewer to:
 - a. Know how to interpret and use the technology’s output to make the decision;
 - b. Review and analyze the output of the technology, and any other information that is **necessary** ~~relevant~~ to make or change the decision; and
 - c. Have the authority to make or change the decision based on their analysis in subsection (b).
2. Automated decisionmaking technology includes profiling.
3. Automated decisionmaking technology does not include **search-term software**, web hosting, domain registration, networking, caching, website-loading, data storage, firewalls, anti-virus, anti-malware, spam- and robocall-filtering, spellchecking, calculators, databases, and spreadsheets, ~~provided that they do not replace human decisionmaking.~~

§ 7001(ddd)(4) – “Significant Decision”: “Employment or independent contracting opportunities or compensation” means **hiring and/or termination.:**

- ~~a. Hiring;~~
- ~~b. Allocation or assignment of work for employees; or salary, hourly or assignment compensation, incentive compensation such as a bonus, or another benefit (“allocation/assignment of work and compensation”);~~
- ~~c. Promotion; and~~
- ~~d. Demotion, suspension, and termination.~~

~~§ 7150(b)(5) – Profiling – Sensitive Location:~~

§ 7150(b)(6) – AI/ADMT Training: Processing the personal information of consumers, which the business intends to use to train an automated decisionmaking technology for a significant decision concerning a consumer; ~~or train a facial recognition, emotion recognition, or other technology that verifies a consumer’s identity, or conducts physical or biological identification or profiling of a consumer.~~ For purposes of this paragraph, “intends to use” means the business is using; **or** plans to use; ~~permits others to use, plans to permit others to use, is advertising or marketing the use of, or plans to advertise or market the use of.~~

§ 7152(a)(3) – Risk Assessment Requirements: Identify and document in a risk assessment report the following operational elements of the processing:

...

~~(F) The names or categories of the service providers, contractors, or third parties to whom the business discloses or makes available the consumers' personal information for the processing; and the purpose for which the business discloses or makes the consumers' personal information available to them~~

(G) For the uses of automated decisionmaking technology set forth in section 7150, subsections (b)(3), the business must identify: (i) The logic of the automated decisionmaking technology, including any assumptions or limitations of the logic, **provided such logic is used to make a significant decision regarding a consumer**; and (ii) The output of the automated decisionmaking technology, and how the business will use the output to make a significant decision.

§ 7156(b) – Conducting Risk Assessments for a Comparable Set of Processing Activities or in Compliance with Other Laws or Regulations: 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 **complies with another state privacy law reasonably similar in scope and effect** ~~contains the information that must be included in, or is paired with the outstanding information necessary for, compliance with section 7152.~~

§ 7157(b) – Risk Assessment Materials to be submitted: A business **that processes sensitive data** must submit to the Agency the following risk assessment information....

§ 7200(a)(1) – Significant Decision: See entry for § 7001(ddd)(4).

§ 7200(b) – Effective Date: ~~A business that uses automated decisionmaking technology for a significant decision prior to January 1, 2027, must be in compliance with the requirements of this Article no later than January 1, 2027.~~ A business that uses automated decisionmaking technology on or after January 1, 2027, must be in compliance with the requirements of this Article any time it is using automated decisionmaking technology for a significant decision.

§ 7220(a) – Pre-Use Notice Requirements: A business that uses automated decisionmaking technology as set forth in section 7200, subsection (a), **and subject to the exceptions in section 7221(b) and section 7222(a)(1),** must provide consumers with a Pre-use Notice....

§ 7220(c)(5) – Explainability: ...The additional information must include a plain language explanation of the following:

- ~~A. How the automated decisionmaking technology processes personal information to make a significant decision about consumers, including the categories of personal information that affect the output generated by the automated decisionmaking technology. An “output” may include predictions, decisions, and recommendations (e.g., numerical scores of compatibility).~~
- ~~B. The type of output generated by the automated decisionmaking technology, and how that output is used to make a significant decision. For example, this may include whether the output is the sole factor in the decisionmaking process or what the other factors are in that decisionmaking process; and to the extent that a human is part of the decisionmaking~~

~~process in a manner that does not meet the requirements of “human involvement” in section 7001, subsection (e)(1), what that human’s role is in the decisionmaking process.~~

- C. What the alternative process for making a significant decision is for consumers who opt out, unless an exception to providing the opt-out of automated decisionmaking technology set forth in section 7221, subsection (b), applies.

Sections 7221(b)(2)-(3) – Requests to Opt-Out of ADMT: Employee Exceptions: A business is not required to provide consumers with the ability to opt-out of a business’s use of ADMT to make a significant decision in the following circumstances:

- (2) For admission, acceptance, or hiring decisions as set forth in section 7001, subsections (ddd)(3)(A) and (ddd)(4)(A), the business:
- (A) Uses the ADMT ~~solely~~ for the business’s assessment of the consumer’s ability to perform at work or in an educational program to determine whether to admit, accept, or hire them; and
 - (B) Takes reasonable measures to ensure ~~Ensures~~ that the automated decisionmaking technology works as intended for the business’s proposed use and does not unlawfully discriminate based upon protected characteristics
- (3) For allocation/assignment of work and compensation decisions as set forth in section 7001, subsection (ddd)(4)(B), the business:
- (A) Uses the automated decisionmaking technology ~~solely~~ for the business’s allocation/assignment of work or compensation; and
 - (B) Takes reasonable measures to ensure ~~Ensures~~ that the automated decisionmaking technology works as intended for the business’s proposed use and does not unlawfully discriminate based upon protected characteristics.

§ 7221(i) – Requests to Opt-Out of ADMT: Single Opt-Out: In responding to a request to opt-out of ADMT, a business may present the consumer with the choice to allow specific uses of automated decisionmaking technology ~~as long as the business also offers a single option to opt out of all of the business’s use of automated decisionmaking technology set forth in subsection (a).~~

§ 7222(a) – Requests to Access ADMT: When Access Rights Apply: A business that uses ADMT to make an ~~adverse~~ significant decision must provide a consumer with information about this use when responding to a consumer’s request to access ADMT, ~~unless the business:~~

- (A) Uses the ADMT for the business’s assessment of the consumer’s ability to perform at work or in an educational program to determine whether to admit, accept, or hire them; and
- (B) Takes reasonable measures to ensure that the automated decisionmaking technology works as intended for the business’s proposed use and does not unlawfully discriminate based upon protected characteristics.

§ 7222(b)(1) – Requests to Access ADMT: Specific Purpose: The specific purpose for which the business used ADMT with respect to the consumer, ~~if the use of ADMT resulted in a significant adverse decision concerning the consumer.~~ The business must not describe the purpose in generic terms, such as “to improve our services.”

~~**§ 7222(b)(2)-(3) – Requests to Access ADMT: ADMT Logic:**~~

Grenda, Rianna@CPPA

From: Ridhi Shetty <rshetty@cdt.org>
Sent: Monday, June 2, 2025 11:42 AM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: CDT Public Comment on Modifications to Proposed CCPA Regulations on ADMTs.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 Candice Sanders,

The Center for Democracy & Technology respectfully submits the attached comments in response to the California Privacy Protection Agency's notice of modifications to text of proposed regulations under the California Consumer Privacy Act.

Best,
Ridhi Shetty

Ridhi Shetty | Senior Policy Counsel, Privacy & Data Project
Center for Democracy & Technology | cdt.org
E: rshetty@cdt.org | P: 202-407-8830 | [she/her/hers]

CDT is celebrating its 30th Anniversary! Please join the fun by [staying updated on our work](#), [connecting with us](#), or [making a contribution](#).



June 2, 2025

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

Re: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations –
Modifications to Text of Proposed Regulations

I. Introduction

The Center for Democracy & Technology (CDT) respectfully submits these comments to the California Privacy Protection Agency (Agency) in response to the Agency's Notice of Modifications to Text of Proposed Regulations under the California Consumer Privacy Act (CCPA). CDT is a nonpartisan, nonprofit 501(c)(3) organization that works to advance civil rights and civil liberties in the digital age. CDT's work includes advocating for strong, effective requirements for the responsible, rights-respecting use of automated systems.

In [our comments](#) to the Agency regarding this proceeding on February 19, 2025, we commended the Agency's continued work to strengthen regulatory oversight of automated decision-making technologies (ADMT), and we recommended ways to further strengthen the proposed measures.¹ We are therefore concerned about the direction this proceeding has taken. As Agency staff communicated during the Agency Board's meeting on May 1, 2025, **only ten percent of California businesses subject to the CCPA would have been subject to the version of the proposed rules as updated on May 1.** The revisions made to the proposed rules since then would further reduce the number of California businesses that would be subject to the ADMT requirements. Considering the increasing role that ADMTs play in causing privacy harms that the CCPA was intended to prevent, this move to minimize industry's transparency obligations would undercut the purpose of the ADMT regulations and the CCPA itself. We urge

¹ Center for Democracy & Technology, Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations (Feb. 19, 2025), <https://cdt.org/wp-content/uploads/2025/02/CDT-Public-Comment-on-CCPA-Updates-Cyber-Risk-ADMT-and-Insurance-Regulations.pdf>.

the Agency to undo the recent revisions and refocus on strengthening the proposed transparency measures for ADMTs to better protect consumers and increase trust in AI.

II. The Definition of ADMT Should Be Expanded.

The previous definition of ADMT included technologies that process personal information to execute a decision or to replace or substantially facilitate human decision-making. The phrase “substantially facilitate human decision-making” was described as the use of the ADMT’s output as a key or primary factor in a human’s decision-making. In our February 2025 comments, we explained that businesses have the incentive to interpret the definition narrowly so as to conclude that the outputs of their systems are not “key” or “primary” factors and therefore that their systems are not ADMTs within the scope of the rules.² We therefore recommended defining ADMTs using the California State Administrative Manual’s definition of “automated decision system”: “a computational process derived from machine learning, statistical modeling, data analytics, or artificial intelligence that issues simplified output, including a score, classification, or recommendation, that is used to assist or replace human discretionary decision-making and materially impacts natural persons.”³

The latest version of the proposed rules goes in the opposite direction. It defines ADMT to include only technologies that process personal information to *replace or substantially replace* human decision-making. The proposed definition of “substantially replace human decision-making” is limited to using the technology’s output “to make a decision without human involvement.” This new definition will make it even easier for businesses to avoid complying with the rules simply because they have personnel who can theoretically change the decision made using that output, even if in practice personnel do not exercise that capability and instead defer to the output.⁴ The ultimate result is that consumers interacting with only a very small fraction of ADMT systems would have any protections against harms from those systems.

² *Id.*

³ California Department of General Services, State Administrative Manual: Definitions - 4819.2, <https://www.dgs.ca.gov/Resources/SAM/TOC/4800/4819-2>.

⁴ See e.g., Hilke Schellmann, *The Algorithm: How AI Decides Who Gets Hired, Monitored, Promoted & Fired, And Why We Need to Fight Back Now* (Hachette Book Group 2024) (discussing employers’ decision to rely on “cut scores” set by vendors of ADMTs used for employment decisions); Patrick Rucker, Maya Miller, and David Armstrong, *How Cigna Saves Millions by Having Its Doctors Reject Claims Without Reading Them*, ProPublica (Mar. 25, 2023), <https://www.propublica.org/article/cigna-pdx-medical-health-insurance-rejection-claims> (describing deference by insurance company doctors to ADMT outputs to deny claims instead of using their expertise).

III. The Types of Profiling Subject to the Rules Should Be Broadened.

The latest version of the proposed rules specifies that “physical or biological identification or profiling” is limited to using “automated measurements or analysis” of a person’s physical or biological characteristics or body to identify or profile them, and does not include the processing of physical or biological characteristics that do not identify and cannot be linked to a particular person.

The latest proposed rules make three problematic changes to the risk assessment requirements with respect to profiling. One, the general risk assessment requirements now apply to profiling based on observation of people in sensitive locations but not in retail or other publicly accessible spaces. Two, they now apply when a business intentionally processes personal data to train a technology that conducts physical or biological identification or profiling, but not when a business uses but does not train such technology. Three, additional risk assessment requirements specific to the use of physical or biological identification or profiling for significant decisions were removed.

Some vendors offer technology trained to use physical or biological characteristics to help businesses flag certain customers’ gait or similar characteristics as suspicious and link the observed characteristics to specific customers without necessarily establishing customers’ identities.⁵ A retail store that uses this technology would not be subject to the risk assessment requirements, even if the use of the technology disproportionately flags people of color and people with disabilities that affect how they move.⁶ Due to the narrowed coverage of profiling, businesses that deploy technologies off the shelf that enable physical or biological profiling could avoid performing risk assessments that capture how their specific uses of such technologies cause consumers to be targeted unfairly.

IV. The Rules Should Better Cover ADMTs Used for Advertising Concerning Significant Decisions.

The latest version of the proposed rules remove behavioral advertising from the scope of the requirements. This change was not necessary for businesses to be able to continue advertising,

⁵ Kyle Wiggers, *Cashierless Tech Could Detect Shoplifting, But Bias Concerns Abound*, VentureBeat (Jan. 23, 2021), <https://venturebeat.com/ai/cashierless-tech-could-detect-shoplifting-but-bias-concerns-abound/>.

⁶ *Id.*

as the previous version of the proposal did not prevent other forms of advertising, including contextual advertising and paid search advertising. Instead, this change allows businesses to continue monetizing people's personal data through privacy-invasive behavioral advertising.

Advertising in general has also been removed from the scope of the requirements for ADMTs. Previously, "significant decision" included decisions that result in access to or the provision or denial of several critical opportunities and services enumerated within the definition. ADMTs used for advertising could result in access to some of the services in those enumerated areas. The latest proposal explicitly excludes advertising from the definition of "significant decision," and eliminates "access to" from the definition. This change means that the requirements for ADMTs do not apply to ADMTs used to deliver advertising related to a significant decision. This will enable businesses to continue using, without any meaningful safeguards, behavioral advertising to determine – and limit – who receives advertisements about employment, housing, and other critical opportunities and services. The latest proposal therefore no longer addresses the use of personal data to prevent different groups of consumers from learning of and pursuing available opportunities and services. The Agency should restore the definitions and coverage of advertising and significant decisions in the previous version of the proposed rules.

V. Additional Provisions That Have Been Narrowed or Eliminated Should Be Restored.

In addition to reducing the scope of automated systems that are covered, the latest proposal reduces requirements for the relatively small percentage of businesses that would still be subject to these rules. Under the latest proposal, businesses would no longer be required to identify in their risk assessments whether they have implemented policies, procedures, and training to ensure that their ADMTs work as intended for their proposed use and that their ADMTs do not discriminate based on protected classes. The only provisions under which a business will now be obligated to ensure that their ADMTs work as intended and do not discriminate are the proposed exceptions to the right to opt out.

