

Grenda, Rianna@CPPA

From: Zhang, Jenna <JZhang@cov.com>
Sent: Monday, June 2, 2025 1:25 PM
To: Regulations@CPPA
Cc: Zhang, Jenna
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: ESA CCPA Comments (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

Attached please find comments from the Entertainment Software Association regarding the CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations.

Thank you,
Jenna

Jenna Zhang

Covington & Burling LLP
Salesforce Tower, 415 Mission Street, Suite 5400
San Francisco, CA 94105-2533
T +1 415 591 7045 | jzhang@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.

June 2, 2025

By Electronic Filing

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

To Whom It May Concern:

The Entertainment Software Association (“ESA”) submits these comments in connection with the California Privacy Protection Agency’s (“CPPA”) publication of further revisions to draft rules updating the existing California Consumer Privacy Act (“CCPA”) regulations.

ESA appreciates the significant improvements the CPPA has made to the draft rules. However, ESA urges the CPPA to take further action to address remaining issues with the revised rules pertaining to cybersecurity audits and risk assessments. Specifically, ESA recommends that the CPPA take the following steps:

- Align the criteria for triggering a cybersecurity audit with each of the statutorily mandated factors;
- Revise the proposed cybersecurity audit rules to avoid requiring businesses to disclose information that could enable malicious activity and cyber attacks;
- Avoid overreaching the statutory text with respect to content required in risk assessments and provide a meaningful safe harbor for risk assessments conducted in compliance with other laws or regulations; and
- Provide assurances of confidentiality and attorney-client privilege protection over risk assessments.

These points are discussed further in the sections below.

* * *

I. THE REVISED CYBERSECURITY AUDIT RULES CONFLICT WITH THE STATUTE AND WOULD JEOPARDIZE CALIFORNIANS’ SECURITY.

While the revised rules regarding cybersecurity audits improve on the previous draft made available for comment, significant issues remain. In particular, ESA urges the CPPA to tailor the application of the cybersecurity audit rules as required by the statute and avoid requiring businesses to include information in audit reports that malicious actors could misuse, particularly if such audits are not more explicitly treated as confidential.

A. To Adhere to the Statute, Cybersecurity Audits Should Only Be Required Where Processing Poses a Significant Risk to Consumer Privacy and Security.

The statute's rulemaking provision concerning cybersecurity audits provides a clear limiting principle for when audits may be required: rules are to apply to "businesses whose processing of consumers' personal information presents **significant risk** to consumers' privacy or security."¹ The statute further requires that "factors to be considered in determining when processing may result in significant risk . . . **shall** include the **size and complexity of the business** and the **nature and scope of processing activities**."² The proposed rule revisions do not implement this statutorily prescribed applicability test.

The section of the revised rules addressing the applicability of cybersecurity audit requirements remains unchanged from the previous version.³ These rules cross-reference portions of the statute's definition of a "business," rather than incorporate the criteria required by statute.⁴ As noted in ESA's prior submission and the submissions of other commenters, it is overbroad and inconsistent with the text of the statute to treat a business's processing as presenting "significant risk" simply because the business meets the minimum threshold for application of the statute.⁵ If the statute's drafters had wanted standards for the applicability of cybersecurity audit requirements to mirror the statute's definition of a "business," they could simply have said so.

The revised rules' approach neglects the range of "factors" described in the statute, which calls for a more nuanced and fact-specific evaluation of the level of risk generated by a business's "complexity" and the "nature and scope" of particular processing. For example, the revised rules would cover any business with \$25 million in annual revenue that processes the personal information of 250,000 consumers, regardless of the nature of the processing performed by that business.⁶ As such, a mid-sized video game company that enables players to register to receive emails about in-game events would be deemed to be engaging in processing that presents "significant risk," even if it collects no other personal information. The evident overbreadth of the proposed applicability provisions cuts against the statute's stated goal of promoting the implementation of "reasonable security procedures and practices appropriate to the nature of the personal information" collected.⁷

While the cybersecurity audit rules have been revised to modify the timelines for conducting cybersecurity audits, those revisions do nothing to align the revised rules with the thresholds for when a cybersecurity audit is required.⁸ Timing and applicability are separate considerations. ESA requests that the CCPA implement further changes to the revised rules to

¹ Cal. Civ. Code § 1798.185(a)(14) (emphasis added).

² *Id.* § 1798.185(a)(14)(A) (emphasis added).

³ See Revised Rules § 7120.

⁴ See *id.* § 7120(b) (cross-referencing sections of Cal. Civ. Code § 1798.140(d)(1)).

⁵ See, e.g., Comments of the California Chamber of Commerce at 12–15; Comments of the U.S. Chamber of Commerce at 11–12.

⁶ See Revised Rules § 7120(b)(2).

⁷ Cal. Civ. Code § 1798.100(e).

⁸ See Revised Rules § 7121(a).

clarify that a business need not perform a cybersecurity audit unless the complexity, nature, and scope, in addition to size, of its processing activities each pose a significant risk to consumers' privacy and security.

B. The Rules Should Not Require That Audit Reports Include Information That Would Endanger the Security of Systems.

The proposed revisions do not address commenters' concerns that the cybersecurity audit requirements will inadvertently undermine businesses' security by requiring them to disclose information that could enable malicious actors to bypass security measures. Despite revisions to requirements for the content of audit reports, the revised rules retain language requiring auditors to "[i]dentify and describe in detail the status of any gaps or weaknesses" in the business's policies, procedures, and security program components.⁹ The revised rules identify dozens of specific elements of a business's security program that must be evaluated as part of an audit.¹⁰ These elements touch every part of a business's security environment, from details about the configuration of hardware and software to the technologies relied upon to implement network monitoring and defenses. Absent a right to exclude sensitive details from audits, the revised rules essentially require that auditors produce a roadmap for defeating a business's security measures, jeopardizing the security of consumers' personal information.

Accordingly, ESA requests that the cybersecurity audit requirements be modified to limit the information that must be included in a cybersecurity audit report and permit businesses to exclude information that they deem to be sensitive. Additionally, the CPPA should confirm that it will take precautions to protect audits received from businesses against breaches or inappropriate disclosure, including by clarifying that audits will be treated as confidential and exempt from disclosure under public records laws. To protect businesses and consumers, all personal information and confidential business information should be redacted from the audits 30 days after they are received by the CPPA.

II. THE REQUIRED RISK ASSESSMENTS SHOULD BE FURTHER REVISED TO ALIGN WITH THE STATUTE AND ANALOGOUS LEGAL FRAMEWORKS.

While ESA recognizes the significant improvements made to the risk assessment requirements, the revised rules nevertheless remain inconsistent with both the statutory text and other similar legal frameworks in important ways. Specifically, ESA recommends that the required content for risk assessments be further revised and that the rules include explicit assurances of confidentiality and attorney-client privilege protections for risk assessments.

A. The Required Content for Risk Assessments Still Exceeds the Statutory Text.

The statutory text requires that minimal information be included in privacy risk assessments. Specifically, risk assessments need only cover (i) the processing of personal information and (ii) identifying and weighing the benefits of this processing against the potential

⁹ See Revised Rules § 7123(e)(3).

¹⁰ See Revised Rules § 7121(a)–(d).

risks of the processing.¹¹ This text reflects the importance of ensuring privacy assessments remain focused on actual risks to consumers and do not become a costly paperwork exercise with no countervailing benefits for California consumers. While the revised rules contain a number of line edits to the risk assessment content requirements, the revisions remain overly prescriptive and burdensome. Specifically, the revised rules have not eliminated any of the nine required elements, many with additional subparts, that must be addressed in the risk assessment.¹² These voluminous requirements continue to exceed the statutory text, with no evidence that this additional information provides consumers any actual benefit. Aligning the rules to the text of the statute would bring the CCPA's risk assessment content more in line with assessments found in other similar state privacy law frameworks.¹³ All of the other topics in the revised rules should be optional guidance that businesses may, but are not required to, take into consideration when completing their risk assessments.