The latest proposal also eliminates other provisions that would have protected consumers' interests, including the following:

- Requirements for pre-use notice and for the right to access when a consumer's personal data is processed to train ADMTs, which would add some necessary friction as businesses are incentivized to stockpile people's personal data to train their products.
- A requirement for notice of a consumer's right to access after an ADMT was used to make a significant decision that was adverse to the consumer, which would be a necessary tool for a consumer to pursue recourse under consumer protection and civil rights laws.
- Guidance advising that the safeguards a business could incorporate in its risk assessment can include an evaluation of the need for human involvement, so that businesses would at least consider how human reviewers should be involved before an ADMT's output affects a consumer.

These changes further diminish the already limited reach of the proposed rules, and should be walked back.

VI. Conclusion

The CCPA gives the Agency clear direction to create protections regarding ADMTs. The transparency requirements laid out in the original proposed rules were the result of over three years of work by Agency staff and a variety of stakeholders to carry out the CCPA's mandate. The Agency's most recent move to scale back the proposed rules will hurt consumers and undermine the trust necessary to promote adoption of AI tools. We urge the Agency to reconsider its latest changes, which provide very few protections for California consumers, and return to a version of the previous rules that more effectively protected consumers and put in place guardrails that would grow trust in and adoption of AI.

Grenda, Rianna@CPPA

From: Ani Boyadjian <aboyadjian@ccala.org>
Sent: Monday, June 2, 2025 3:24 PM
To: Regulations@CPPA
Cc: Anh Nguyen; Nella McOsker
Subject: Public Comment on CPPA Updates for Automated Decisionmaking Technology (ADMT) Regulations
Attachments: CCA CPPA Comment Letter 6.2.25.pdf

This Message Is From an Untrusted Sender

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

Report Suspicious

Good afternoon,

On behalf of CCA, please see attached for our public comment on CPPA's Automated Decisionmaking Technology Regulations.

Thank you for your consideration.



Ani Boyadjian

Policy Associate

she/hers | 213.995.5402 | aboyadjian@ccala.org |

ccala.org

626 Wilshire Blvd., Suite 850, Los Angeles, CA 90017

[CCA Reflects](#)





June 2, 2025

California Privacy Protection Agency
2101 Arena Blvd
Sacramento, CA 95834

Submitted via email at: regulations@coppa.ca.gov

RE: Public Comment on CPPA Updates for Automated Decisionmaking Technology (ADMT) Regulations

To Whom It May Concern:

Established in 1924, Central City Association (CCA) represents approximately 300 member organizations committed to advancing policies and projects that enhance Downtown Los Angeles' vibrancy and increase economic opportunities. On behalf of CCA, I write to express our continued opposition to the proposed Automated Decision-Making Technology and Risk Assessment regulations. While we share the agency's goal of strengthening consumer privacy, these regulations as written still remain overly broad, extend beyond the agency's privacy mandate, and would impose substantial burdens on businesses that are out of proportion to any corresponding gains in consumer privacy. The agency should continue to revise these rules to focus on the kinds of specific, meaningful privacy risks that motivated California voters to create the agency, rather than creating sweeping requirements that would regulate and hamper a swath of routine business operations across California.

At a high level, these regulations still extend far beyond the reason voters, through Proposition 24, created the agency: to be an "independent watchdog whose mission is to protect consumer privacy." Instead, they persist in creating an expansive regulatory framework that would capture and regulate even basic, decades-old technologies that businesses large and small use every day, even if these systems pose no meaningful (let alone significant) privacy risks. The proposed rules remain overly broad and seek to regulate such a wide range of activities and policy areas that they would be unrecognizable to the Californians who supported Proposition 24. The result is that, according to the agency's own analysis, these revised regulations could cost businesses \$1.2 billion in compliance costs- and even this substantial figure likely understates the true economic impact.

We ask that you carefully consider the problematic issues described below:

- The regulations continue to define "automated decisionmaking" so broadly that they would apply to common, decades-old tools that are in no way autonomous or invasive. Even with changes to the definition, the current draft would still capture basic software systems used for everyday functions like analyzing employee performance, tracking safety metrics, or determining eligibility for routine bonuses. In such cases, the software functions solely as a decision-support tool for human managers, rather than as an autonomous decision-maker. Yet, these tools would still fall under the agency's regulatory authority, triggering extensive new requirements simply because they assist human judgment. That is not what voters intended when they approved Proposition 24 to safeguard consumer privacy.
- Second, while the regulations purport to target cutting-edge technologies with real privacy implications, such as facial recognition or emotion detection tools, they instead sweep in a vast range of routine, low-risk business activities. For example, even automated systems that calculate small performance-based incentives or attendance-based bonuses could be subject to regulation. There is no identified privacy harm posed by such systems, yet they would be treated as if they represent the same kind of risk as unregulated AI tools with no human oversight. This disconnect reveals the underlying flaw in the agency's approach: rather than targeting high-risk, high-impact use cases, the rules cast an unnecessarily wide net over ordinary business practices.

- Third, as currently drafted, Section 7150(b)(5) should be reassessed. The revised rule does address the initial issue by limiting the definition of "sensitive location" which would trigger the need for a risk assessment. However, even with the narrowed scope, the provision still creates operational uncertainty and compliance costs for businesses whose data practices may not pose real privacy risks such as providing discounts for prescriptions at specific pharmacies based on a consumer's prior use or college merchandise based on a student's resident at college. Thus, we recommend removal of this provision to enhance clarity and reduce administrative burdens on businesses.
- Finally, the proposed regulations seek to require businesses to perform risk assessments where ADMT was used before the effective date of January 1, 2027. This creates retroactive compliance obligations that are unclear, burdensome and difficult to implement. Hence, the first sentence in 7200(b) should be removed to prevent confusion for businesses.

While we recognize the agency's efforts to respond to feedback, the revised approach would still create significant costs and complications while failing to effectively address the privacy concerns that motivated California voters to give the agency its mandate to adopt these rules. We strongly urge the agency to once again substantially revise these proposed regulations to focus on meaningful privacy risks while avoiding unnecessary burdens on California's business community.

Sincerely,



Nella McOskey
President & CEO
Central City Association

Grenda, Rianna@CPPA

From: Gebriel Saleh <gebriel@cfca.energy>
Sent: Monday, June 2, 2025 9:22 AM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: CFCA Comments - CCPA ADMT Proposed Amendments (OFFICIAL).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

Good Morning!

Please see the attached comments on behalf of CFCA.

If you have any questions, do not hesitate to reach out to CFCA's Sr. Director, Government Affairs, Alessandra Magnasco at alessandra@cfca.energy

Kind regards,
Gebriel Saleh
Policy Aide

2520 Venture Oaks Way, Suite 100 | Sacramento, CA 95833
Main: (916) 646-5999 ext 972 | Fax: (916) 646-5985 | www.cfca.energy





day
at the
capitol.

protect your k
shape policy.
make an impa

APRIL 30, 2025

Advocates for the fuels and convenience store industries since 1952



California Fuels and Convenience Alliance

2520 Venture Oaks Way, Suite 100

Sacramento, CA 95833

916.646.5999

May 21, 2025

California Privacy Protection Agency
400 R Street, Suite 350
Sacramento, CA 95811

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

The California Fuels and Convenience Alliance (CFCA) represents about 300 members, including nearly 90% of all the independent petroleum marketers in the state and more than half of the state's 12,000 convenience retailers. Our members are small, family- and minority-owned businesses that provide services to nearly every family in California. Additionally, CFCA members fuel local governments, law enforcement, city and county fire departments, ambulances/emergency vehicles, school district bus fleets, construction firms, marinas, public and private transit companies, hospital emergency generators, trucking fleets, independent fuel retailers (small chains and mom-and-pop gas stations), and California agriculture, among many others.

CFCA appreciates the opportunity to provide feedback on the proposed updates to the California Consumer Privacy Act (CCPA), particularly regarding the sections on automated decision-making technology (ADMT), risk assessments, and cyber regulations.

SUPPORT REMOVAL OF AI LANGUAGE

CFCA supports the Agency's decision to remove language related to artificial intelligence (AI) from the proposed rule. Given the early and rapidly evolving nature of AI tools and foundational models, attempts to regulate this space prematurely risk unintended consequences. Regulatory frameworks at this stage are particularly vulnerable to misapplication and could lead to inconsistent enforcement or undue burdens on businesses. Introducing vague or overly broad AI-related requirements could have created significant compliance challenges without delivering meaningful consumer protections. By choosing to hold off on regulating AI at this time, the Agency has wisely preserved room for innovation while ensuring that responsible development and deployment of these technologies can continue unimpeded.

SUPPORT REMOVAL OF SYSTEMATIC OBSERVATION FROM EXTENSIVE PROFILING

CFCA also strongly supports the Agency's removal of "systematic observation" from the definition of "extensive profiling."

This change provides critical clarity and relief to fuel retailers and convenience operators who rely on security and surveillance systems to protect their customers, staff, and assets. In recent years, the rise of

organized retail crime—including fuel skimming, drive-offs, and identity theft at pumps—has made video surveillance and license plate recognition technology an essential safety measure.

For example:

- Retailers use cameras and LPRs to identify vehicles involved in fuel theft or tampering with point-of-sale systems.
- Many stations coordinate with local law enforcement using this footage in active criminal investigations.
- These tools are passive, non-discriminatory, and used solely to monitor for criminal activity or emergencies—not to derive behavioral profiles or make marketing decisions.

Had “systematic observation” remained in the rule, these legitimate and narrowly tailored uses of security footage could have been swept into high-risk profiling definitions—triggering unnecessary audits, disclosures, or opt-out mechanisms for routine, legally permitted surveillance.

ADDITIONAL COMMENTS ON ADMT AND RISK ASSESSMENTS

While we support the Agency’s revised approach to ADMT, CFCA urges continued consideration of the practical realities facing small and mid-sized businesses in the fuel and convenience sector. Many members use software that could, depending on interpretation, fall under the definition of ADMT—including:

- Automated hiring platforms that screen applicants for driver or cashier roles;
- Inventory management systems that adjust restocking schedules or pricing algorithms without human review.

If such tools are ultimately covered under ADMT definitions, we urge the Agency to:

- Provide clear thresholds and carve-outs for low-risk or operational ADMT uses that do not materially impact consumer rights or access;
- Clarify how “human involvement” is evaluated **in practice**, especially for businesses with limited staffing resources.

CFCA appreciates the Agency’s ongoing efforts to strike a balance between consumer protection and operational feasibility. We are encouraged by the revisions that remove unnecessarily broad or vague language and align the regulations more closely with real-world business practices.

We look forward to working with the Agency to ensure that California’s privacy regulations remain clear, enforceable, and considerate of the needs of business operators who serve as the foundation of the state’s fuel and convenience economy.

If you have any questions, please contact Alessandra Magnasco at alessandra@cfca.energy.

Sincerely,



Alessandra Magnasco
Sr. Director, Government Affairs

Grenda, Rianna@CPPA

From: Robert Singleton <robert@progresschamber.org>
Sent: Monday, June 2, 2025 1:47 PM
To: Regulations@CPPA
Cc: Todd O'Boyle
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: Chamber of Progress_June2_Comments on Modified Text_CPPA.pdf

This Message Is From an Untrusted Sender

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

Report Suspicious

Dear Executive Director Kemp and Board Members of the California Privacy Protection Agency:

On behalf of Chamber of Progress – a tech industry association supporting public policies to build a more inclusive society in which all people benefit from technological advancements – I write regarding your recently published Modified Text of Proposed Regulations for Updates to Existing CCPA Regulations, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies.

Please see our attached letter that outlines our concerns with the Modified Text of the draft regulations.

Sincerely,
Robert

--



Robert Singleton

He/him

Senior Director of Policy and Public Affairs, CA & US West

707.569.4546

robert@progresschamber.org



June 2, 2025

The Honorable Tom Kemp
Executive Director,
California Privacy Protection Agency
2101 Arena Boulevard
Sacramento, CA 95834

Re: *Modified Text of Proposed Regulations for Updates to Existing CCPA Regulations, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies.*

Dear Executive Director Kemp and Board Members of the California Privacy Protection Agency:

On behalf of Chamber of Progress – a tech industry association supporting public policies to build a more inclusive society in which all people benefit from technological advancements – I write regarding your recently published *Modified Text of Proposed Regulations for Updates to Existing CCPA Regulations, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies*. While the Modified Text is significantly better than the initially proposed draft regulations, it still contains several flaws that, if adopted, would harm California businesses, workers, and consumers.

Critical terms are poorly defined and over-inclusive

The Modified Text's language on "significant decision" is still deeply problematic. It applies to "a decision that results in the provision or denial of financial or lending services, housing, education enrollment or opportunities, **employment or independent contracting opportunities or compensation**, or healthcare services. [Emphasis added]" Notably, it further includes "allocation or assignment of work for employees." This broad wording implicates large swathes of the platform economy. California-based platform companies like Uber, DoorDash, and Instacart use algorithmic tools to assign tasks in their normal course of business. These are not "significant decisions" in the sense of granting or denying employment, determining an annual bonus, etc.

By burdening these platform companies, the Agency is not merely regulating tech companies, it is undermining the drivers, restaurateurs, grocers, and consumers that depend on these services daily. At a time when the Trump tariffs have wrought havoc on the California economy, the CPPA should not be making it harder for independent

contractors to find sidework or restaurants to find business. This burden is perhaps most acute for homebound and disabled Californians who may lose access to delivery services for groceries and prepared meals.

We were encouraged by Board Member Mactaggart's comments at the April 4th board meeting of the Commission. He stated that after reviewing the hundreds of pages of comments submitted by various civil society organizations, businesses, and consumer groups, he agreed and sympathized with the shared criticism that the CPPA was potentially overstepping its statutory authority, and was opening the door to potential legal challenges. Furthermore, Board Member Mactaggart correctly pointed out that critics of the draft regulations worried that "inclusion of the new term 'behavioral advertising', invented in the regulations, which is not defined anywhere in the statute... will destroy first party advertising, i.e. from business to its own customers."¹

Given this direct response to ours and others' previously submitted comments, we would be remiss to not acknowledge, and thank, both Mr. Mactaggart and the CPPA Board for having considered and meaningfully addressed these concerns within their Modified Text of these draft regulations. We have thus attempted to narrow our comments to specific concerns in relation to the management of independent contractors and other decisions we believe to be significant.

The CPPA still needs to narrow its focus to consumer privacy

California voters created the CPPA, and in so doing, gave it a clear remit to protect their privacy. They did not vote to police automated decisionmaking or scrutinize algorithmic task allocation on food delivery platforms.

We share Governor Newsom's concern that the CPPA's regulatory undertakings "could create significant unintended consequences and impose substantial costs that threaten California's enduring dominance in technological innovation."² The CPPA should focus on its core mission and **withdraw** the Modified Text, pending significant revisions.

Sincerely,

A large black rectangular box redacting the signature of Robert Singleton.

Robert Singleton

¹ <https://www.youtube.com/watch?v=qvRonzmjUgY>

² See <https://www.politico.com/news/2025/04/24/newsom-california-privacy-cppa-ai-00307233>

Senior Director of Policy and Public Affairs, California and US West

Grenda, Rianna@CPPA

From: Reisman, Matthew <MReisman@hunton.com>
Sent: Monday, June 2, 2025 3:32 PM
To: Regulations@CPPA
Cc: Clarington, Malachi; Abdelaziz, Laila; Smith, Mark
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: CIPL Response to Modified CCPA Regulations FINAL.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](#)

Dear Sir or Madam,

Please find attached comments from the Centre for Information Policy Leadership (CIPL) in response to the Agency's call for Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations.

Kind regards,
Matthew Reisman



Matthew Reisman (he/him)
Director of Privacy and Data Policy
mreisman@Hunton.com
p 202.955.1832
m [REDACTED]

Hunton Andrews Kurth LLP
2200 Pennsylvania Avenue, NW
Washington, DC 20037

www.informationpolicycentre.com

This communication is confidential. If you are not an intended recipient, please advise by return email immediately and then delete this message, including all copies and backups.

Comments by the Centre for Information Policy Leadership (CIPL) on the California Privacy Protection Agency's Notice of Modifications to Text of Proposed Regulations and Additional Materials Relied Upon

Submitted June 2, 2025

The Centre for Information Policy Leadership (CIPL)¹ welcomes the opportunity to respond to the California Privacy Protection Agency's (the Agency)'s Notice of Modifications to Text of Proposed Regulations and Additional Materials Relied Upon.² CIPL commends the Agency for the steps it has taken to clarify key concepts, tailor heightened obligations for processing that may present significant risk, and reduce regulatory burdens, while striving to ensure a high level of data privacy and security and enable beneficial data use. CIPL notes with appreciation that the Agency has incorporated many of the key suggestions offered in its comment submitted in February (available [here](#)).³ CIPL's comments below identify opportunities to further strengthen the rules via a risk-based approach grounded in concepts of organizational accountability.⁴

Article 1. General Provisions

§7001 Definitions

- The agency has taken useful steps to clarify the definition of **automated decisionmaking technology (ADMT)** at §7001(e). The application of a risk-based approach to the obligations for ADMT is vital, and the Agency advances this through the associated concept of “**significant decision**.” The new definition of significant decision at §7001(ddd) helpfully clarifies circumstances in which ADMT activities will necessitate a risk assessment as per §7150(b)(3) and be subject to the requirements under Article 11. It more clearly focuses on processing activities likely to pose higher risks to individuals than the definition that previously appeared within the

¹ **The Centre for Information Policy Leadership (CIPL)** is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

² The Notice of Modifications to Text of Proposed Regulations and Additional Materials Relied Upon can be found here: https://Agency.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_notice.pdf

³ CIPL Response to the California Privacy Protection Agency's Draft CCPA Updates, Insurance, Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking Technology (ADMT) Regulations, submitted February 25, 2025, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_public_comments_Agency_regulations_risk_assessments_automated_decisionmaking_technology.pdf.

⁴ CIPL Report, “What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework” (May 2020), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_mapping_report_27_may_2020_v2.0.pdf.

text of §7150. The exclusion of “advertising to a consumer” from the definition is especially helpful in this regard.

- At the same time, further changes could be helpful for sharpening the focus of the obligations in connection with the Agency’s consumer privacy mandate and providing businesses with necessary clarity. The Agency should:
 - Add a materiality threshold to the definition of significant decision, so that it applies to activities that have “material adverse legal or economic effects.”
 - Modify §7001(e)(2) to indicate that profiling is included within the definition of ADMT only to the extent that it is used to produce a significant decision.
 - Modify §7001(ddd)(B)(4) to remove “allocation or assignment of work.” Allocation of assignments is a lower-risk activity with respect to consumers while constituting an important aspect of businesses’ operations.
 - Bind the language on compensation to focus on decisions with material adverse legal or economic effects and to exclude activities that do not meet this threshold, such as routine administrative actions needed to process payroll.
 - Limit “financial and lending services” to a more clearly delineated set of high-risk activities. For example, the “provision” of deposit and checking accounts, transmitting funds, and facilitating installment payments may all capture lower-risk processing to operate existing accounts; the language should focus more specifically on the “opening” of accounts. Greater clarity should also be provided as to how these obligations will work with respect to the Gramm-Leach-Bliley Act (GLBA) exemptions specified in the law.
 - Explicitly exclude from the definition technology and decisions intended to detect and respond to security incidents and resist malicious, deceptive, fraudulent, or illegal actions.

The concept of “**profiling**” subject to heightened regulatory obligations should be limited to activities that effectuate a significant decision concerning a consumer. The current scope of regulations would extend risk assessment requirements to many beneficial profiling decisions that do not present significant risk to consumers’ privacy and security, thereby burdening businesses with compliance processes that do not provide meaningful privacy and security protections to consumers. Importantly, the current approach contravenes the statutory requirement to issue regulations requiring risk assessments for processing that presents significant risk.⁵ As currently drafted, businesses would need to complete risk assessments for low-risk profiling decisions such as automated processing that predicts a person’s font or music preferences in a particular software or application. The current definition is also likely to capture longstanding, uncontroversial systems that employers and managers use in the workplace. For example, even rudimentary systems that track metrics like production, sales targets, or staffing levels all “analyze” “performance at work,” and simple software that tracks whether employees are late to

⁵ Cal. Civ. Code § 1798.185(a)(14) (2024).

clock in to work analyzes “reliability.” These systems do not replace human decisionmaking, make significant decisions, or pose any consumer privacy risk.

- The concept of “**automated processing**” appears several times throughout the modified rules and is important in the definition of profiling (§7001(ii)) as well as the rules for determining when a risk assessment must be completed (§7150(4) and (5)). The phrase appears intended to address instances where processing is *solely* automated. The text should clarify this scope accordingly.
- The Agency should align the definition of “**penetration testing**” (§7001(bb)) with the most current definition provided by the U.S. National Institute of Standards and Technology (NIST).⁶ This modification would foster interoperability with other data privacy and security rules and standards, consistent with the CCPA’s instruction to “cooperate with other agencies with jurisdiction over privacy laws and with data processing authorities in California, other states, territories, and countries to ensure consistent application of privacy protections.”⁷
- The revised definition of “**physical or biological identification or profiling**” at §7001(ee) should be further tailored by introducing an intent standard, so that the obligations apply to systems intended to be used to identify individuals and exclude systems not used for identification purposes. The intent requirement should consider whether developers and deployers of biometric technologies take reasonable measures (e.g., technical, organizational, and contractual) to ensure that the processing of biometric characteristics cannot be used for identifying purposes.⁸ Adding this intent standard would align this definition with the statutory definition of “biometric information”, where data is in scope if it is “is used or is intended to be used” for identifying purposes.⁹ Furthermore, emotion recognition should only be within scope to the extent that it is used to make a significant decision or to identify or recognize a consumer.
- The definition of “**systematic observation**” at §7001(eee) should be revised to clarify that it applies to truly systematic recordings, such as CCTV and video surveillance, which present a greater degree of risk than other types of recording (such as recording of business meetings).

§7004 Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent

- The symmetry in choice requirement (§7004(a)(2)(A)) should reflect that there may be a different number of steps needed for a consumer to opt in (e.g., through a single click) versus opt out of sharing information – which could, for example, necessitate follow-on verifications. The regulations should require symmetry as a general principle but not limit opt outs to the “same or fewer” steps in all instances.

⁶ NIST has provided different definitions in different publications; the most recent dates from November 2022 and is based on the definition from ISO/IEC 19989-3:2020. See https://csrc.nist.gov/glossary/term/penetration_testing.

⁷ Cal. Civ. Code § 1798.199.40.

⁸ For more on this topic, please see CIPL, *Enabling Beneficial and Safe Uses of Biometric Technology Through Risk-Based Regulations*, April 2024.

⁹ Cal. Civ. Code § 1798.140(c).

- The Agency should take care to ensure that the proposed prohibition on “general or broad terms of use” (§7004(a)(4)(C) within choice architecture is not in tension or conflict with the broader requirements of the law for business to provide Notice at Collection.

Article 3. Business Practices for Handling Consumer Requests

- With respect to the requirement in §7020(e) to provide consumers the ability to specify a date range for “requests to know”, the regulations should acknowledge that a business should only be expected to respond with respect to information that the business continues to maintain.
- With respect to obligations related to Requests to Correct, the Agency should restore the “implement measures to” language stricken from §7023(c) in the most recent version. Doing so would appropriately task the business with striving to keep corrected information accurate but recognize that its ability to do so may be affected by factors outside its control.
- The Agency should add language indicating that where illustrative examples are provided, such as under §7023(m)(2) and (3), those examples are not meant to be exhaustive.

Article 10. Risk Assessments

CIPL appreciates the Agency’s effort to clarify and simplify the risk assessment requirements using an approach tiered to the level of likely risk. The updated draft regulations are more aligned with the statutory requirement to produce risk assessments when processing may pose significant risk.

- The regulations include some requirements that add administrative burden without corresponding privacy benefits for consumers. For example, the obligation set forth in § 7157(b)(3) to submit to the Agency information about the number of risk assessments conducted or updated *for each processing activity* would require businesses to link each risk assessment to individual processing activities, even though processing activities may cross over multiple risk assessments and a single risk assessment may cover multiple processing activities. In addition, the obligation set forth in § 7155(a)(2) to review and update as necessary all risk assessments would impose undue burden in light of the obligation to update the assessment where there are material changes in processing practices set forth in § 7155(a)(3).
- In our previous submission, CIPL noted that §7050(h)(2) and §7153(a) appropriately acknowledge that service providers may have a role to play in assisting customers (“recipient-businesses”) with meeting their risk assessment compliance obligations. The Agency has taken useful steps to adjust the language in these sections to avoid misaligned expectations between recipient-businesses and service providers on roles and responsibilities with regards to risk assessments. The Agency should amend the language further to ensure that the obligations under §7050(h)(2) and §7153(a) do not pose an undue and unintended burden on service providers. Because service providers may have a high number of customers needing support for their risk assessments, the regulations should explicitly enable service providers to share information with their business customers in a standardized and readily replicable way about how their products and services work. Additionally, service providers should not be required to disclose trade secrets or intellectual property when complying with these obligations (see below).
- §7150(b)(6), which enumerates when processing poses a significant risk to consumers’ privacy, includes training of ADMT for a list of enumerated purposes “or profiling of a consumer.” The “or” introduces uncertainty as to the intended scope of the provision. CIPL

recommends that profiling be included only to the extent that it is associated with activities that make a significant decision concerning a consumer, consistent with the suggestion regarding the definition of profiling above.

- The draft regulations would require the participation of a number of individuals to conduct risk assessments that are not always needed. For example, § 7151(a) states that employees whose job duties include participating in the processing of personal information that would be subject to a risk assessment must be included in the risk assessment process for the relevant activity. Section 7152(a)(8) further states that risk assessment must identify and document individuals who provided the information for the risk assessment, barring only legal counsel from this obligation. Many employees may have “job duties” that include participating in the processing of personal information or determining the methods whereby it will be processed. Requiring businesses to seek the feedback of every such person could require large expenditures of time and resources that would not necessarily enhance the quality of the risk assessment. As an alternative the Agency should require that businesses consult with an individual who is primarily responsible for the processing activity in question. The Agency should similarly revise the regulations such that businesses need not provide the name of every individual who provided information for the risk assessment and instead include, for example, the individual who has the authority to participate in deciding whether the business will initiate the processing that is the subject of the risk assessment.
- The draft regulations would prohibit the use of the phrase “to improve our services” in risk assessments (e.g., § 7152(a)(1)) as well as in communications to consumers (§ 7222(b)(1)). CIPL urges the Agency to provide organizations flexibility to identify a range of potential improvements without identifying them granularly. The potential for new and unforeseen needs for product improvement to arise as technology and consumer interactions with products and services evolve necessitates greater flexibility.
- The Agency takes useful steps in § 7156 to clarify interoperability mechanisms with risk assessment requirements in other states. The Agency should consider a more flexible approach that would allow a business to more readily rely on a single risk assessment to cover a set of similar and interconnected processing activities across states, provided that all substantive elements are included. Interoperability mechanisms for risk assessment obligations are extremely impactful as they allow businesses to harmonize compliance and technical processes and avoid procedural burdens, without impacting the level of privacy and security afforded to individuals.
- The Agency has added helpful language clarifying that ADMT Pre-use Notice Requirements (§ 7220(d)) and responses to Requests to Access ADMT (§ 7222(c)) are not required to include trade secrets or information that would compromise a business’s ability to combat fraud or prevent and address security, safety, and illegal behavior. As CIPL suggested in its previous submission, the Agency should extend the same protections to risk assessments, e.g., with respect to requirements to describe the “logic” of ADMT at § 7152 (a)(3)(G) and required disclosures to “recipient businesses” of ADMT at § 7153(a). Furthermore, the regulations should provide assurances that the Agency will protect the confidentiality of materials submitted by businesses related to risk assessments.

- The requirement that a member of the business’s executive management team with specialist knowledge of risk assessments must attest, under penalty of perjury, that risk assessment information submitted to the Agency is true and correct (§ 7157(b)(5)) could have the unintended effect of deterring otherwise qualified individuals from leading data privacy management programs. The Agency could address this concern while preserving accountability by requiring attestation that the information is correct “to the best of [the individual’s] knowledge” and removing the reference to perjury.

Article 11. Automated Decisionmaking Technology

The Agency has taken useful steps to tailor the ADMT requirements to situations more clearly meeting the proposed definition of the technology and posing higher risks while enabling beneficial uses of the technology. The removal of training from the list of uses in §7200 is especially important in this regard. The Agency has also helpfully simplified and clarified the rules on opt-out and requests to access.