As drafted, the revised rules fail to provide any safe harbor for risk assessments conducted in compliance with other laws or regulations. Although the revised rules state that a business may use a risk assessment prepared for another purpose to satisfy the risk assessment requirement, they also state that such a risk assessment will only be sufficient if it “contains the information that must be included in, or is paired with the outstanding information necessary for, compliance with section 7152.”¹⁴ This language effectively neuters the safe harbor provision because the revised rules’ required content for risk assessment does not align with any other similar privacy law framework for risk assessments, notwithstanding the flexible statutory text.¹⁵ ESA urges the CPPA to reconsider the safe harbor provisions and requests that the CPPA revise Section 7156(b) of the proposed rules as follows:

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 ~~contains the information that must be included in, or is paired with the outstanding information necessary for, compliance with section 7152~~ is reasonably similar in scope and effect to the assessment that would otherwise be conducted pursuant to this Article.

B. The Rules Should Contain Explicit Confidentiality and Attorney-Client Privilege Protections.

ESA urges the CPPA to revise the draft rules to include explicit assurances of confidentiality and attorney-client privilege protection over any assessments produced to the CPPA or Office of the Attorney General. First, this addition would be consistent with the statutory text itself, which guarantees that the risk assessment shall not require “a business to divulge trade secrets.”¹⁶ Second, it would align with the approach taken by the California legislature for

¹¹ Cal. Civ. Code § 1798.185(a)(14)(B).

¹² Revised Rules § 7152.

¹³ See, e.g., Con. Gen. Stat. § 42-522(b); Va. Code Ann. § 59.1-580(B); Or. Rev. Stat. § 646A.586(2); Tex. Bus. & Com. Code § 541.105(b)(1); Mont. Code Ann. § 30-14-2814(2)(a); Del. Code Ann. tit. 6, § 12D-108(b).

¹⁴ See Revised Rules § 7156(b).

¹⁵ See, e.g., Comments of California Chamber of Commerce at 24; Comments of California Grocers Association at 3; Comments of California Retailers Association at 6.

¹⁶ See Cal. Civ. Code § 1798.185(a)(14)(B).

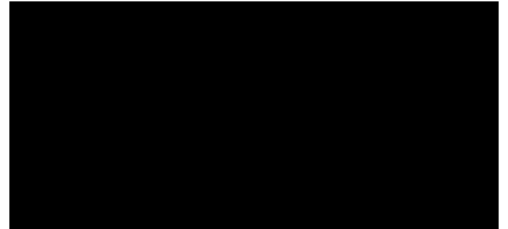
the risk assessments required by the Age-Appropriate Design Code Act.¹⁷ Third, this modification would align the CCPA regulations with other state consumer privacy laws that provide these protections for risk assessments.¹⁸ For these reasons, the regulations should provide such protections for risk assessments.

Indeed, multiple other commentors similarly recommended that the rules offer confidentiality and attorney-client privilege protections for risk assessments submitted pursuant to the regulations.¹⁹ Providing confidentiality and attorney-client privilege protections to risk assessments would help further the stated goal of the risk assessments in the revised rules, to “restrict[] or prohibit[] the processing of personal information if the risks to privacy of the consumer outweigh the benefits resulting from the processing,”²⁰ by encouraging businesses to engage in the cost-benefit analysis without fear of disclosing confidential or privileged information to the public. The CPPA should reconsider its decision to exclude these protections from the proposed rules.

* * *

ESA and its members appreciate the opportunity to provide further feedback on the CPPA's rulemaking process.

Sincerely,



Maya McKenzie
Senior Counsel, Tech Policy
Entertainment Software Association

¹⁷ See Cal. Civ. Code § 1798.99.31(a)(4)(B)–(C).

¹⁸ See, e.g., Conn. Gen. Stat. § 42-522(c), Va. Code Ann. § 59.1-580(C), Colo. Rev. Stat. § 6-1-1309(4).

¹⁹ See, e.g., Comments of Bank Policy Institute at 12; Comments of American Financial Services Association at 2; Comments of Google at 25.

²⁰ Revised Rules § 7154(a).

Grenda, Rianna@CPPA

From: Mayu Tobin-Miyaji <tobin-miyaji@epic.org>
Sent: Monday, June 2, 2025 4:33 PM
To: Regulations@CPPA
Cc: John Davisson; Kara Williams; Sara Geoghegan
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: Comments of EPIC on Cybersecurity Risk Assessments and ADMTs - Final.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,

Please see attached the comments from the Electronic Privacy Information Center (EPIC) regarding the CCPA updates, Cyber, Risk, ADMT and Insurance Regulations.

Thank you,

Mayu Tobin-Miyaji (she/her)
Law Fellow
[Electronic Privacy Information Center](#)
1519 New Hampshire Ave. NW
Washington, DC 20036

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

CALIFORNIA PRIVACY PROTECTION AGENCY

on

Proposed Rulemaking Regarding CCPA Updates, Cybersecurity Audits,
Risk Assessments, and Automated Decisionmaking Technology

June 2, 2025

The Electronic Privacy Information Center (“EPIC”) submits these comments in response to the invitation of the California Privacy Protection Agency (“CPPA” or “the Agency”) for input from stakeholders in response to the Agency’s proposed regulations on Cybersecurity, Risk Assessments, and Automated Decisionmaking Technology (“ADMT”) under the California Consumer Protection Act (“CCPA”), as modified by the California Privacy Rights Act (“CPRA”). We urge the Agency to reinstate the previous proposed provisions that offered consumers stronger protections from the harms caused by unchecked data collection and automated decisionmaking technologies and to resist industry pressure to weaken the proposed regulations.

EPIC is a public interest research center based in Washington, D.C., that was established in 1994 to focus public attention on emerging privacy and related human rights issues and to protect privacy, the First Amendment, and constitutional values.¹ EPIC has a long history of advocating for

¹ EPIC, *About EPIC* (2022), <https://epic.org/about/>.

safeguards for businesses' use of ADMT. EPIC has previously provided comments on the CCPA,² published a detailed analysis of the California Privacy Rights Act before its approval by California voters,³ and presented oral testimony to the Agency to encourage the strongest protections for Californians.⁴

The initial proposed regulations were a promising start to providing more consumer privacy protections and transparency and accountability mechanisms through risk assessments. However, under significant pressure from industry lobbyists and Governor Gavin Newsom, every iteration of the proposed regulations has been weakened in terms of consumer protection, transparency, and

² Comments of Electronic Privacy Information Center (EPIC) and Consumer Federation of America to the California Privacy Protection Agency (Feb. 19, 2025), <https://epic.org/documents/comments-to-the-cppa-on-proposed-regulations-regarding-cybersecurity-risk-assessments-and-admts/> [hereinafter EPIC CPPA Feb. 2025 Comments]; Comments of Consumer Reports, Electronic Frontier Foundation (EFF), Electronic Privacy Information Center (EPIC) and Privacy Rights Clearinghouse (PRC) In Response to the California Privacy Protection Agency's Invitation for Preliminary Comments On Proposed Rulemaking Under Senate Bill 362 (June 25, 2024), <https://advocacy.consumerreports.org/wp-content/uploads/2024/06/Comments-of-Consumer-Reports-In-Response-to-the-California-Privacy-Protection-Agency's-Invitation-for-Preliminary-Comments-On-Proposed-Rulemaking-Under-Senate-Bill-362.pdf>; Comments Of The Electronic Privacy Information Center, Center For Digital Democracy, and Consumer Federation Of America, to the California Privacy Protection Agency (Mar. 27, 2023), <https://epic.org/documents/comments-of-the-electronic-privacy-information-center-center-for-digital-democracy-and-consumer-federation-of-america-to-the-california-privacy-protection-agency/>; Comments of EPIC to Cal. Privacy Prot. Agency (Nov. 20, 2022), <https://epic.org/wp-content/uploads/2022/11/EPIC-CPPA-Comments-Nov-20.pdf>; Comments of EPIC et al. to Cal. Privacy Prot. Agency (Aug. 23, 2022), <https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf>; Comments of EPIC et al. to Cal. Privacy Prot. Agency (Nov. 8, 2021), <https://epic.org/wp-content/uploads/2021/11/PRO-01-21-Comments-EPIC-CA-CFA-OTI.pdf>; Comments of EPIC to Cal. Office of the Att'y Gen. (Feb. 25, 2020), <https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf>; Comments of EPIC to Cal. Office of the Att'y Gen. (Dec. 6, 2019), <https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Dec2019.pdf>.