- The Agency should restore and expand language in § 7221(b) indicating that a business is not required to provide consumers the ability to opt out of ADMT when the use of ADMT is necessary “to resist, prevent, and detect malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions,” consistent with the language of ADMT pre-use notices (§ 7220(d)) and responses to Requests to Access ADMT (§ 7222(c)).

Grenda, Rianna@CPPA

From: Lucy Chinkezan <lchinkezan@cjac.org>
Sent: Monday, June 2, 2025 1:40 PM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations - CJAC
Attachments: CJAC Comments to CPPA on ADMT and Risk Assessments 6-2-25.pdf

This Message Is From an Untrusted Sender

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

[Report Suspicious](#)

Dear CPPA Board and Staff:

Enclosed please find public comment from the Civil Justice Association of California on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations.

Lucy Chinkezan

Senior Counsel

Mobile [REDACTED] | www.cjac.org





June 2, 2025

Sent Via Email

California Privacy Protection Agency
Attn: Legal Division – Regulations Public Comment
regulations@coppa.ca.gov

Re: *Comments by the Civil Justice Association of California on Proposed Rulemaking Regarding Automated Decisionmaking Technologies, Cybersecurity Audits, and Risk Assessments*

Dear California Privacy Protection Agency Board and Staff:

Thank you for the opportunity to provide comment on the proposed rulemaking regarding Automated Decisionmaking Technologies, Cybersecurity Audits, and Risk Assessments. Founded in 1979, the Civil Justice Association of California (CJAC) is the only statewide association dedicated solely to improving California's civil liability system, in the legislature, the regulatory arena, and the courts. Our membership base consists of businesses and associations from a broad cross-section of California industries.

We commend this agency for taking on the tremendous task of updating these draft regulations in a short period of time, and for its willingness to cooperate with stakeholders to reach a compromise that is in the best interest of all Californians. Below we highlight our most pressing concerns with the updated draft regulations. We respectfully request that you address these concerns as recommended below.

Article 1

Section 7001(e)

As currently drafted, it is unclear what information would be "relevant" to make a decision. It also may be impossible for a human reviewer to consider all such factors. A business protocol on what information is needed to make a decision or exception should suffice.

Relatedly, while we appreciate the comprehensive list of exceptions to ADMT identified in section 7001(e)(3), we suggest striking the qualifier language at the end of the list as it negates the purpose of the list. We also suggest adding "search term software" to the list, in order to exclude from ADMT manual searches made by employers or recruiters using terms to narrow the scope of an applicant pool.

Proposed Revision

We recommend revising section 7001(e)(1)(b) as follows:

Review and analyze the output of the technology, and any other information that is ~~relevant~~ necessary to make or change the decision; and

We recommend revising section 7001(e)(3) as follows:

ADMT does not include web hosting, domain registration, networking, caching, website-loading, data storage, firewalls, anti-virus, anti-malware, spam- and robocall-filtering, spellchecking, calculators, databases, search term software, and spreadsheets, ~~provided that they do not replace human decisionmaking.~~

Section 7001(ddd)

Employment-related decisions should be limited to hiring or firing, not allocation or assignment of work, compensation, bonuses, etc.

Article 10

Section 7150(b)(4)

We recommend striking this section entirely.

Section 7150(b)(5)

We support the revision in this section that limits the locations where the obligation to conduct risk assessments is triggered. However, the draft rules continue to regulate the use of ADMT to process publicly available information. Consumers do not have a reasonable expectation of privacy in a public space, whether on a college campus or at a grocery store with a pharmacy.

The CPRA already regulates the use of data collected from geo-trackers which identify a consumer's precise geolocation. Per the draft rulemaking, a controller must still conduct a risk assessment and provide an opt out.

This broad requirement captures low-risk activities. Such activities may include a business providing discounts for prescriptions at specific pharmacies based on a consumer's prior use.

Proposed Revision

We propose striking section 7150(b)(5).

Section 7150(b)(6)

We appreciate that the draft rules now regulate ADMT that a business "intends to use" rather than "is capable of" using.

However, as currently drafted, the term "intends to use" includes "permits others to use, plans to permit others to use" and advertising such uses. This qualifying

language should be removed, as it negates the change and will capture a wide-range of general use models that are primarily used for other, low-risk purposes.

Further, risk assessments should not be required for the processing of model training used for emotion recognition, if it does not otherwise identify a specific person. The rulemaking should also not expressly call out training for models used for biological identification.

Risk assessments are already required for processing of sensitive data, which includes biometric data as defined under CPRA. They should not be required for models that are not trained on biometric data, to continue incentivizing developers to minimize the sensitive data that they use in training.

Section 7152(a)(3)

As a general matter, the approach to risk assessments in the proposed rules under section 7152 is overly prescriptive. This could lead a company to complete reports for the sole purpose of satisfying the requirement rather than for its intended purpose.

The purpose of the risk assessment report is to ensure the business weighs the potential privacy harms resulting from certain high-risk processing activities against the benefits. Processing activities that require risk assessments will evolve as businesses continue to innovate. Businesses should retain flexibility in how to approach assessments to make sure that they identify and weigh the right factors.

This approach will be unreasonably burdensome and costly for both businesses and innovation in the state, outweighing any potential privacy benefits to consumers. Many California companies operate beyond the state's borders. Nearly all other privacy frameworks including the GDPR require a business to prepare risk assessments tailored to the processing activity. This agency's formulaic approach is inconsistent with those frameworks, meaning businesses will need to prepare a supplemental report specific to California for the same processing activity. It is unclear what, if any, benefits this requirement will have for the state's consumers.

More specifically, section 7152(a)(3)(F) is too prescriptive. Section 7152(a)(1) already requires an assessment to identify the processing purpose. Section (a)(3)(F) goes a step further, requiring mapping those purposes to specific third parties. A business should consider in its assessment both processing purposes and sharing, but mapping will not always be necessary; businesses already disclose categories of data sharing in their privacy notice and the purpose of processing in agreements with service providers.

Further, as to Section 7152(a)(3)(G)(i), research is still being conducted on the logic of ADMT models. Moreover, the focus on methodology is not tethered to the risk

to the consumer—privacy or otherwise. Instead, the risks are related to an adverse impact of a significant decision and whether a data subject can exercise rights. These are sufficiently addressed by other Risk Assessment provisions.

Section 7156(b)

For consistency with other state privacy laws, the rulemaking should permit businesses to utilize and submit assessments prepared for another purpose whose requirements are reasonably similar in scope and effect to this rulemaking.

Section 7157(b)

We appreciate that the revised rules eliminate the requirement to submit abridged assessments that identify processing activities that triggered the assessment and explain the purpose of processing.

However, we continue to have concerns about the information that is required to be submitted to the agency per this subsection. The agency should consider limiting the submission requirement to certain processing activities only—namely, sales of sensitive data.

Alternatively, the agency should seek to limit the information sought to metrics, or the number of assessments. Companies are already obligated to disclose in their privacy notice the types of personal data that they collect, process, and share. Including this information in the submission is thus unnecessary.

Article 11

Section 7200(a)(1)

A business should not be required to provide a risk assessment where ADMT was used prior to the effective date of this rulemaking, and is not used on or after the effective date.

Proposed Revision

We recommend striking the first sentence in section 7200(b) as follows:

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

Section 7220(a)

The regulations have not been revised to limit the pre-use notice requirement to instances where ADMT processing is otherwise subject to access and opt-out rights. Businesses will thus be required to provide such notices even if they use ADMT for exempt purposes.

Proposed revision:

We suggest revising this provision as follows:

A business that uses automated decisionmaking technology as set forth in section 7200, subsection (a), [and subject to the exceptions in section 7221\(b\) and section 7222\(a\)\(1\)](#), must provide consumers with a Pre-use Notice. The Pre-use Notice must inform consumers about the business's use of automated decisionmaking technology and consumers' rights to opt-out of ADMT and to access ADMT, as set forth in this section. A business may provide a Pre-use Notice in its Notice at Collection, provided that the Notice at Collection complies with, and includes the information required by, subsections (b) and (c).

Section 7220(c)(5)

The draft rules continue to require disclosure of a significant amount of information in a pre-use notice.

The most concerning provisions in this section include 7220(c)(5)(A) and (B), which require disclosure of the type of outputs generated and how the output is used to make a significant decision.

This agency should carefully consider whether disclosure of this information outweighs any potential risks, and whether the risks are better mitigated through an assessment that requires rigorous testing.

Further, it is unclear how section (A) relates to 7222(b)(2) regarding the access right, as one requires disclosing how ADMT processes personal information to make a decision and other the ADMT logic.

Section 7221(b)(2) & (3)

As written, the language in this section suggests that the exception to opt-out would not apply to ADMT that is used for assignment of work and business management of its products and services. The latter is not a significant decision.

Further, an ADMT deployer should be able to rely on an assessment or instructions from developer rather than be required to conduct an independent assessment.

Proposed revision

We suggest revising section 7221(b)(2) as follows:

(A) The business uses the ADMT ~~solely~~ for the business's assessment of the consumer's ability to perform at work or in an educational program to determine whether to admit, accept, or hire them; and

We suggest revising subsection 7221(b)(3) as follows:

(A) Uses the automated decisionmaking technology ~~solely~~ for the business's allocation/assignment of work or compensation; and

Section 7221(i)

The agency has not addressed the concerns raised previously about this subsection.

Mandating a single opt-out presumes that the use of ADMT is generally harmful to consumers or lacks benefits. It is antithetical to California's pursuit of innovation, efficiency, and tools that reduce human error and bias.

The draft rulemaking requires businesses to provide consumers with an option to opt-out of all covered ADMT, while still presenting consumers a choice to allow specific uses. This will confuse consumers, who will struggle to comprehend the impact of a general opt out in the abstract.

Consumers will thus opt out to avoid certain high risk use cases, and in effect lose out on the benefits of a vast range of potential use cases, such as screening for health risks.

Instead, business should be required to provide an opt-out option that is targeted to the specific use case. This way, the consumer can make a decision in real time and in the context of what is being opted out of, rather than in the abstract.

Proposed Revision

We suggest amending 7221(i) as follows:

In responding to a request to opt-out of ADMT, a business may present the consumer with the choice to allow specific uses of automated decisionmaking technology ~~as long as the business also offers a single option to opt-out of all of the business's use of automated decisionmaking technology set forth in subsection (a).~~

Section 7222(a)

We appreciate that the rules have been revised to expressly state that a business need not include in its pre-use notice, or responses to requests to "access" ADMT, any trade secrets or information that would compromise protection against security incidents, fraud, or other illegal activity.

The revised rules, however, still require that business responses be tailored to the *specific consumer* making the request.

As previously discussed, at minimum, the access right should be limited to an *adverse* decision. A company should not be required to explain details about when and how it uses technology when no harm is involved, such as where a consumer is pre-approved for credit. This is consistent with the FCRA and the Equal Credit Opportunity Act. We are not aware of any other regulatory framework that requires a company to disclose how it made a non-adverse decision to a consumer.

If the terms "ADMT" and "significant decision" are broadly interpreted to include interim hiring decisions or filtering tools, it would be impractical to require a business to respond to consumer-specific access requests on how the ADMT was

applied to them, regardless of whether it was adverse. This will eliminate the advantages of using automated tools in the first place.

Section 7222(b)

If pre-use notice is required when accessing ADMT, it should at minimum be limited to where ADMT use results in an adverse decision.

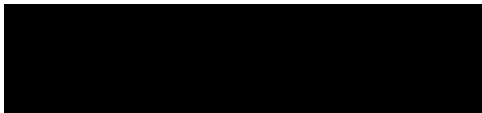
That said, we recommend striking section 7222(b)(2) entirely, even if limited to where ADMT is used for an adverse decision. No other regulatory frameworks that compel a business to explain an adverse decision require disclosing methodology.¹ The methodology has no correlation to any privacy risk to the consumer. Requiring disclosure instead creates a moral hazard. The only foreseeable reason a consumer would access methodology is to copy it for their own business needs or use it to exploit the system, defeating the purpose of the technology and harming all consumers.

Further, section 7222(b)(3) is inconsistent with the definition of ADMT, which is limited to technologies that fully replace or substantially replace human decisionmaking. As currently written, the language suggests that this requirement applies to interim automated tools. If the intention of the rule is to inform consumers about the purpose of the decision, it is achieved under section 7222(b)(1).

Conclusion

For the foregoing reasons, CJAC respectfully asks that the proposed revisions be amended to address the concerns that we have raised. Please do not hesitate to contact me at 916-217-5863 if you should have additional questions.

Respectfully submitted,

A black rectangular redaction box covering the signature of Lucy Chinkezan.

Lucy Chinkezan
Senior Counsel

¹ For example, under the Fair Credit Reporting Act, the notice when taking an adverse action based on a consumer report must explain that an adverse action occurred, identify the consumer rights, and provide contact info of consumer reporting agency. The notice need not disclose the methodology of the decisionmaking.

From: Shanthi Ramakrishna <shanthi.ramakrishna@connectedcouncil.org>
Sent: Monday, June 2, 2025 1:16 PM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: 3C Public Comment on CPPA Updates_ ADMT (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

Dear CPPA,

On behalf of the Connected Commerce Council (3C), we would like to submit the following comment to the CPPA for consideration.

"California Privacy Protection Agency Chair Urban, Board Members, and Staff:

On behalf of the Connected Commerce Council (3C) — a nonprofit organization dedicated to promoting small businesses' access to essential digital tools — I write to share our continued concerns about the CPPA's proposed regulations for automated decision-making technology (ADMT). While we appreciate the revisions adopted last month, we remain concerned that the regulations will hurt California small businesses.

ADMT-powered tools significantly improve California small businesses' efficiency — boosting their bottom lines and helping them grow and compete with larger firms. By providing affordable assistance with time-consuming tasks like staff scheduling, employee benefits selection, and fraud detection, ADMT-powered tools allow small businesses to use their limited time and money to improve their core offerings, connect with customers, and grow.

Our [research](#) shows that:

- 55% of all SMB leaders say AI tools will be critical to the success of their business during the next two years. 81% (+26%) of those already using AI in their business feel that way.
- 63% of all SMB leaders believe AI tools help "level the playing field" for businesses of all sizes. 83% (+20%) of those already using AI in their business feel that way.