³ EPIC, *California's Proposition 24* (2020), <https://epic.org/californias-proposition-24/>.

⁴ *EPIC Commends CPPA on Strong Proposed Regulations on Cybersecurity, Risk Assessments, and ADMT*, EPIC (Feb. 20, 2025), <https://epic.org/epic-commends-cppa-on-strong-proposed-regulations-on-cybersecurity-risk-assessments-and-admts/>; Testimony on the California Privacy Protection Agency's Draft Regulations on ADMT, Risk Assessments, and Cybersecurity, EPIC (May 2025), <https://epic.org/documents/california-testimony-on-the-california-privacy-protection-agencys-draft-regulations-on-admt-risk-assessments-and-cybersecurity/>.

accountability.⁵ These comments address the Agency’s proposed regulations⁶ in three parts: (I) ADMT regulations, (II) risk assessment regulations; and (III) cybersecurity assessment regulations. While we will not repeat the substance of our comments submitted to the CPPA in February 2025, they still remain relevant.

I. ADMT Regulations

Our chief concern with the proposed ADMT regulations is that the definition of “automated decisionmaking technology” is too narrow, leaving out many harmful and concerning uses of such tools. EPIC urges that the definition of ADMT cover situations where the system is used to “assist or replace” human decisionmaking, even if the system does not make the final call.⁷ Covering circumstances where both a human and ADMT are involved in a decisionmaking process is essential because research shows humans tend to over-rely on automated systems.⁸ The latest proposed definition of ADMT ignores this reality by excluding from coverage ADMTs that assist (but do not fully replace) human decisionmaking.

⁵ Kara Williams, Testimony on the California Privacy Protection Agency’s Draft Regulations on ADMT, Risk Assessments, and Cybersecurity, EPIC (May 2025), <https://epic.org/documents/california-testimony-on-the-california-privacy-protection-agencys-draft-regulations-on-admt-risk-assessments-and-cybersecurity/>.

⁶ Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies, § 7001 (May 9, 2025) https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf [hereinafter May 2025 Proposed Regulations].

⁷ See, e.g., Miranda Bogen & Aaron Rieke, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, Upturn (Dec. 2018), <https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20-%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf>; Charlotte Lytton, *AI Hiring Tools May be Filtering Out the Best Job Applicants*, BBC (Feb. 16, 2024), <https://www.bbc.com/worklife/article/20240214-ai-recruiting-hiring-software-bias-discrimination>; T. Christian Miller, Patrick Rucker & David Armstrong, “*Not Medically Necessary*”: *Inside the Company Helping America’s Biggest Health Insurers Deny Coverage for Care*, ProPublica (Oct. 23, 2024), <https://www.propublica.org/article/evicore-health-insurance-denials-cigna-unitedhealthcare-aetna-prior-authorizations>; *Screened Out of Housing: How AI-Powered Tenant Screening Hurts Renters*, Tech Equity (July 2024), <https://techequity.us/wp-content/uploads/2025/03/Screened-out-of-housing-paper-2025-updates.pdf>.

⁸ Eric Bogert, Aaron Schechter & Richard T. Watson, *Humans rely more on algorithms than social influence as a task becomes more difficult*, *Sci Rep* 11, 8028 (2021), <https://doi.org/10.1038/s41598-021-87480-9>.

The November 2025 proposed regulations defined ADMT as “any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking.”⁹ “Substantially facilitate” was defined as “using the output of the technology as a key factor in a human’s decisionmaking.”¹⁰ This definition, while narrower than the “assist or replace” language that EPIC recommends, does include situations where ADMT is used to generate a score about a consumer that a human reviewer uses as a primary factor to make a significant decision about them.¹¹ This definition would have captured, for example, ADMT that calculates a score about a rental applicant that the landlord would primarily rely on to make a decision about whether to accept or deny the application, which presents serious privacy risks to consumers including discrimination and unfair or erroneous decisions.¹²

The new proposed definition for ADMT covers “any technology that processes personal information and uses computation to replace human decisionmaking or substantially *replace* human decisionmaking.”¹³ “Substantially replace human decisionmaking” is defined as a business “us[ing] the technology’s output to make a decision without human involvement.”¹⁴ The example of a system

⁹ Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies, § 7001(f) (Nov. 22, 2024) https://coppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf [hereinafter November 2024 Proposed Regulations].

¹⁰ November 2024 Proposed Regulations § 7001(f)(2).

¹¹ November 2024 Proposed Regulations § 7001(f)(2).

¹² *Screened Out of Housing: How AI-Powered Tenant Screening Hurts Renters*, Tech Equity (July 2024), <https://techequity.us/wp-content/uploads/2025/03/Screened-out-of-housing-paper-2025-updates.pdf>; Thomas McBrien, Ben Winters, Enid Zhou & Virginia Eubanks, EPIC, *Screened & Scored in the District of Columbia*, 27-28 (2022), <https://epic.org/wp-content/uploads/2022/11/EPIC-Screened-in-DC-Report.pdf>; Lydia X. Z. Brown, *Tenant Screening Algorithms Enable Racial and Disability Discrimination at Scale, and Contribute to Broader Patterns of Injustice*, Center for Democracy and Technology (July 7, 2021), <https://cdt.org/insights/tenant-screening-algorithms-enable-racial-and-disability-discrimination-at-scale-and-contribute-to-broader-patterns-of-injustice/>.

¹³ May 2025 Proposed Regulations § 7001(e).

¹⁴ May 2025 Proposed Regulations § 7001(e)(2).

that generates a score about a consumer that the human reviewer uses as a primary factor in their decision is thus removed from coverage.

The new definition is even narrower than the original proposed definition, insofar as it removes from coverage situations when ADMT is the primary basis for a human decisionmaking or otherwise substantially facilitates the human decisionmaking (without fully replacing it). “Human involvement”—the presence of which would disqualify a system as ADMT—requires only that a person: “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).”¹⁵ Many ADMT examples involve a human decisionmaker in the loop, such as an employer making the final decision to hire or progress a job candidate based on AMDT outputs,¹⁶ law enforcement making the decision to arrest based on a false facial recognition match,¹⁷ or a landlord relying on ADMT score to accept or deny a rental application.¹⁸ But human involvement in a decision impacted by ADMT does not eliminate the significant privacy, accuracy, and equity concerns. Humans tend to over-rely on ADMT outputs, and business practices may

¹⁵ May 2025 Proposed Regulations § 7001(e).