Even as revised, the proposed rules would make it significantly harder for small businesses to adopt and use these valuable tools. Many firms would face costly and burdensome new obligations, including implementing complex technical upgrades to help manage notice requirements, opt-out processes, and appeals; responding to detailed information-access requests; and documenting and reporting on security policies and measures. Small businesses don't have in-house lawyers or compliance teams. To follow the rules, they'd need to hire expensive consultants they can't afford, or devote staff time they can't spare. Some would likely abandon key efficiency-enhancing tools — hurting their business — to reduce legal risk. But because many ADMT functions are embedded in third-party software (e.g., retailers use [financial service](#) firms' software to offer customers "buy now

pay later” options), even the most scrupulous businesses could find themselves in unwitting noncompliance with the rules.

In addition, firms that provide ADMT-powered tools to small businesses would be forced to redesign their products to comply with the regulations, likely raising development costs. Those costs would almost certainly be passed on to small businesses — making it harder for them to access and benefit from the tools, and putting them at a competitive disadvantage relative to bigger firms with bigger budgets.

Finally, small businesses would face a Catch-22 when considering new or continued use of ADMT that helps them navigate complex and ever-changing local, state, and federal regulations (e.g., [city-specific sick leave requirements](#) and [20 different types of mandated leaves of absence](#)). Without automated tools, many small businesses will have more trouble managing compliance with various regulations — including location-specific wage laws, state and [local](#) rules governing housing applicant screening processes, and [workplace safety requirements](#). This could expose California small businesses to new risks and legal challenges.

Over 99.9 percent — 4.2 million — of California’s businesses are small businesses. Together, they employ over 7 million workers. The state recently [declared](#) them “the lifeline of the state’s economy.” They need clear, thoughtful rules that consider their needs and limitations, as well as how they use digital tools to keep their businesses thriving.

California small businesses are already struggling with extreme economic uncertainty. We urge the CPPA to more carefully consider the impact and costs of the proposed regulations on small businesses and the state, and strive for balanced regulations that reduce — rather than increase — barriers to California small businesses’ success.”

A PDF of the comment above is also attached to this email. Thank you for your consideration.

Best,



Shanthi Ramakrishna

3C Community Engagement Lead

shanthi.ramakrishna@connectedcouncil.org



Connected Commerce Council (3C)
1701 Rhode Island Avenue NW
Washington, DC 20036

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

California Privacy Protection Agency Chair Urban, Board Members, and Staff:

On behalf of the Connected Commerce Council (3C) — a nonprofit organization dedicated to promoting small businesses’ access to essential digital tools — I write to share our continued concerns about the CPPA’s proposed regulations for automated decision-making technology (ADMT). While we appreciate the revisions adopted last month, we remain concerned that the regulations will hurt California small businesses.

ADMT-powered tools significantly improve California small businesses’ efficiency — boosting their bottom lines and helping them grow and compete with larger firms. By providing affordable assistance with time-consuming tasks like staff scheduling, employee benefits selection, and fraud detection, ADMT-powered tools allow small businesses to use their limited time and money to improve their core offerings, connect with customers, and grow.

Our [research](#) shows that:

- 55% of all SMB leaders say AI tools will be critical to the success of their business during the next two years. 81% (+26%) of those already using AI in their business feel that way.
- 63% of all SMB leaders believe AI tools help “level the playing field” for businesses of all sizes. 83% (+20%) of those already using AI in their business feel that way.

Even as revised, the proposed rules would make it significantly harder for small businesses to adopt and use these valuable tools. Many firms would face costly and burdensome new obligations, including implementing complex technical upgrades to help manage notice requirements, opt-out processes, and appeals; responding to detailed information-access requests; and documenting and reporting on security policies and measures. Small businesses don’t have in-house lawyers or compliance teams. To follow the rules, they’d need to hire expensive

consultants they can't afford, or devote staff time they can't spare. Some would likely abandon key efficiency-enhancing tools — hurting their business — to reduce legal risk. But because many ADMT functions are embedded in third-party software (e.g., retailers use [financial service](#) firms' software to offer customers “buy now pay later” options), even the most scrupulous businesses could find themselves in unwitting noncompliance with the rules.

In addition, firms that provide ADMT-powered tools to small businesses would be forced to redesign their products to comply with the regulations, likely raising development costs. Those costs would almost certainly be passed on to small businesses — making it harder for them to access and benefit from the tools, and putting them at a competitive disadvantage relative to bigger firms with bigger budgets.

Finally, small businesses would face a Catch-22 when considering new or continued use of ADMT that helps them navigate complex and ever-changing local, state, and federal regulations (e.g., [city-specific sick leave requirements](#) and [20 different types of mandated leaves of absence](#)). Without automated tools, many small businesses will have more trouble managing compliance with various regulations — including location-specific wage laws, state and [local](#) rules governing housing applicant screening processes, and [workplace safety requirements](#). This could expose California small businesses to new risks and legal challenges.

Over 99.9 percent — 4.2 million — of California's businesses are small businesses. Together, they employ over 7 million workers. The state recently [declared](#) them “the lifeline of the state's economy.” They need clear, thoughtful rules that consider their needs and limitations, as well as how they use digital tools to keep their businesses thriving.

California small businesses are already struggling with extreme economic uncertainty. We urge the CPPA to more carefully consider the impact and costs of the proposed regulations on small businesses and the state, and strive for balanced regulations that reduce — rather than increase — barriers to California small businesses' success.

Thank you for considering these comments.

Sincerely,

A black rectangular box redacting the signature of Rob Retzlaff.

Rob Retzlaff
Executive Director, Connected Commerce Council

Grenda, Rianna@CPPA

From: Kris Quigley <kquigley@cdiaonline.org>
Sent: Monday, June 2, 2025 4:09 PM
To: Regulations@CPPA
Subject: CCPA Updates Cybersecurity, Audits, Risk Assessments, ADMT, and Insurance Companies
Attachments: Final Comments CPPA ADMT June 2 2025.pdf

This Message Is From an Untrusted Sender

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

Report Suspicious

Kris Quigley
Consumer Data Industry Association
Director, Government Relations
kquigley@cdiaonline.org
c: [REDACTED]



Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905
P 202 371 0910 CDIAONLINE.ORG

California Privacy Protection Agency
Attn: Regulations Coordinator
2101 Arena Blvd.
Sacramento, CA 95834

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

The Consumer Data Industry Association (CDIA) appreciates the opportunity to comment on the rulemaking for the California Consumer Privacy Act (CCPA) through the California Privacy Protection Agency (CPPA).

CDIA is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk.

Through data and analytics, CDIA members empower economic opportunities all over the world, helping ensure fair and safe transactions for consumers, facilitating competition, and expanding consumer access to financial and other products suited to their unique requirements. They help people meet their credit needs; they ease the mortgage and employment processes; they help prevent fraud; they help people acquire homes, jobs, and cars with quiet efficiency. CDIA members locate crime victims and fugitives; they reunite consumers with lost financial assets; they keep workplaces and apartment buildings safe. CDIA member products are used in more than nine billion transactions each year.

Definition of ADMT

CDIA appreciates the revision to narrow the scope of ADMT to “any technology that processes personal information and uses computation to replace human decisionmaking or substantially replace human decisionmaking.” This updated definition is an improvement and more clearly targets technologies that operate without human oversight.

Further, we support the clarification that “substantially replace human decisionmaking” refers to instances in which a business uses the output of ADMT to make a decision without any human involvement. This refinement helps to better focus regulatory obligations on higher-risk technologies and aligns with the intent to safeguard consumers in cases where meaningful human oversight is absent.



Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905
P 202 371 0910 CDIAONLINE.ORG

Recognition of Existing CCPA Exemptions

It is important to ensure that the draft regulations reflect the exemptions under Civil Code section 1798.145. While it is our belief that exemptions under §1798.145 remain applicable in the absence of contrary language, we believe explicit clarification is warranted. This is important with respect to ADMT-related opt-out rights, access rights, training, and profiling activities, as any ambiguity could create compliance challenges and disrupt longstanding practices built around the current statutory framework.

As discussed below, we also specifically request confirmation that the commercial credit reporting exemption under §1798.145 applies in the context of ADMT-related opt-out rights.

Pre-Use Requirements

Concerns remain that the draft pre-use requirements were complex and exceeded the statutory mandates of the CCPA. We appreciate the revisions which significantly streamline these obligations.

The removal of certain overly detailed sub-requirements, such as the need to disclose specific training use cases, categories of personal information processed for training, and the logic behind the ADMT output, is a welcome improvement. These changes reduce operational burden while still ensuring appropriate accountability.

While our preference remains for the complete removal of the pre-use requirement or alignment with more general disclosures, we can support the current language. In particular, the ability to rely on the trade secret exemption will help protect proprietary algorithms and models.

Commercial Credit

CDIA has concerns regarding the scope of the regulations—particularly as they relate to Automated Decision-Making Technology (ADMT) used in making significant decisions—and the potential ramifications for commercial credit reporting.

As regulations developed under the California Consumer Privacy Act (CCPA), the proposed ADMT rules are inherently subject to the statutory exemptions established by the CCPA, including those outlined in Section 1798.145(d)(2), which reference activities governed by the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.). While the proposed regulations are bound by these legislative exemptions, they currently lack clarity on how narrower, consumer-specific exemptions—such as opt-out rights—interact with the new ADMT provisions.



Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905
P 202 371 0910 CDIAONLINE.ORG

For instance, it is not clear whether ADMT-related rights, like the right to opt out, would extend to commercial credit reporting activities when the data in question might technically meet the definition of “personal information” under the CCPA.

This ambiguity is particularly relevant in situations where lenders rely on commercial credit reports to make financing decisions. These reports often contain data that can be considered personal information, such as the identities of business owners, guarantors, directors, or other key personnel associated with the business. Without further clarification, such information could be misclassified as subject to the ADMT opt-out, potentially requiring its exclusion from critical systems. This could lead to major disruptions in the credit evaluation process and introduce significant uncertainty for businesses and service providers alike.

The CCPA already addresses this issue by exempting certain categories of personal information, specifically that which is used solely in connection with a business and not an individual consumer, from rights such as deletion, opt-out of sale, and opt-out of sharing. This exemption is essential to preserving the availability of accurate and reliable data for commercial credit reporting, which in turn supports the flow of credit to businesses throughout California. These protections are especially important for small and mid-sized enterprises that depend on access to credit to expand operations, invest in innovation, and reach new markets.

However, the ADMT framework, while not granting rights to opt out of sales or sharing, does introduce a right to opt out of ADMT used in significant decision-making. As drafted, the proposed regulations do not clearly reflect the CCPA’s commercial credit reporting exemption.

To remedy this, we recommend adding the following language to the proposed regulations to clarify that “significant decisions” do not include commercial credit reporting activities as outlined in the CCPA:

Proposed Amendment:

(ddd)(7): A significant decision does not include the purposes set forth in Section 1798.145(o).

Omitting this clarification could negatively affect small businesses across California. Without access to data that confirms a business’s management and credit history, companies may face new challenges in securing financing for product development, market expansion, and other strategic initiatives.

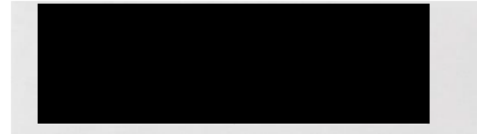


Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905
P 202 371 0910 CDIAONLINE.ORG

In conclusion, CDIA believes the May 2025 draft represents meaningful progress. We respectfully request that the final regulations explicitly reaffirm the application of statutory exemptions under §1798.145 to ADMT-related activities, including opt-outs, and clarify the continued applicability of the commercial credit reporting exemption.

Thank you for your time and consideration. Should you have questions please contact me at kquigley@cdiaonline.org.

Best,



Kris Quigley
Director, Government Relations

Grenda, Rianna@CPPA

From: Grace Gedye <grace.gedye@consumer.org>
Sent: Monday, June 2, 2025 2:05 PM
To: Regulations@CPPA
Subject: Consumer Reports' Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: Consumer Reports June 2 ADMT Risk Assessment Comment.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 CPPA team,

I hope this note finds you well. I'm respectfully submitting Consumer Reports' comments on the May draft of the Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking Technology (ADMT) draft rules, attached here.

Sincerely,
Grace

--

Grace Gedye
AI Policy Analyst
m [REDACTED]
Pronouns: she, her, hers
[CR.org](https://www.consumerreports.org)



This e-mail message is intended only for the designated recipient(s) named above. The information contained in this e-mail and any attachments may be confidential or legally privileged. If you are not the intended recipient, you may not review, retain, copy, redistribute or use this e-mail or any attachment for any purpose, or disclose all or any part of its contents. If you have received this e-mail in error, please immediately notify the sender by reply e-mail and permanently delete this e-mail and any attachments from your computer system.

Comments of Consumer Reports
In Response to the
California Privacy Protection Agency's
Invitation for Comment on
Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated
Decisionmaking Technology (ADMT), and Insurance Companies

By
Grace Gedye, Policy Analyst
Matt Schwartz, Policy Analyst
Justin Brookman, Director of Technology Policy
May 30, 2025



Consumer Reports¹ appreciates the continued work of the California Privacy Protection Agency (CPPA) staff and board to implement the California Consumer Privacy Act and safeguard the privacy rights of Californians. The rulemaking process around automated decisionmaking technology (ADMT) and risk assessments is both timely and essential; these systems increasingly influence access to critical opportunities, like admissions into school,² applicant selection for rental units³ or job opportunities,⁴ work scheduling,⁵ and more.

In previous comments,⁶ we expressed concern that the scope of the proposed ADMT regulations was too limited and that the ambiguity in terms like “key factor”—combined with businesses’ strong incentive to interpret the rules as narrowly as possible—would result in companies withholding information on ADMT that shape consumers’ life opportunities. Unfortunately, the May draft narrows the scope much further, making clear that many ADMT recommendation tools are not covered. Several other revisions remove due diligence requirements for companies and provisions that would make it easier for consumers to exercise their rights.

This direction is particularly concerning given the sustained engagement from privacy, labor, and other civil society advocates, many of whom have offered specific recommendations to strengthen transparency and accountability in the use of ADMT. The May draft—if adopted—will result in fewer Californians gaining insight into how their personal data is being processed in consequential decisions, as compared to earlier drafts.

¹ Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers’ interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

² Liam Knox, *Inside Higher Education*, “Admissions Offices Deploy AI,” October 9, 2023 <https://www.insidehighered.com/news/admissions/traditional-age/2023/10/09/admissions-offices-turn-ai-application-reviews>

³ Patrick Sisson, *Bloomberg*, “For Tenants, AI-Powered Screening Can Be a New Barrier to Housing,” September 11, 2024, <https://www.bloomberg.com/news/features/2024-09-11/ai-powered-tenant-screening-tech-worries-fair-housing-advocates>

⁴ Hilke Schellman, *The Algorithm*, January 2024, Hachette Books

⁵ Ben Rand, *Harvard Business School - Working Knowledge*, “Bad Data, Bad Results: When AI Struggles to Create Staff Schedules,” February 27th 2025, <https://www.library.hbs.edu/working-knowledge/bad-data-bad-results-when-ai-struggles-to-create-staff-schedules>

⁶ Grace Gedy, Stacey Higgenbotham, Matt Schwartz, Justin Brookman, “Comments of Consumer Reports In Response to the California Privacy Protection Agency’s Invitation for Comment on Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies,” February 19th, 2025. <https://advocacy.consumerreports.org/research/consumer-reports-comments-on-california-privacy-protection-agency-draft-rules-regarding-cybersecurity-audits-risk-assessments-and-automated-decision-making-technology/>

There are some improvements in this draft that are worth noting. We are pleased to see that Pre-Use Notices must now inform consumers how decisions will be made if they choose to opt out of ADMT use⁷—an improvement we specifically called for in our last round of comments.⁸ This will provide consumers with information they need in order to weigh the benefits and drawbacks of opting out. We also appreciate the clarification in the Request to Access provisions that businesses must disclose the outcome of any significant decision;⁹ this is essential information for affected individuals and it was previously ambiguous.

Nonetheless, the overall contraction in scope and the rollback of key protections is disappointing. As CR and other organizations such as the American Civil Liberties Union of Northern California have articulated in previous comments, these rules are well within the CPPA’s authority.¹⁰ The remainder of our comments outlines our specific concerns with the May draft of the automated decisionmaking technology and risk assessment regulations, as well as suggestions for how the CPPA might better align the final rule with the statute’s consumer protection goals. They include:

- Revised definition of “automated decisionmaking technology” leaves many Californians unprotected
- Restore requirements for businesses to assess whether their physical or biological profiling is actually working, and whether it is discriminating.
- Remove trade secret protections for Pre-Use Notice and Right to Access
- Restore opt-out of behavioral advertising
- Restore reminder of Right to Access after adverse decisions

⁷ May draft, Section 7220. Pre-use Notice Requirements, (c)(5)

⁸ Grace Gedy, Stacey Higgenbotham, Matt Schwartz, Justin Brookman, “Comments of Consumer Reports In Response to the California Privacy Protection Agency’s Invitation for Comment on Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies,” February 19th, 2025, See “Require that businesses explain to consumers what happens if they choose to opt-out when presenting them with the right to opt-out”

⁹ May draft, Section 7222 (b)(3)

¹⁰ Grace Gedy, Stacey Higgenbotham, Matt Schwartz, Justin Brookman, “Comments of Consumer Reports In Response to the California Privacy Protection Agency’s Invitation for Comment on Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies,” February 19th, 2025,

<https://advocacy.consumerreports.org/research/consumer-reports-comments-on-california-privacy-protection-agency-draft-rules-regarding-cybersecurity-audits-risk-assessments-and-automated-decision-making-technology/> and

ACLU California Action “Re: Comments on Proposed Risk Assessments and Automated Decisionmaking Technology Regulations” February 19, 2025,

<https://www.aclunc.org/sites/default/files/2025-02-19%20ACLU%20CA%20Action%20EPIC%20EFF%20CFA%20PRC%20CPPA%20Comments.pdf> and Electronic Privacy Information Center and Consumer Federation of America,

“Comments of the Electronic Privacy Information Center and the Consumer Federation of America to the California Privacy Protection Agency on Proposed Rulemaking Regarding Cybersecurity, Risk Assessments, and Automated Decisionmaking Technology” February 19, 2025

<https://epic.org/documents/comments-to-the-cppa-on-proposed-regulations-regarding-cybersecurity-risk-assessments-and-admts/>

- Restore prohibition on processing if risks outweigh benefits and clarify that CPPA has the authority to contest business' assessments of cost-benefit tradeoffs

Revised definition of “automated decisionmaking technology” leaves many Californians unprotected

The May draft’s revision to the definition of “automated decisionmaking technology” dramatically alters the scope of the regulations, leaving many Californians completely in the dark when ADMT play an influential role in whether they land a job, receive a home loan, are suspended from school, are approved for a rental unit, and more. Unfortunately, the minimal human oversight established in the May draft is not a meaningful substitute for transparency for impacted Californians.¹¹ One reason is automation bias; research suggests that humans tend to view automated systems as authoritative and trustworthy and are inclined to defer to a system’s recommendations even when they suspect it is malfunctioning.¹² This bias limits the efficacy of human review for catching and addressing errors.

A second reason is that companies have an incentive to speed through review processes. This has been documented in the insurance industry, where laws and regulations in many states require doctors to review claims before an insurer rejects a claim for a medical reason.¹³ Doctors are supposed to examine patient records and use their expertise in the decision. Yet, an investigation by ProPublica found that health insurer Cigna set up a system that enabled doctors to reject claims without even opening patient files, and documents indicate that doctors were spending an average of 1.2 seconds on each case.¹⁴ A second investigation by ProPublica found that Cigna was tracking its medical directors’ productivity on a dashboard, and at least one doctor was warned that she would be fired if she didn’t work faster.¹⁵

The new definition of ADMT would exempt recommendation systems that are highly influential in consequential decisions. For example, many companies that use AI hiring systems do not use them autonomously; they may use them to flag the most promising candidates out of thousands of resumes, or to analyze hours of virtual job interviews, and then have a human hiring manager look at the recommendations to make a final decision. Investigations by journalists suggest that

¹¹ May draft, Section 7001, (e)(1)(A-C)

¹² See, e.g., Danielle Keats Citron, Washington University Law Review, ‘Technological Due Process,’ 2008 at 1271–72; https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1166&context=law_lawreview

¹³ Patrick Rucker, The Capitol Forum, and Maya Miller, David Armstrong, ProPublica, “How Cigna Saves Millions by Having Its Doctors Reject Claims Without Reading Them” March 25, 2023, <https://www.propublica.org/article/cigna-pxdx-medical-health-insurance-rejection-claims>

¹⁴ *ibid*

¹⁵ Patrick Rucker, The Capitol Forum, and David Armstrong, ProPublica, “A Doctor at Cigna Said Her Bosses Pressured Her to Review Patients’ Cases Too Quickly. Cigna Threatened to Fire Her.” April 19, 2024 <https://www.propublica.org/article/cigna-medical-director-doctor-patient-preapproval-denials-insurance>

these systems can be alarmingly off base, or can discriminate based on protected status. For example, investigative journalists found that AI hiring startup Retorio’s assessment of an applicant varied when he or she added glasses, a headscarf, or items like a painting or bookshelf in the background.¹⁶ Another AI hiring assessment, Curious Thing, provided high scores in English proficiency even when questions were answered exclusively in German.¹⁷ The use of systems like these by human decisionmakers may have been covered by the April draft rules; they likely would not be under the May draft.

The April draft rules also had several provisions which might have prompted appropriate scrutiny. For example, Section 7201 (“Requirement for Physical or Biological Identification or Profiling”) likely would have required a company using Retorio’s application to assess whether the software was working as intended, and whether it was discriminating—an assessment that might have revealed the issues the journalists found. That section was cut entirely from the May 1st draft. The April draft also prohibited companies from processing data when the risks outweighed the benefits; that provision might have applied to these flawed systems, but it has now been weakened. Lastly, the information contained in the Pre-use Notice and Request for Access might have prompted Californians impacted by these flawed systems to reach out to the hiring entity or file a complaint with the CPPA or the Attorney General. Now, so long as companies using systems like Retorio and Curious Thing apply at least some human review, Californians won’t receive those disclosures. Taken together, the previous draft provided several important junctures at which flawed systems would come under scrutiny; the current draft removes many of these checks.

Restore requirements for businesses to assess whether their physical or biological profiling is actually working, and whether it is discriminating.

The May draft completely cuts Section 7201, “Requirements for Physical or Biological Identification or Profiling.” Previously, businesses that were using physical or biological identification or profiling for a significant decision or for extensive profiling would have had to evaluate the profiling to ensure it works as intended and does not unlawfully discriminate, and implement policies to ensure that both of those things happen. This was an important requirement; inaccurate or discriminatory biometric profiling systems are a documented problem. For example, in 2023 the Federal Trade Commission banned Rite Aid from using facial recognition for in-store surveillance because it failed to implement reasonable procedures to reduce harm.¹⁸ About the decision, the FTC wrote: “Employees, acting on false positive alerts,

¹⁶ Elisa Harlan, Oliver Schnuck, BR24, “Objective or Biased” February 16th 2021
<https://interaktiv.br.de/ki-bewerbung/en/>

¹⁷ Sheridan Wall, Hilke Schellmann, MIT Technology Review, “We tested AI interview tools. Here’s what we found.” July 7, 2021
<https://www.technologyreview.com/2021/07/07/1027916/we-tested-ai-interview-tools/>

¹⁸ Federal Trade Commission, “Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards” December 19, 2023,

followed consumers around its stores, searched them, ordered them to leave, called the police to confront or remove consumers, and publicly accused them, sometimes in front of friends or family, of shoplifting or other wrongdoing, according to the complaint.”¹⁹ Fourteen Uber couriers shared evidence with *Wired* in 2021 that Uber’s facial identification software, used to confirm a courier’s identity, failed to recognise their faces.²⁰ Some of these drivers were threatened with termination, or were fired after their selfies failed the company’s “Real Time ID Check.”²¹

The previous requirements to evaluate and implement practices to prevent unintended consequences and unlawful discrimination were reasonable and not overly burdensome. They should be restored.

Remove trade secret protections for Pre-Use Notice and Right to Access

The May draft regulations also added trade secret and security-related exemptions to the Pre-Use Notice and the Right to Access. The trade secret exemptions in particular threaten to completely undercut the utility of the Pre-Use Notices and Right to Access—two of the most important provisions for consumers who want to understand how their data is being used to make major decisions about them.

The only technology-specific disclosures required in the Pre-Use Notice are 1) how the automated decisionmaking technology processes personal information to make a significant decision; 2) the categories of personal information that affect the output; and 3) the type of output the system generates.²² This is essential information for consumers, and sharing it does not require a company to disclose its code, its weights, or non-personal data the system relies on. Indeed, one would expect these basic categories of information to be included in marketing pitches to clients. What Fortune 500 company is going to buy a hiring recommendation algorithm without asking what information about the candidates the recommendation is based on, or whether the output is a score from 1-10, a qualitative summary of the applicant’s strengths and weaknesses, or something else?

These trade secret exemptions are ripe for abuse, particularly by companies that are using information of dubious validity or quality and who have a strong incentive to keep those shortcomings secret. Theranos founder Elizabeth Holmes famously invoked trade secret protections as the rationale for withholding from investors and journalists the fact that her

<https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without>

¹⁹ *ibid*

²⁰ Andrew Kersley, *Wired*, “Couriers say Uber’s ‘racist’ facial identification tech got them fired” March 1, 2021 <https://www.wired.com/story/uber-eats-couriers-facial-recognition/>

²¹ *ibid*

²² Section 7220 (c)(5)(A-B)

company was not using proprietary “finger prick” blood testing devices and was instead using equipment purchased from other companies.²³

The case that either of these notices would require a company to disclose their trade secrets is weak. Moreover, the public interest rationale for these disclosures, we believe, outweighs these weak trade secret claims. We suggest striking the trade secret exemptions from the Pre-Use Notice and Right to Access.

Restore opt-out of behavioral advertising

The May draft regulations removed proposed privacy protections for behavioral advertising based on first party data. This runs counter to the text of the CCPA and should be reversed: California consumers should have the ability to turn off first-party ad targeting if they wish.

The CCPA directs the CPPA to issue “regulations governing access and opt-out rights with respect to businesses’ use of automated decision-making technology, including profiling”²⁴ Profiling itself is defined broadly to include “any 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 performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements”²⁵ Clearly, first-party ad targeting is logically included within that definition, and the CPPA should follow the statute’s directive to give consumers a way to opt-out of such profiling.

The CCPA already provides a mechanism for consumers to opt out of *cross-context* targeted advertising, including through the use of universal opt-out mechanisms such as the Global Privacy Control. However, it does not explicitly provide for an opt-out for first-party targeting, other than the general directive to the CPPA to create opt-out rights for profiling. While first-party targeting should not be subject to a global opt-out as consumers are more likely to have varying preferences for personalization for individual companies, they still should have the ability to turn off personalization of offers if they so desire. Companies already offer individuals tools to manage first-party advertising as required by laws such as CAN-SPAM and the TCPA. The CPPA should further require those companies to let consumers turn off first-party ad behavioral profiling.

Restore reminder of Right to Access after adverse decisions

²³ James Pooley, *IP Watchdog*, “Lessons From Theranos and the Trade Secret Defense” January 30, 2022, <https://ipwatchdog.com/2022/01/30/lessons-theranos-trade-secret-defense/> and Sara Randazzo, *Wall Street Journal*, “Prosecutor Takes Aim at Holmes’s Trade-Secret Defense” December 16, 2021 <https://www.wsj.com/livecoverage/elizabeth-holmes-trial-theranos/card/prosecutor-takes-aim-at-holmes-s-trade-secret-defense-tQjRekJB1f5w9UUJM6PZ>

²⁴ Cal. Civ. Code § 1798.185(a)(16).

²⁵ Cal. Civ. Code § 1798.140(z).

The April draft included provision (k) in Section 7222 “Requests to Access ADMT” that required companies to remind consumers of their Right to Access additional information after an ADMT is used in an adverse significant decision.²⁶ (We refer to this as the “reminder notice”). This was an important protection; often consumers are not aware of their privacy rights, and therefore do not use them.²⁷ The reminder notice would have prompted consumers to consider their right to receive more information precisely when they would be most interested in using it—in the immediate aftermath of being denied a rental unit or a home loan, or being terminated or demoted at work. Importantly, this reminder had to be delivered “as soon as feasibly possible but no later than 15 business days from the date of the adverse significant decision.”²⁸ If a consumer was denied a home or a loan, or was fired based on faulty information, this reminder notice might cause them to request information that would reveal the problem and enable them to talk to the landlord, bank, or employer about reevaluating the decision before the harms, such as lost wages, had accrued.

This provision is not particularly burdensome for businesses. The reminder notice could be automated, requiring limited ongoing costs once a process is set up. Additionally, these notices are not individualized; the same notice could be used for many consumers.