¹⁶ Miranda Bogen & Aaron Rieke, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, Upturn (Dec. 2018), <https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20-%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf>;

¹⁷ Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men’s Lives*, Wired (Mar. 7, 2022), <https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/>; Alyxaundria Sanford, *Artificial Intelligence Is Putting Innocent People at Risk of Being Incarcerated*, Innocence Project (Feb. 14, 2024), <https://innocenceproject.org/artificial-intelligence-is-putting-innocent-people-at-risk-of-being-incarcerated/>.

¹⁸ Thomas McBrien, Ben Winters, Enid Zhou & Virginia Eubanks, EPIC, *Screened & Scored in the District of Columbia*, 27-28 (2022), <https://epic.org/wp-content/uploads/2022/11/EPIC-Screened-in-DC-Report.pdf>; *Screened Out of Housing: How AI-Powered Tenant Screening Hurts Renters*, Tech Equity (July 2024), <https://techequity.us/wp-content/uploads/2025/03/Screened-out-of-housing-paper-2025-updates.pdf>.

pressure the human in the loop to spend as little time as possible on each decision or may impose other barriers to the human's ability to disagree with ADMT outputs.¹⁹

While the “without human involvement” portion of the definition is seemingly included to prevent covered entities from relying on humans to act as rubber stamps for ADMT outputs, in reality, businesses are likely to use this provision to self-certify out of coverage. Even if a human is unqualified to assess or disagree with ADMT outputs, has little time to assess each decision, or otherwise feels pressure to rubber-stamp ADMT outputs, businesses will be incentivized to avoid compliance burdens by taking the stance that its system has a human in the loop. Coupled with the lack of public access or an affirmative obligation for companies to submit risk assessments to the CPPA, it will be extremely difficult for regulators to enforce risk assessment requirements as to companies who self-select out of compliance using this loophole.

This is the same strategy businesses have adopted to circumvent New York City's algorithmic transparency law, Local Law 144,²⁰ concerning automated decision technology used in employment decisions. The city's regulations cover circumstances in which an automated tool is “substantially assisting” discretionary decisionmaking, which occurs where either (1) the tool's output is the only factor in the decision; (2) the tool's output the most important factor in a set of criteria; or (3) the tool's output is used to override conclusions based on other factors, including

¹⁹ Patrick Rucker, Maya Miller & David Armstrong, *How Cigna Saves Millions by Having Its Doctors Reject Claims Without Reading Them*, ProPublica (March 25, 2023), <https://www.propublica.org/article/cigna-pdx-medical-health-insurance-rejection-claims>; Casey Ross & Bob Herman, *UnitedHealth pushed employees to follow an algorithm to cut off Medicare patients' rehab care*, STAT (Nov. 14, 2023), <https://www.statnews.com/2023/11/14/unitedhealth-algorithm-medicare-advantage-investigation/>.

²⁰ Local Law 2021/144, The New York City Council Legislative Research Center, <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4344524&GUID=B051915D-A9AC-451E-81F8-6596032FA3F9&Options=ID%7CText%7C&Search=>.

human decisionmaking.²¹ This standard allows businesses to effectively decide for themselves whether they are covered, as it is difficult for officials to identify a business that should be in compliance but is not.²² A similar fate likely awaits the CPPA's ADMT regulations if the Agency moves forward with a narrowed definition of ADMT. Many businesses will likely risk an (improbable) enforcement action over their failure to treat automated systems as covered ADMTs rather than proactively complying with the regulations given the considerable challenges and limitations of enforcement.

II. Risk Assessment Regulations

The first part of this section covers the three key changes in the latest draft regulations that substantially weaken the proposed risk assessment requirements. The second part of this section responds to common industry arguments against risk assessment. While the proposed regulations still represent a positive step forward in providing California consumers with transparency, the most recent proposal is a disappointing step back from the strong substantive risk assessment provisions in the previous version.

a. The revised risk assessment requirements are significantly weaker.

This section addresses three main problems with the revised regulations: (1) some processing activities that pose substantial privacy risks are excluded from the risk assessment requirement threshold; (2) numerous important risk assessment factors, such as the privacy risks of processing and how the business ensures the system works as intended, would no longer be reported to the

²¹ Grace Gedy, *New Research: NYC Algorithmic Transparency Law is Falling Short of Its Goals*, Consumer Reports (Feb. 8, 2024), <https://innovation.consumerreports.org/new-research-nyc-algorithmic-transparency-law-is-falling-short-of-its-goals/>.

²² *Id.*

CPPA (let alone the public); and (3) there is very little, if any, ability for the public to access risk assessments conducted by covered entities.

i. The thresholds for risk assessment obligations are too high and will wrongly exclude ADMT uses that pose significant privacy risks.

There are two large categories of triggers for risk assessments under the proposed regulations: (1) a business's actions pertaining to consumer personal information and (2) a business's use of automated decisionmaking technologies. For the first category, the current draft regulations are unchanged from prior versions, and the thresholds for coverage based on processing personal information are sufficiently broad. For the second category, however, there was a significant narrowing in the revised draft; the proposed regulations no longer require risk assessments or provide other consumer rights for some ADMT uses that pose serious privacy concerns.

In the latest proposal, the uses of ADMT that trigger risk assessments were narrowed, and many concerning uses were removed from coverage, meaning risk assessments and other ADMT-related provisions do not apply. Namely, the "significant decision" definition no longer includes decisions about criminal justice, insurance, or essential goods or services.²³ Some of the riskiest uses of ADMT are in criminal justice, as incorrect or biased outputs can expose individuals to wrongful arrest and have a tremendous impact on their wellbeing, including employment, housing, and mental health.²⁴ Removing the risk assessment requirement allows ADMTs to be deployed in such contexts

²³ May 2025 Proposed Regulations at § 7001(ddd).

²⁴ Eleni Manis, Fatima Ladha, Nina Loshkajian, Aidan McKay & Corinne Worthington, *Seeing Is Misbelieving*, Surveillance Technology Oversight Project (2024), <https://www.stopspying.org/seeing-is-misbelieving>; Aaron Sankin, Dhruv Mehrota, Surya Mattu, Dell Cameron, Annie Gilbertson, Daniel Lempres & Josh Lash, *Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them*, Gizmodo (Dec. 2, 2021), <https://gizmodo.com/crime-prediction-software-promised-to-be-free-of-biases-1848138977>; Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias*, ProPublica (May 23, 2016), <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>; Richard A. Webster, *An Algorithm Deemed This Nearly Blind 70-Year-Old Prisoner a "Moderate Risk."* Now

without a covered entity assessing the privacy risks or ensuring that the ADMT works accurately as intended and without bias. This puts Californians at risk. The definition of “significant decision” has also been narrowed such that it no longer covers Californians’ “access to” the enumerated list of important goods and services; instead, a significant decision is defined as only the “provision or denial of” such goods and services.²⁵ This narrowing means that businesses no longer need to conduct risk assessments or provide people with other ADMT rights if they use ADMT to price necessities like rent, insurance, or health care so prohibitively high that many people can no longer afford to access them, for example.

Further, ADMT used for profiling a consumer for behavioral advertising was also removed from the list of risk assessment triggers. While the “selling or sharing” personal information trigger for risk assessments remains—which captures much of the data broker industry—first-party profiling for behavioral advertising would no longer require risk assessments. Advertisers routinely use characteristics like race, gender, and income or proxies like ZIP codes to filter and target certain audience segments to advertise employment,²⁶ housing,²⁷ and educational opportunities.²⁸ First-party

He’s No Longer Eligible for Parole., ProPublica (April 10, 2025), <https://www.propublica.org/article/tiger-algorithm-louisiana-parole-calvin-alexander>.

²⁵ May 2025 Proposed Regulations § 7001(ddd).

²⁶ *Surveillance Advertising: What About Discrimination?*, Consumer Federation of America (Aug. 26, 2021), https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-discrimination/; Julia Angwin, Noam Scheiber & Ariana Tobin, *Dozens of Companies Are Using Facebook to Exclude Older Workers from Job Ads*, ProPublica (Dec. 20, 2017), <https://www.propublica.org/article/facebook-ads-age-discrimination-targeting>; Ariana Tobin & Jeremy B. Merrill, *Facebook Is Letting Job Advertisers Target Only Men*, ProPublica (Sept. 18, 2018), <https://www.propublica.org/article/facebook-is-letting-job-advertisers-target-only-men>.

²⁷ *Charge of Discrimination, HUD, et al v. Facebook, Inc.*, FHEO No. 01-18-0323-8 (Mar. 28, 2019), https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf.

²⁸ Press Release, *New Lawsuit Challenges Big Tech Firm Meta for Discrimination in Advertising Higher Education Opportunities*, Lawyers’ Committee for Civil Rights Under Law (Feb. 11, 2025), <https://www.lawyerscommittee.org/new-lawsuit-challenges-big-tech-firm-meta-for-discrimination-in-advertising-higher-education-opportunities/>.

or not, profiling for behavioral advertising poses consumer privacy and equity risks and should therefore trigger the risk assessment requirement.

Profiling in public places was removed and replaced with profiling in “sensitive locations,” which are defined as “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.”²⁹ This new construction leaves out the profiling of consumers in other public spaces—such as retail businesses, streets, entertainment venues, or public transit—from the risk assessment requirements. Profiling in such public, non-sensitive spaces still threatens consumer privacy. Businesses often surreptitiously and continuously collect personal information on consumers and create a system of surveillance that can track individuals’ locations, habits, and associations as well as gatekeep entry into businesses and entertainment venues on opaque and unaccountable criteria.³⁰

²⁹ May 2025 Proposed Regulations § 7001(aaa).

³⁰ See, e.g., Suzanne Smalley, *Facial Recognition Technology Widely Used at Sporting Events, Privacy Watchdog Says*, The Record (May 23, 2024), <https://therecord.media/facial-recognition-tech-used-in-sporting-events>; Khari Johnson, *Get Used to Facial Recognition in Stadiums*, Wired (Feb. 2, 2023), <https://www.wired.com/story/get-used-to-face-recognition-in-stadiums/>; Joel R. McConvey, *Facial Recognition Comes to Great American Ballpark with MLB Go-Ahead Entry*, Biometric Update (Aug. 13, 2024), <https://www.biometricupdate.com/202408/facial-recognition-comes-to-great-american-ballpark-with-mlb-go-ahead-entry>; Abigail Opiah, *Facial Recognition Targets Scalping at Concerts and Festivals*, Biometric Update (Aug. 20, 2024), <https://www.biometricupdate.com/202408/facial-recognition-targets-scalping-at-concerts-and-festivals>; Manuela López Restrepo, *She Was Denied Entry to a Rockettes Show — Then the Facial Recognition Debate Ignited*, NPR (Jan. 21, 2023), <https://www.npr.org/2023/01/21/1150289272/facial-recognition-technology-madison-square-garden-law-new-york>; Eduardo Medina, *Rite Aid’s A.I. Facial Recognition Wrongly Tagged People of Color as Shoplifters*, N.Y. Times (Dec. 21, 2023), <https://www.nytimes.com/2023/12/21/business/rite-aid-ai-facial-recognition.html>; Shanti Das, *Facial recognition cameras in supermarkets ‘targeted at poor areas’ in England*, Guardian (Jan. 27, 2024), <https://www.theguardian.com/uk-news/2024/jan/27/facial-recognition-cameras-in-supermarkets-targeted-at-poor-areas-in-england>.

The revised proposal narrows the threshold concerning training ADMT as well. The prior version of the regulations would have required a risk assessment when a business is “processing personal information to train ADMT 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.”³¹ The recent version narrows the initial scope of coverage by replacing “capable of being used for” with “which the business intends to use for,” deferring to the business’s intent rather than acknowledging the inherent risk that some ADMT can be put to high-impact uses.³² This again makes it easier for businesses to self-certify out of risk assessment requirements by claiming they didn’t intend to use the resulting model for the enumerated uses when they were training the model.

The list of enumerated use cases also removed “for the generation of a deepfake” and “for the operation of generative models, such as large language models.” These two removals are concerning because large language models, other generative models, and especially the generation of deepfakes all pose grave privacy concerns. Many tech companies have been training large language models on content scraped from the internet without the knowledge or consent of the data subjects, which has been shown to include children and copyrighted material.³³ This information then becomes baked into the model, with no clear means for consumers to prevent their personal information from being

³¹ November 2024 Proposed Regulations § 7200(a)(3).

³² May 2025 Proposed Regulations § 7150(b)(6).

³³ Maggie Harrison Dupré, *AI Is Being Trained on Images of Real Kids Without Consent*, Futurism (June 12, 2024), <https://futurism.com/ai-trained-images-kids>; Vittoria Elliott, *AI Tools Are Secretly Training on Real Images of Children*, Wired (June 10, 2024), <https://www.wired.com/story/ai-tools-are-secretly-training-on-real-childrens-faces/>; Vish Gain, *Grok AI is training on user data by default – here’s how to stop it*, Silicon Republic (July 29, 2024), <https://www.siliconrepublic.com/business/grok-ai-training-x-twitter-default-user-data-privacy-turn-off>; <https://therecord.media/linkedin-lawsuit-private-messages-ai-training>; Suzanne Smalley, *LinkedIn sued for allegedly training AI models with private messages without consent*, The Record (Jan. 23, 2025), <https://thehackernews.com/2025/05/meta-to-train-ai-on-eu-user-data-from.html>.

exploited or leaked.³⁴ This removal effectively allows Big Tech to continue training large language models on any data it can access, without regard to consent or privacy harms. And the use of generative AI to produce deepfakes presents clear privacy risks, which is why the federal government and many states—including California—have taken quick action to regulate this use of AI.³⁵ This acknowledgment of the risks posed by generative AI models makes it difficult to understand why the CPPA would remove these uses from the scope of the risk assessment requirements.

ii. The proposed regulations do not require the assessment of privacy risks.

The November 2024 proposed regulations required businesses to conduct a detailed risk assessment and submit an abridged version to the CPPA, with the CPPA reserving the right to request the full risk assessment. By contrast, the CPPA’s revised proposal not only strips out key required elements (including assessing privacy risks), but also requires only the barest of risk assessment information to be submitted to the CPPA by default.

A. The ‘risk assessment report’ fails to require an analysis of the benefits and risks of processing.

The risk assessment requirement in the May 2025 proposed regulations undermines the core goal of risk assessments: forcing businesses to assess whether the benefits of processing outweigh

³⁴ Chris Tozzi, *How bad is generative AI data leakage and how can you stop it?*, Tech Target (Dec. 19, 2024), <https://www.techtarget.com/searchenterpriseai/answer/How-bad-is-generative-AI-data-leakage-and-how-can-you-stop-it>.