In our February 19th comments on this rulemaking, Consumer Reports advocated for strengthening this provision and making it easier for consumers to use.²⁹ We wrote:

The pre-use notice paired with a post-decision explanation (“right to access”) are two of the most critical provisions of Article 11. The additional information consumers will receive as a result of these provisions will help consumers understand how their personal data is being used to make decisions that impact their lives, exercise their right to appeal if necessary, and in some cases, may enable them to exercise rights under existing laws,

²⁶ April draft, Section 7222 (k)

²⁷ Consumer Reports Survey Research Department, “Consumer Reports American Experiences Survey: A Nationally Representative Multi-Mode Survey, September 2024 Omnibus Results.” https://article.images.consumerreports.org/image/upload/v1728423752/prod/content/dam/surveys/Consumer_Report_s_AES_September_2024.pdf The survey asked the following question: “Some states have laws that regulate how companies can collect, store, share, and use people’s personal data, like their shopping habits, internet history, and personal information like age, race/ethnicity, and where they live. To the best of your knowledge, does your state have a law like that?” 54% said “I don’t know if there’s a law like that at all” and 25% said “I think there is a law like that, but I don’t know if it’s state or federal.”

²⁸ April draft, Section 7222 (k)

²⁹ Grace Gedy, Stacey Higgenbotham, Matt Schwartz, Justin Brookman, “Comments of Consumer Reports In Response to the California Privacy Protection Agency’s Invitation for Comment on Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies,” February 19th, 2025. See “Send post-decision explanations to consumers by default; ensure explanations are sufficiently detailed and put in context” https://advocacy.consumerreports.org/wp-content/uploads/2025/02/CR-comments-re_CCPA-cyber-risk-assessment-ADMT-rulemaking.pdf

such as civil rights laws, consumer protection laws, and labor laws. For these disclosures to live up to their promise, they must be easy for consumers to access, detailed, and easy for them to understand.

Currently, in order for a consumer to receive information about how an adverse significant decision was made about them, the regulations require consumers to take a proactive step to exercise their right to “access.” Many consumers will not take this step even when doing so may benefit them; they may not see the additional notice required under 7222(k); consumers may not understand the potential upside of receiving the information provided by their access right, and therefore may not choose to spend time requesting it. We recommend that instead of requiring consumers to take a proactive step when an adverse decision is made about them, businesses should instead be required to provide the information to consumers by default via their typical means of communicating with consumers.

Instead of lightening the burden on consumers as we suggested, the CPPA has moved in the opposite direction, removing the reminder notice altogether making it less likely that consumers will utilize this right. We stand by the recommendation in our February 19th comment. If the CPPA does not adopt that recommendation, it should restore the reminder notice at the very least.

Risk Assessments

Restore prohibition on processing if risks outweigh benefits and clarify that CPPA has the authority to contest businesses’ assessments of cost-benefit tradeoffs

Another disappointing change made in the May draft was to weaken the prohibition on processing consumers’ personal data if the risks of doing so outweigh the benefits. The April draft contained a clear prohibition in Section 7154; the May draft revised that prohibition to be a statement that “The goal of a risk assessment is restricting or prohibiting the processing of personal information . . .” when the risks outweigh the benefits. This change should be reversed for several reasons. The first is that the new text is ambiguous; If a business reaches the conclusion that the risks of the processing outweigh the benefits, do they have a legal obligation to do anything at all? It is unclear—especially in the context of the regulatory history on this particular provision.

This specific revision from a clear prohibition to a goal statement also does not seem to fulfill the requirement laid out in the CPRA. Section 1798.185(a)(15)(B) specifically instructs the CPPA to issue regulations requiring companies whose data processing presents a significant risk to privacy or security “to submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information . . . 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.” That goal was served by the prohibition in the April draft. The May draft, however, does not fulfill this goal, it merely restates it.

We recommend that this provision is modified not only to make clear that businesses are prohibited from processing data when the risks outweigh the benefits, but to also make clear that the CPPA has the formal ability to challenge businesses' assessments of the tradeoffs between the benefits of their processing activities and the harms, as we suggested in our February comments.³⁰ Businesses will have a strong incentive to downplay risks if they believe there is no chance their analysis will be questioned.

We propose the following language, based on the statutory damages provisions in Section 1798.155(a), creating an explicit mechanism for the CPPA to question and take action against deficient risk assessments:

Upon review of a business’s Risk Assessment, if the Agency has a cause to conclude that the benefits of the processing do not outweigh the costs as required by statute, the Agency may require additional documentation or evidence from the business. If the Agency determines, after reviewing any further materials as necessary, that there is probable cause for believing that the benefits of the processing do not outweigh the costs in violation of the statute, the Agency may hold a hearing pursuant to Section 1798.199.55(a) to determine if a violation has occurred. If the Agency so determines that a violation has occurred, it may issue an order requiring the violator to restrict the processing to address such costs or prohibiting the business from such processing.

³⁰ Grace Gedy, Stacey Higgenbotham, Matt Schwartz, Justin Brookman, “Comments of Consumer Reports In Response to the California Privacy Protection Agency’s Invitation for Comment on Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies,” February 19th, 2025.
https://advocacy.consumerreports.org/wp-content/uploads/2025/02/CR-comments-re_CPPA-cyber-risk-assessment-ADMT-rulemaking.pdf

Grenda, Rianna@CPPA

From: Karen Kaya <karen.kaya@crowdstrike.com>
Sent: Wednesday, May 21, 2025 11:15 AM
To: Regulations@CPPA
Cc: Elizabeth Guillot
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: CrowdStrike Comment on CA CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations.pdf

This Message Is From an External Sender

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

Report Suspicious

California Privacy Protection Agency:

Attached please find CrowdStrike's Public Comment on the Modified Text of CCPA Updates, Cyber, Risk, ADMT and Insurance Regulations.

Regards,

Karen Kaya

Senior Manager, Public Policy
CrowdStrike, Inc.
karen.kaya@crowdstrike.com
<http://www.crowdstrike.com>



REQUEST FOR COMMENT ON MODIFIED TEXT OF CCPA UPDATES, CYBER, RISK, ADMT, AND INSURANCE REGULATIONS

May 21, 2025

I. INTRODUCTION

In response to California Privacy Protection Agency's (CPPA) modified text of CCPA Cyber, Risk, ADMT, and Insurance regulations (modified regulation) CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

CrowdStrike appreciates the CPPA's continued engagement with stakeholders and the opportunity to provide comments on the modified regulation. We continue to support the proposed regulation's goal of better protecting California's businesses and citizens from cybersecurity threats. Incentivizing the adoption of effective cybersecurity practices and technologies is paramount to achieving the CPPA's goal of protecting citizen's data.

CrowdStrike previously commented on the proposed regulation, and we've reemphasized certain points in this response.¹ We do not have feedback on every aspect of the modified regulation, but we do want to offer several points that may be of value to the CPPA.

¹ Request for Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations, CrowdStrike, February 19, 2025.

<https://www.crowdstrike.com/content/dam/crowdstrike/marketing/en-us/documents/pdfs/legal/CA%20Cybersecurity%20Audits.%20Risk%20Assessments.%20and%20AI%20Comments.pdf>



A. Cybersecurity Audits

Audits have significant limitations in driving cybersecurity outcomes. They are a useful tool for an organization to capture a snapshot of the existence of cybersecurity plans, strategies, or controls. But ultimately audit results are only reflective of a point in time and cannot reflect a real-time measure of the state of an organization's security posture. With this in mind, we would caution organizations against being overly reliant on the results.

Many of the practices and tools the CPPA has outlined for organizations to check for in an audit represent many of today's cybersecurity best practices; however, we are disappointed to see that Zero Trust was removed. As noted previously by the CPPA, closely related to identity protection is Zero Trust Architecture (ZTA), which eliminates transitive trust and radically reduces lateral movement and privilege escalation during a compromise. This constrains threat actors' ability to achieve actions on objective and provides additional opportunities for defenders to detect threats. ZTA is an important adjunct to multifactor authentication (MFA)-based guidance, and other baseline identity measures, because it can stop attacks even if legitimate credentials are compromised and MFA is bypassed. Therefore, it is a constructive element of the proposed regulation and we urge CPPA to consider including it in the final version of this regulation.

B. Risk Assessments

Risk assessments are distinct from audits and should not be standards-driven. The fundamental question of a risk assessment is "how effectively does the security program address the cyber risks the organization faces?" Flexible frameworks are ideal for this type of evaluation as risk assessments need to be tailored for the organization completing it. The best risk assessments should combine the types of security measures but place them in an operational context - both in terms of what threat actors are likely to exploit and what defenders can realistically accomplish.

Risk assessments are an internal exercise, often done under client privilege with a third-party firm, and businesses should not be required to submit risk assessments to the CPPA. We appreciate the modifications in the modified regulation to reflect this.

C. Automated Decisionmaking



We continue to support the inclusion of a security carveout in the regulations for automated decisionmaking technologies. This is central to maintaining uninterrupted use of best-in-class cybersecurity capabilities under the regulation.

The use of Artificial Intelligence (AI) to detect cyber threats is an enormous advantage. Today, security teams demand contextual awareness and visibility from across their entire environments, including within cloud and ephemeral environments, and AI can help defenders process this data and make detections more actionable. AI is the best tool defenders have to identify and prevent zero-day attacks and malware-free attacks, because AI can defeat novel threats based on behavior cues rather than known signatures. Leveraging these technologies is essential to meeting constantly-evolving threats.

III. CONCLUSION

As the CPPA moves forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any final regulation includes a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.



Learn more: <https://www.crowdstrike.com/>.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E

VP & Counsel, Privacy and Cyber Policy

Elizabeth Guillot

Senior Manager, Public Policy

Email: policy@crowdstrike.com

©2025 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are trademarks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.

Grenda, Rianna@CPPA

From: Avonne Bell <ABell@ctia.org>
Sent: Monday, June 2, 2025 2:17 PM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: CTIA Comments on Modifications to CPPA Proposed Regulations - 06.02.25.pdf

This Message May Be Unsafe

Please verify with the sender offline and avoid replying with sensitive information, clicking links, or downloading attachments.

Report Suspicious

To the California Privacy Protection Agency,

Please find attached the comments of CTIA in response to the Agency's Notice of Modifications to Proposed Rulemaking regarding CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations.

Thank you,

ctia

Avonne Bell

Director, Connected Life

1400 16th Street, NW

Washington, DC 20036

202-736-3246 (office)

[REDACTED] (mobile)

abell@ctia.org

**Before the
California Privacy Protection Agency**

In the Matter of)	
)	
Proposed Regulations on CCPA Updates,)	Request for Public Comments
Cybersecurity Audits, Risk Assessments,)	
Automated Decisionmaking Technology,)	
And Insurance Companies)	

COMMENTS OF CTIA

Umair Javed
Senior Vice President and General Counsel

Gerard Keegan
Vice President, State Legislative Affairs

David Valdez
Vice President, Privacy and Cybersecurity

Avonne S. Bell
Director, Connected Life

Jake Lestock
Director, State Legislative Affairs

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

June 2, 2025

TABLE OF CONTENTS

I.	Introduction.....	1
II.	The Regulations Should Be Revised to Align with Global Frameworks and Other State Regimes.	3
A.	The risk assessment requirement should be interoperable with other global frameworks and other state regimes, and it should embody flexibility rather than prescriptiveness.	3
B.	Entities should not be subject to an annual cybersecurity audit requirement, consistent with globally recognized frameworks.	5
III.	The Agency Should Not Require the Submission of Sensitive Information in Risk Assessments and Should Permit Companies to Maintain Confidentiality Where Submission Is Necessary.....	6
IV.	The Agency Should Establish Compliance Deadlines for Amendments and Clarify Deadlines for Risk Assessment Requirements.	8
A.	Compliance deadlines should be established for the amended regulations.....	8
B.	The compliance deadlines for risk assessments should be clarified and harmonized.	9
V.	The Exemption Allowing ADMT Use for Security, Fraud Prevention, and Safety Without a Consumer Opt-Out Should Be Restored.	10
VI.	Conclusion.	11

**Before the
California Privacy Protection Agency**

In the Matter of)	
)	
Proposed Regulations on CCPA Updates,)	Request for Public Comments
Cybersecurity Audits, Risk Assessments,)	
Automated Decisionmaking Technology,)	
And Insurance Companies)	

COMMENTS OF CTIA

I. INTRODUCTION.

CTIA¹ appreciates the opportunity to comment in this important rulemaking and commends the California Privacy Protection Agency’s (“CPPA” or “Agency”) efforts to evaluate closely its proposed regulations regarding cybersecurity audits, risk assessments, and automated decisionmaking technology (“ADMT”).

The wireless industry prioritizes privacy protection and data security—successful communications services depend on consumer trust. Stakeholders in the wireless industry actively protect consumers’ privacy and safeguard their data, including with robust company-based policies, commitments to voluntary codes of conduct, and compliance with applicable laws and regulations. Entities across the wireless communications ecosystem, including network operators, device manufacturers, operating system developers, and application service providers,

¹ CTIA – The Wireless Association® (“CTIA”) (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association’s members include wireless providers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. CTIA represents a broad diversity of stakeholders, and the specific positions outlined in these comments may not reflect the views of all individual members. The association also coordinates the industry’s voluntary best practices, hosts educational events that promote the wireless industry and co-produces the industry’s leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

work independently and together to develop innovative privacy and other consumer safety features that protect wireless networks and consumers.

CTIA and its members leveraged their substantial experience with these issues to provide suggestions earlier this year² on ways the Agency could refine the proposed regulations to better protect consumer privacy and advance the California Consumer Privacy Act's ("CCPA" or "Act") goals while also avoiding unnecessary regulatory burdens on businesses. The Agency has made substantial progress in the latest iteration of the proposed regulations,³ and CTIA respectfully recommends additional modest adjustments to improve clarity. Specifically, CTIA recommends that the Agency:

- Ensure that the risk assessment requirement is flexible and interoperable with other global frameworks and state requirements;
- Decline to impose an annual cybersecurity audit requirement consistent with other globally recognized frameworks;
- Not require the submission of sensitive information in risk assessments (or, at a minimum, allow companies to maintain confidentiality when the submission of certain sensitive information is necessary);
- Establish compliance deadlines for the amended regulations, and clarify and harmonize the compliance deadlines for the new risk assessment requirements; and
- Restore the exemption that clarifies that ADMT may be used for security, fraud prevention, and safety without offering a consumer opt-out.

² See Comments of CTIA (Feb. 19, 2025), <https://tinyurl.com/putfww26>.