³⁵ Barbara Ortutay, *President Trump signs Take It Down Act, addressing nonconsensual deepfakes. What is it?*, AP (May 20, 2025), <https://apnews.com/article/take-it-down-deepfake-trump-melania-first-amendment-741a6e525e81e5e3d8843aac20de8615>; *Governor Newsom signs bills to combat deepfake election content*, Office of Gov. Gavin Newsom (Sept. 17, 2024), <https://www.gov.ca.gov/2024/09/17/governor-newsom-signs-bills-to-combat-deepfake-election-content/>; Zach Williams, *New York Bans Deepfake Revenge Porn Distribution as AI Use Grows*, Bloomberg Law (Oct. 2, 2023), <https://news.bloomberglaw.com/in-house-counsel/n-y-outlaws-unlawful-publication-of-deepfake-revenge-porn>; Bill Kramer, *More and More States Are Enacting Laws Addressing AI Deepfakes*, MultiState (April 5, 2024), <https://www.multistate.us/insider/2024/4/5/more-and-more-states-are-enacting-laws-addressing-ai-deepfakes>.

the privacy risks (and be accountable to that assessment). The revised regulations invent a “risk assessment report” that a covered business must complete. The proposed regulations lay out specific required components of a risk assessment. However, only some of these components are required components of the “risk assessment report.”³⁶ Several important components of a risk assessment, including an assessment of the benefits of the proposed processing and an assessment of the privacy risks of the processing, are not required to be included in the risk assessment report.³⁷ Thus, even though the risk assessment portion “requires” the business to assess the benefits and privacy risks of processing, the contents of such analysis would never be routinely reported to the CPPA because they are not required parts of the risk assessment report. This problem is exacerbated by the regulations’ lack of an affirmative obligation to disclose more detailed assessment information to the CPPA and by limitations on the CPPA’s ability to request and obtain risk assessment report material.

The exclusion of the benefits and privacy risks of processing from the risk assessment report runs counter to the text of the CCPA, stymies the goal of risk assessments, and undercuts the CPPA’s oversight authority. The CCPA directs the CPPA to promulgate regulations requiring businesses “whose processing of consumers’ personal information presents significant risk to consumers’ privacy or security” to submit to the CPPA on a regular basis a risk assessment.³⁸ By excluding the assessment of privacy risks from the risk assessment report, the revised regulations will no longer compel an adequate assessment of risks to consumers’ privacy or security. Further, because the proposed regulations no longer require businesses to routinely disclose meaningful risk assessment information to the Agency, they fail to fulfill the CCPA’s mandate that businesses

³⁶ May 2025 Proposed Regulations § 7152.

³⁷ *Id.* at § 7152(a)(4)–(5).

³⁸ Cal. Civ Code § 1798.185(a)(14)(B).

“submit to the CPPA on a regular basis a risk assessment.”³⁹ Thus, the CPPA is abdicating its role in ensuring that businesses adequately assess “whether the risks to consumers’ privacy from the processing personal information outweigh the benefits”—the primary goal of a risk assessment, as stated in the proposed regulations.⁴⁰ Finally, the CPPA is diminishing its own ability to gain insight into privacy risks of processing activities that businesses would have had to disclose.

B. The required content of the risk assessment report exhibits dangerous gaps.

The removal of key risk assessment content requirements since the November 2024 version of the regulations has significantly weakened the proposed risk assessment framework.

The new version strikes the following sentence, which would have made the provision more robust: “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.”⁴¹ The removal of this sentence makes the assessment of mitigation measures less robust because it no longer requires businesses to assess the extent to which the negative privacy impacts are mitigated. Once again, this undercuts the overall goal of conducting risk assessments—to force businesses to weigh the benefits and risks of processing—which should include an assessment of how effectively the mitigation measures would decrease risks and impact the overall risk-benefit calculus. Removing the requirement that businesses identify how they will maintain knowledge of emergent risks is also counter to the interests of consumers: the CPPA is effectively allowing businesses to stick their heads in the sand after system deployment, even if serious real-life harms emerge.

³⁹ *Id.*

⁴⁰ May 2025 Proposed Regulations § 7152(a).

⁴¹ May 2025 Proposed Regulations § 7152(a)(6).

To fulfill its CCPA directive to protect consumer privacy, the CPPA should, at minimum, require businesses to conduct and submit the full risk assessment report by default, and correct the other deficiencies identified above.

C. The May 2025 version no longer requires businesses to test and show that their ADMT is safe for California consumers.

The revised proposal introduces several other glaring deficiencies with respect to ADMT. First, the May 2025 version removed the provision that required businesses to identify, for uses of ADMT, the actions the business will take to maintain the quality of personal information processed by the ADMT, with clear examples of how the business can do so.⁴² The “quality of personal information” included the completeness, representativeness, timeliness, validity, accuracy, consistency, and reliability of the sources of the personal information used in a business’s application of ADMT. Businesses could have verified the quality of personal information by (1) identifying the source of personal information and its reliability; (2) identifying how the personal information is relevant to the task being automated and will be useful; (3) identifying whether the personal information contains sufficient breadth to address the range of real-world inputs; and 4) identifying how errors are measured and limited.⁴³ The November 2024 proposed regulations rightly placed the onus of ensuring the quality of the personal information on the business developing and deploying such automated decisionmaking systems to make significant decisions about consumers’ lives. This removal signals to businesses that they are free to deploy systems without robust policies and practices in place to ensure the quality of personal information, thus forcing consumers bear the brunt of any errors.

⁴² November 2024 Proposed Regulations § 7152 (a)(2)(B).

⁴³ *Id.* § 7152 (a)(2)(B)(i)-(ii) (summarized).

Second, the May 2025 version also removes the requirement that businesses evaluate the need for human involvement and implement policies, training, and procedures to address the degree of human involvement as a potential safeguard, which also harms consumers.⁴⁴ Every business deploying ADMTs should assess the appropriate degree of human involvement in the system to mitigate risks of inaccuracy, arbitrariness, and bias. Businesses should also consider how to properly train the humans involved so they do not give undue weight to ADMT outputs or merely rubber-stamp those outputs.

Lastly, the May 2025 version strikes the provision that would have required businesses to identify whether they evaluated the ADMT to ensure it works as intended for their proposed use and does not discriminate based on an individual's membership in a protected class.⁴⁵ Similar to the first point, this removal allows businesses to avoid testing the system to ensure it works accurately and without discrimination before deployment. Instead of putting the burden on the business to show that its system works as intended, the proposed regulations will allow businesses to deploy untested and potentially dangerous ADMTs while still attesting that they complied with the risk assessment requirements.

iii. Entities are no longer prohibited from engaging in processing activities where risks to consumers' privacy outweigh the benefits.

The May 2025 version completely guts the previously prohibition on processing activities where risks to consumers' privacy outweigh the benefits. The November 2024 proposal included the commonsense rule that if entities found through conducting their required risk assessments that a particular processing activity or use of ADMT presented more risks to privacy than potential

⁴⁴ May 2025 Proposed Regulations § 7152 (a)(6)(A).

⁴⁵ May 2025 Proposed Regulations § 7152 (6)(B)(i).

benefits, the entity was prohibited from engaging in that activity.⁴⁶ The November 2024 proposal gave some teeth to this provision by allowing the CPPA to assess the completed risk assessments and real-life impacts on whether the benefits outweigh the risks of a particular processing activity. The new language takes a huge step backward on this point, now stating that the “goal of a risk assessment is restricting or prohibiting the processing of personal information if the risks to privacy of the consumer outweigh the benefits resulting from processing,” rather than directly prohibiting such processing.⁴⁷ The weakening of this provision renders it largely meaningless and curtails the CPPA’s ability to enforce this portion of the regulations.

This weakened language (combined with the removal of the requirement that businesses analyze the benefits and privacy risks from the risk assessment report) calls into doubt whether the CPPA is interested in enforcing businesses’ obligation conduct effective risk assessments. Under the May 2025 draft regulations, the CPPA would have a dramatically reduced ability to examine how businesses have weighed the benefits and risks of certain processing activities—and even when it can, the language would not allow the CPPA to enforce a prohibition when the risks outweigh the benefits. To incentivize entities to conduct effective risk assessments and to ensure that they only engage in data processing that is more beneficial than harmful, the CPPA should restore the November 2024 language. The current proposal provides lip service to the importance of risk assessments yet allows businesses to continue processing personal data even when they know the privacy risks outweigh potential benefits.

⁴⁶ November 2024 Proposed Regulations § 7154.

⁴⁷ May 2025 Proposed Regulations § 7154.

iv. The proposed regulations require businesses to report very little information to the CPPA, and the public would have no access to risk assessments.

Under the May 2025 proposal, businesses are required to report very little information to the CPPA by default, beyond the fact that they completed the required risk assessment, when it was completed, and who submitted the risk assessment.⁴⁸ The only substantive details businesses must routinely disclose are the categories of processing activities that triggered a risk assessment, which alone provide very little insight into a business's assessment of the risks of processing.

Other than determining whether the business claims to have done the risk assessment, the CPPA has would often have nothing to go on to assess the sufficiency of the risk assessment purportedly conducted by the business. By contrast, the abridged risk assessment that the November 2024 version would have required businesses to submit to the CPPA by default included: (1) the processing activity triggering the risk assessment; (2) a plain language explanation of its purpose for processing consumers' personal information; (3) the categories of personal information processed, and whether sensitive personal information is included; and (4) a plain language explanation of safeguards the business has implemented.⁴⁹ Although EPIC continues to believe that businesses should disclose more information to the CPPA than the November 2024 proposal called for, the May 2025 proposal falls far short of even this meager list of information.

The CPPA is required under the CCPA to "provide a public report summarizing the risk assessments filed with the agency."⁵⁰ But given that the information submitted to the CPPA under the revised proposal would be so scant, there would very little information that for the CPPA to include in such a "public report." Even if the CPPA's public report included the full "risk assessment

⁴⁸ May 2025 Proposed Regulations § 7157(b).

⁴⁹ November 2024 Proposed Regulations § 7257(b)(2).

⁵⁰ Cal. Civ. Code § 1798.199.40(d).

reports” that the CPPA may request businesses produce, those reports would not include the assessment of benefits and risks to consumer privacy from the processing. Thus, the CPPA would struggle to inform the public about the risks of businesses’ processing.

The May 2025 proposal merely requires self-certification from businesses that they conducted a risk assessment. Self-certification alone is not effective at protecting consumers from harmful processing, and in fact it can encourage businesses to do as little as possible while complying with the default reporting requirements. The current regulations provide cover for businesses to claim they complied with the risk assessment requirements while having done little to assess the actual risks to consumer privacy, potentially misleading consumers and further failing to protect their privacy. To protect consumers from harmful processing, the CPPA should require businesses to analyze negative privacy risks, mandate more information be submitted to the Agency by default, and make risk assessments public. These requirements would ensure businesses spend more time and effort undertaking effective risk assessments and would give consumers greater transparency. The CPPA should reinstate the November 2024 version of risk assessment requirements and require businesses to make public (at a minimum) the abridged risk assessment.⁵¹

b. Industry’s arguments against strong risk assessment regulations fail.

Big Tech and other industry groups have consistently pushed the Agency to weaken its proposed privacy regulations, undermining the Agency’s mission and harming consumers while promoting an anti-regulatory agenda.⁵² Big Tech and industry lobbyists have poured resources into fighting regulations for decades, which has left consumers with a failed notice-and-choice regime.

⁵¹ See EPIC CPPA Feb. 2025 Comments.

⁵² Khari Johnson, *California Regulator Weakens AI Rules, Giving Big Tech More Leeway To Track You*, Cal Matters (May 7, 2025), <https://calmatters.org/economy/technology/2025/05/california-regulator-weakens-ai-rules-giving-big-tech-more-leeway-to-track-you/>.

Tech’s infamous goal was to “move fast and break things,”⁵³ and in the destructive wake of this goal, it has left a broken ecosystem that harms consumers and competition.⁵⁴ This broken ecosystem was the very thing that Californians overwhelmingly voted to fix through the ballot initiatives that established the California Consumer Privacy Act and the California Privacy Protection Agency.

This section responds to the tired arguments that industry has made for years to maintain the status quo—a gift to Big Tech at the expense of the consumer. Big Tech now pushes these arguments in written comments, oral testimony, and press materials to the Agency and the public (with the support of some pro-Big Tech politicians) to water down the protections for consumers.⁵⁵ This section aims to provide rebuttals for consumers and consumer advocates in California and beyond to push back on such industry arguments.

Industry Argument: The Agency has exceeded the scope of its authority.

Industry is pushing the argument that the CPPA, California’s dedicated agency tasked with protecting consumer privacy, has overstepped its legal authority in developing these proposed regulations on cybersecurity, risk assessments, and ADMTs. Industry also argues that the Agency should limit itself to privacy-related issues and should not regulate ADMTs more broadly.

Unfortunately for industry, these regulations are squarely within the Agency’s authority. The CCPA explicitly authorizes the Agency to promulgate regulations requiring companies “whose

⁵³ Patrice Taddonio, *WATCH: Inside Facebook’s Early Days*, PBS (Oct. 29, 2018), <https://www.pbs.org/wgbh/frontline/article/watch-inside-facebooks-early-days/>.

⁵⁴ Courtney Radsch, *Meta and Mark Zuckerberg must not be allowed to shape the next era of humanity*, Guardian (Feb. 4, 2024), <https://www.theguardian.com/commentisfree/2024/feb/04/mark-zuckerberg-meta-facebook-ai-future-accountability>.

⁵⁵ Jennifer Sheridan, *California legislators challenge independence of CPPA rulemaking authority*, IAPP (Apr. 2, 2025), <https://iapp.org/news/a/california-legislators-challenge-independence-of-cppa-rulemaking-authority>; Tyler Katzenberger, *Echoing Big Tech, Newsom warns privacy watchdog on AI*, Politico (Apr. 24, 2025), <https://www.politico.com/news/2025/04/24/newsom-california-privacy-cppa-ai-00307233>; Jeremy B. White, *Newsom sends prepaid phones, aka ‘burners,’ to tech CEOs*, Politico (Mar. 18, 2025), <https://www.politico.com/news/2025/03/18/newsom-ceos-burner-phones-00235044>.

processing of consumers' personal information presents significant risk to consumers' privacy or security" to submit risk assessments to the Agency.⁵⁶ When the risks to privacy outweigh the purported benefits, the goal of the regulations is to restrict or prohibit the processing.⁵⁷ The CCPA also explicitly provides the Agency the authority to issue regulations "governing access and opt-out rights with respect to businesses' use of automated decision-making technology."⁵⁸ EPIC joined the ACLU of Northern California in its comments⁵⁹ to the Agency addressing this issue:

The plain terms of the CCPA also enable the agency to promulgate regulations that sweep farther than the specified topics identified in Section 185(a). Section 185 itself makes this clear, directing that authority to issue regulations extends to all areas that would "further the purposes of this title, including, but not limited to, the following areas." Section 1798.185(a). This wider scope of authority is reiterated in Section 185(b), which states that regulations can be adopted "to further the purposes of this title." Those "purposes" are enumerated explicitly in the CPRA and clearly reach the collection, disclosure, and use of personal information: "[i]n enacting this Act, it is the *purpose and intent* of the people of the State of California to further protect consumers' rights, including the constitutional right of privacy. Section 3, CPRA (emphasis added). Those "consumer rights" are detailed in Section 3(A), which indicates that consumers should, under the law, have rights to control the use of their personal information. *See* CPRA Section 3(A)(2) ("[c]onsumers should be able to control the use of their personal information, including limiting the use of their sensitive personal information, the unauthorized use or disclosure of which creates a heightened risk of harm to the consumer, and they should have meaningful options over how it is collected, used, and disclosed."); *see also* CPRA Section 3(A)(2)(7) ("[c]onsumers should benefit from businesses' *use* of their personal information.") (emphasis added).