³ See Proposed Cal. Code Regs. tit. 11, § 7001 *et seq.* (May 9, 2025), <https://tinyurl.com/9wb7e8pz> ("Proposed Regulations").

II. THE REGULATIONS SHOULD BE REVISED TO ALIGN WITH GLOBAL FRAMEWORKS AND OTHER STATE REGIMES.

A. The risk assessment requirement should be interoperable with other global frameworks and other state regimes, and it should embody flexibility rather than prescriptiveness.

The proposed regulations on risk assessments should be revised to conform with global frameworks, such as the National Institute of Standards and Technology (“NIST”) Risk Management Framework or Cybersecurity Framework (“CSF”), and they should enable companies to leverage risk assessments prepared in accordance with other state privacy laws. Harmonizing California’s regime with these requirements will allow covered entities to focus their efforts on assessing activities presenting significant risks to privacy, better protecting Californians while also facilitating compliance.

While California’s proposed regulations on risk assessments provide some flexibility to leverage existing materials (establishing that “[a] business may utilize a risk assessment that it has prepared for another purpose . . . provided that the risk assessment contains the information that must be included in, or is prepared with the outstanding information necessary for, compliance with section 7152”),⁴ they still mandate compliance with all of California’s many specific and unique requirements, even when the underlying reporting obligations are similar in scope to those required by other states. For example, as drafted, companies would only be able to use risk assessments from other states to satisfy the California requirements if they also happen to meet California’s specific requirements, which is unlikely. As proposed, companies are effectively prevented from using widely accepted risk assessment practices that conform with global frameworks or utilizing assessments that have been deemed sufficient in other states.

⁴ *Id.* § 7156(b).

Rather than compel entities to start from square one in developing a California-specific risk assessment with only speculative benefit to consumers, the regulations should permit entities to use assessments that have been prepared consistent with globally accepted frameworks or that have been used in other states with substantially similar standards (*i.e.*, they are reasonably similar in scope to California’s requirements). These frameworks are widely used by industry and reflect best practices refined over time, meaning that their requirements are robust and foster a balanced, risk-based approach to mitigating potential harms. The NIST CSF, for example, empowers organizations to focus on areas that present the highest risks, ensuring that resources are allocated appropriately.⁵

A California-specific variation on risk assessments is not essential for consumer protection. State-specific differences may even lead to consumer confusion, if consumers are not aware that privacy protections could differ across state lines. Further, state-specific variations will only cause resources to be diverted to paperwork. Commissioner Mactaggart has suggested that the Agency “provide a comprehensive list of acceptable assessments from other jurisdictions to reduce duplication and compliance costs.”⁶ CTIA agrees and urges the Agency to more closely align California’s regulations with those in other states, many of which allow companies to use risk assessments that comply with global standards.⁷

⁵ See *The NIST Cybersecurity Framework (CSF) 2.0*, NIST (2024), <https://tinyurl.com/4rze35m8><https://tinyurl.com/3fbrf5xx>; see also *NIST Cybersecurity White Papers*, <https://tinyurl.com/mh36n8mj> (last visited May 30, 2025).

⁶ Audio Transcription of Recorded Public Comment Session, CPPA Board, at 103 (Nov. 8, 2024), <https://tinyurl.com/3edj26cb>.

⁷ See, e.g., Colo. Rev. Stat. § 6-1-1309.5(4).

Additionally, as proposed, the risk assessment mandate is overly prescriptive, detailing a specific and granular list of required content.⁸ For example, a business would be required to document and report numerous operational elements of its processing, including, among other things, the sources of personal information; the approximate number of consumers whose personal information the business plans to process; and the names or categories of the service providers, contractors, or third parties to whom the business discloses or makes available the consumers' personal information.⁹ The proposed regulations also adopt a one-size-fits-all approach, failing to take into account the wide variation in business models, risk profiles, and data practices across industries and potentially leading to unnecessary reporting burdens without meaningful consumer benefit and protection. Adherence to rigid requirements and a lack of flexibility would stifle ADMT development and use and innovation in California. CTIA therefore urges the Agency to provide businesses with greater flexibility to determine and report on the topics that are relevant for the processing activity in completing risk assessments. If the Agency adopts this regulation, it should clarify that the list in Section 7152 is merely illustrative and applies only when relevant to the process at hand.

B. Entities should not be subject to an annual cybersecurity audit requirement, consistent with globally recognized frameworks.

Section 7121(b) requires businesses to complete an annual cybersecurity audit and report.¹⁰ However, an annual reporting requirement would potentially result in a waste of resources by focusing on formality over substance, failing to capture the dynamic nature of cybersecurity risks, which are evolving continuously. Audits at this static cadence may not

⁸ See Proposed Regulations § 7152(a)(3).

⁹ See *id.*

¹⁰ See *id.* § 7121(b).

account for changes in a company's operations, systems, or threat landscape. In contrast, widely recognized frameworks, like NIST's CSF, leverage intervening audits, rather than full annual audits. Intervening audits address cybersecurity issues more effectively by ensuring an interactive approach that permits continuous improvement and adaptation to risk profiles and security controls. They further ensure that organizations are designing their cybersecurity programs to address the highest priority and highest risk areas, rather than non-strategically expending resources for a full audit each year. Leveraging intervening audits and declining to impose annual audits will better serve consumers and reduce needless burdens on entities.

III. THE AGENCY SHOULD NOT REQUIRE THE SUBMISSION OF SENSITIVE INFORMATION IN RISK ASSESSMENTS AND SHOULD PERMIT COMPANIES TO MAINTAIN CONFIDENTIALITY WHERE SUBMISSION IS NECESSARY.

The Agency has proposed requiring business to provide “the approximate number of consumers whose personal information the business plans to process” in risk assessments.¹¹ This requirement should be removed from the final regulations. As an initial matter, it is unclear how this figure could be determined with real accuracy, especially for businesses planning new products where consumer usage is uncertain at the pre-launch phase. Even if this figure could be calculated, disclosing it would raise confidentiality concerns, as it involves competitively sensitive information. Businesses should not be required to submit this information.

Furthermore, the Agency should ensure the confidentiality of all risk assessment information submitted by entities. Specifically, risk assessments and other information submitted should be confidential and exempt from public disclosure. The Agency should make clear that disclosing this information does not waive attorney-client privileges or work-product

¹¹ *Id.* § 7152(a)(3)(D).

protections. These protections are consistent with practices in other states. For instance, Colorado law treats data protection assessments as confidential and exempt from public disclosure, and sharing them with the attorney general does not waive privilege protections.¹² Virginia follows a similar approach.¹³ Assessments under both laws may contain sensitive data or confidential business information, which would be exempt from disclosure under these states' regimes – California should adopt this approach as well.

In addition, the Agency proposes to require the disclosure of employee names associated with aspects of the risk assessments and related decisions.¹⁴ This requirement is overbroad because it would seem to mandate disclosing *all* employees involved in processing personal data. It would also be difficult to implement this requirement and would result in an excessive number of names being subject to disclosure. Even more critically, this requirement lacks confidentiality protections and raises serious privacy concerns. If the requirement is retained in some form, the Agency should acknowledge the risk that disclosed individuals could be targeted for their involvement or affiliation with a particular company, including for phishing or political reasons. Safeguards against public disclosure should be incorporated accordingly.

¹² See Colo. Rev. Stat. § 6-1-1309(4) (“A controller shall make the data protection assessment available to the attorney general upon request. The attorney general may evaluate the data protection assessment for compliance with the duties contained in section 6-1-1308 and with other laws, including this article 1. Data protection assessments are confidential and exempt from public inspection and copying under the ‘Colorado Open Records Act’, part 2 of article 72 of title 24. The disclosure of a data protection assessment pursuant to a request from the attorney general under this subsection (4) does not constitute a waiver of any attorney-client privilege or work-product protection that might otherwise exist with respect to the assessment and any information contained in the assessment.”).

¹³ See Va. Code Ann. § 59.1-580(C) (establishing that data protection assessments are confidential and exempt from public inspection, and sharing them with the attorney general pursuant to a request does not waive attorney-client privilege or work-product protection).

¹⁴ See Proposed Regulations § 7152(a)(9).

IV. THE AGENCY SHOULD ESTABLISH COMPLIANCE DEADLINES FOR AMENDMENTS AND CLARIFY DEADLINES FOR RISK ASSESSMENT REQUIREMENTS.

A. Compliance deadlines should be established for the amended regulations.

A point of clarity is needed on the implementation deadline for several aspects of the proposed regulations. The Agency has established deadlines for stakeholders to comply with some of the proposed new regulations, including the requirements involving cybersecurity audits (between April 1, 2028 and April 1, 2030, depending on gross annual revenue);¹⁵ risk assessments (by April 1, 2028);¹⁶ and use of ADMT (by January 1, 2027).¹⁷ However, the proposed amendments to Articles 1 through 8, which introduce new requirements, do not specify compliance deadlines.

The new requirements include additional privacy policy disclosures, mandatory disclosures (previously optional), and processes for handling sensitive data related to “requests to know” and “requests to correct.”¹⁸ The new process for handling sensitive data must provide consumers a way to verify their information, which will require careful development to address security risks, especially because Social Security numbers are involved. Businesses need time to develop processes that meet consumer needs and safeguard this sensitive information.

Section 11343.4(b)(2) of the California Administrative Procedure Act (“APA”) allows state agencies, including the CPPA, to set an effective date later than the default effective date

¹⁵ See *id.* § 7121 (requiring the first cybersecurity audit report be completed by April 1, 2028, for companies with over \$100 million in 2026 revenue; by April 1, 2029, for companies with \$50-100 million in 2027 revenue; and by April 1, 2030, for companies with under \$50 million in 2028 revenue).

¹⁶ See *id.* § 7157 (requiring the first risk assessment be submitted by April 1, 2028).

¹⁷ See *id.* § 7200(b) (imposing a January 1, 2027 compliance deadline for businesses using ADMT for “significant decision[s]”).

¹⁸ See, e.g., *id.* § 7020.

prescribed by the APA, in a written instrument filed with, or as part of, a proposed regulation.¹⁹

Accordingly, these amendments should take effect on **January 1, 2027**, which will be consistent with other key dates, including the ADMT requirements, and avoid consumer and business confusion. Establishing a compliance date is necessary to provide businesses with a defined deadline to meet the new requirements, which will reduce uncertainty and help businesses allocate their resources accordingly.

B. The compliance deadlines for risk assessments should be clarified and harmonized.

The Agency has proposed various compliance deadlines for risk assessments. The proposed regulations require risk assessments to be completed by December 31, 2027, for activities initiated *before* the effective date and continuing thereafter.²⁰ However, Section 7155(a)(1) requires a risk assessment before initiating any new processing activity—and the first risk assessment is not due until December 31, 2027. Additionally, Section 7155(a)(3) requires that a risk assessment must be updated no later than 45 calendar days if there is a material change related to the processing activity—but again, such risk assessment is not due until December 31, 2027. These three provisions are difficult to reconcile.

We recommend harmonizing the requirements as follows: (1) risk assessments for existing processing activities must be completed by **December 31, 2027**; (2) risk assessments for new processing must be completed **before initiation**; and (3) risk assessments for material changes must be updated **within 45 days after December 31, 2027**.

¹⁹ See Cal. Gov. Code § 11343.4(b)(2).

²⁰ See Proposed Regulations § 7155(b).

V. THE EXEMPTION ALLOWING ADMT USE FOR SECURITY, FRAUD PREVENTION, AND SAFETY WITHOUT A CONSUMER OPT-OUT SHOULD BE RESTORED.

The Agency initially proposed exempting businesses from the consumer ADMT opt-out requirements if the data was used solely for security, fraud prevention, or safety purposes.²¹ The latest modifications remove this exemption in Section 7221. While entities may be able to use ADMT for security, fraud, and safety purposes under other legal authorities,²² this language should be restored in Section 7221, as it provided a helpful clarification for covered entities regarding ADMT uses that can be undertaken without offering a consumer opt-out.

Consistent with the other provisions of the Act, the Agency should revise Section 7221 to clarify that businesses are exempt from offering consumers the ability to opt-out of ADMT usage when data is used for security, fraud prevention, or safety purposes. The Agency should also ensure that Section 7221 provides an ADMT opt-out not only when the data is used *exclusively* for security, fraud prevention, or safety purposes, but also when that data is used for those purposes *combined with* other uses. Many commenters support this exemption and note that privacy protections should not hinder critical safety, fraud prevention, and safety efforts.²³ Restoring the language in this section would provide greater clarity—and better protect consumers from bad actors. Moreover, this change would ensure consistency with similar

²¹ See Proposed Cal. Code Regs. tit. 11, § 7221(b)(1) (Nov. 22, 2024), <https://tinyurl.com/jrxbpe4p>.

²² See, e.g., Cal. Civ. Code § 1798.145 Exemptions.

²³ See, e.g., Comments of the Consumer Technology Association, at 5 (filed Feb. 19, 2025), <https://tinyurl.com/yd26nch9>; Comments of the Centre for Information Policy Leadership, at 8 (filed Feb. 19, 2025), <https://tinyurl.com/2mjyhhr3>; Comments of the Computer and Communications Industry Association, at 8 (filed Jan. 13, 2025), <https://tinyurl.com/bdctrxyz>.

provisions in U.S. privacy laws that broadly exempt offering opt-out rights for ADMT used for security, fraud, and safety reasons.²⁴

VI. CONCLUSION.

CTIA appreciates the opportunity to comment on these proposed regulations. We applaud the Agency's efforts to date to make the regulations more useful for consumers and navigable for companies. By adopting the modifications recommended above, the Agency can continue to protect consumers, while minimizing unnecessary regulatory burdens on businesses.

Respectfully submitted,

/s/ Gerard Keegan

Gerard Keegan

Vice President, State Legislative Affairs

Umair Javed

Senior Vice President and General Counsel

David Valdez

Vice President, Privacy and Cybersecurity

Avonne Bell

Director, Connected Life

Jake Lestock

Director, State Legislative Affairs

CTIA

1400 16th St. NW, Suite 600

Washington, DC 20036

(202) 736-3200

www.ctia.org

June 2, 2025

²⁴ See, e.g., Colo. Rev. Stat. § 6-1-1304(3)(a)(X); Conn. Gen. Stat. § 42-524(a)(9); Fla. Stat. § 501.716(1)(f); Ind. Code § 24-15-8-1(a)(7); Iowa Code § 715D.7(1)(g); Mont. Code § 30-14-2816(1)(i); Tex. Bus. & Com. Code § 541.201(a)(6); Va. Code Ann. § 59.1-582(A)(7).