Based on these clear statutory directives, the CPPA is acting within its authority—and is, in fact, fulfilling its CCPA-assigned mission—by promulgating these regulations. Thus, industry's

⁵⁶ Cal. Civ. Code § 1798.185(a)(14)(b).

⁵⁷ *Id.*

⁵⁸ *Id.* at § 1798.185(a)(15).

⁵⁹ ACLU California Action, et al., *Re: Comments on Proposed Risk Assessments and Automated Decisionmaking Technology Regulations*, ACLU of Northern California (Feb. 19, 2025), <https://www.aclunc.org/sites/default/files/2025-02-19%20ACLU%20CA%20Action%20EPIC%20EFF%20CFA%20PRC%20CPPA%20Comments.pdf>.

repeated argument that regulating ADMTs is outside of the CPPA's authority and should be left to the Legislature is without merit.

Industry Argument: The Agency should leave regulation of automated decisionmaking technology to Governor Newsom and the Legislature.

The Agency was created through a ballot measure whereby Californians expressed their clear desire to have a privacy agency tasked with protecting them. The state Legislature and Governor have approved the statutes that give the Agency the explicit authority to regulate data practices that harm consumers. This Agency, and these very regulations, are the exact type of regulation that the Agency was created to address.

Industry Argument: Regulations in California must be harmonized with other emerging regulations that are not so overly broad.

California, or any state for that matter, should not water down its regulations because other jurisdictions impose weaker standards. States are not fulfilling their roles as laboratories of democracy if they merely adopt exactly what other jurisdictions have done without using their own experiences and expertise to craft tailored rules. If other jurisdictions promulgate risk assessment requirements that have fewer or lower requirements, companies that operate across jurisdictions will likely conduct risk assessments consistent with California's standards, if they are indeed stronger. California should promulgate requirements that create the floor for risk assessments, especially because of its position as the only state with an entire agency dedicated to developing privacy expertise. Further, because California is home to many tech companies and major industry players, it is arguably in the best position to develop regulations that would affect its own resident businesses.

Industry Argument: Training of ADMTs should be excluded from the risk assessment requirements.

As explained above, the statute explicitly provides the Agency the authority to regulate a business's processing of personal information when the processing poses significant risks to consumers' privacy. The voter guide for California's constitutional right to privacy, which was

passed by voters and legislatures in 1972, explained the right to privacy was meant to address privacy mischiefs, including “the improper use of information properly obtained for a specific purpose, for example, the use of it for another purpose or the disclosure of it to some third party.”⁶⁰ Using personal information to train AI, when it was not collected for this specific purpose, contradicts California’s constitutional right to privacy and is the exact type of misuse of personal information that the Agency is mandated to protect consumers against.

Industry Argument: Reporting requirements are onerous and will lead to a deluge of paperwork for the industry.

In 2025, companies should already be in the habit of conducting risk assessments before they collect or process personal information. Any entity that is processing information in a way that could hurt consumers should calculate the risks and determine what safeguards should be in place to mitigate any harm. If companies have not done any paperwork regarding risks associated with their processing of personal information, it is past time for them to consider how their data processing could harm consumers. And if a company has already been doing so as a general safety practice or to comply with requirements in another jurisdiction, the burden of compiling those risks into a CCPA-mandated assessment will be minimal. Because some form of risk assessment is required in many states and many international jurisdictions, including the EU,⁶¹ it is likely that many companies are already required to compile this information.

⁶⁰ *White v. Davis*, 13 Cal.3d at 775 (citing ballot argument).

⁶¹ Kara Williams, *Assessing the Assessments: Comparing Risk Assessment Requirements Around the World*, EPIC (Dec. 4, 2023), <https://epic.org/impact-comparison/>.

Moreover, assessments actually promote compliance: These assessments will help businesses comply with CCPA provisions like section 7002, which limits data collection to what is necessary,⁶² and section 7027, which empowers consumers to restrict the use of sensitive personal information.⁶³

Industry Argument: The costs of regulation are too high. Businesses will be hurt by regulation, especially small businesses.

The Agency has given careful consideration to the benefits and costs to these regulations. After a detailed economic analysis, the Agency determined that regulation—specifically, the November 2024 proposal—is the best path forward. While the Agency has concluded there will likely be an economic impact from regulation, it has determined that the benefits will outweigh the costs in the long run. Additionally, it is especially critical to also consider non-monetary costs and benefits of the proposed regulations, given that many privacy harms are abstract and difficult to quantify.

In terms of monetary costs and benefits, the Agency estimates that the compliance costs per firm will be \$6,768 in the first year for the November 2024 proposed risk assessment framework.⁶⁴ Moreover, the majority of the costs for a risk assessment will be mitigated by the baseline (given that “quantification of certain benefits and negative impacts to consumers should already be considered by businesses”), and the only additional costs should be organizational.⁶⁵ Because many businesses are already subject to the GDPR and Colorado’s privacy law, some of the costs will be mitigated.⁶⁶ This expense may seem substantial in the short term, but it reflects what is necessary to protect the

⁶² Cal. Civ. Code § 1798.100(c).

⁶³ Cal. Civ. Code § 1798.135.

⁶⁴ Standardized Regulatory Impact Assessment: California Privacy, 57 (Oct. 2024), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_impact.pdf.

⁶⁵ ISOR Appendix A, pp. 57-58,

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

⁶⁶ *Id.*

privacy of Californians in the modern commercial surveillance ecosystem according to the Agency's expert cost-benefit analysis.

Some of these costs would also be offset by covered businesses avoiding falling victim to cybercrime or other expensive cybersecurity incidents. Conducting risk assessments and cybersecurity audits increases the likelihood of detecting and preventing security breaches, which helps to mitigate the monetary losses of cybersecurity incidents.⁶⁷ With respect to the November 2024 proposal, the Agency notes: "The direct benefits to California businesses of a 12.6% reduction of these seven cybercrimes are estimated to be approximately \$1.5 billion in 2027 and \$66.3 billion in 2036."⁶⁸

As far as non-monetary costs and benefits, the Agency acknowledges that the benefits to consumers, competition, health, safety, welfare, and quality of life are difficult to quantify.⁶⁹ The Agency explained that these benefits include "avoiding the physical, reputational, and psychological harm that results from unauthorized access, destruction, use, modification, or disclosure of PI; and from unauthorized activity that results in the loss of availability of PI. The unquantified benefits include avoiding the social and psychological costs of identity theft and fraud, such as fear, anxiety, stress, and other inconveniences."⁷⁰ Other benefits include increased transparency and awareness, which leads to consumers becoming more informed about their rights. This awareness leads to more consumer control over their personal information, which leads to increased quality, accuracy, and efficiency of data that firms use.⁷¹

⁶⁷ *Id.* at 70.

⁶⁸ *Id.* at 77.

⁶⁹ *Id.* at 64.

⁷⁰ *Id.* at 81.

⁷¹ *Id.* at 81.

Businesses and the economy also benefit from regulation in ways that are difficult to quantify. Businesses gain more guidance about compliance and lower costs of consumer privacy by standardizing their processes. Businesses will benefit from more trust and loyalty from consumers, as well as increased reputation, which leads to more potential customers.⁷²

Moreover, there are also real costs, monetary and otherwise, to not implementing privacy-protective regulations. The Agency was right to determine that promulgating the November 2024 proposed regulations would work more benefits than harms—and it should still trust that conclusion now.

Industry Argument: Regulation stifles innovation.

This argument is one that the tech industry and their lobbyists raise in any situation where any government is considering any meaningful regulation; this rulemaking process is no exception. However, it is an argument that falls flat. Regulation actually can promote innovation; regulation and innovating are not opposing ideas. The status quo allows tech giants to move fast and break things. Regulations can make the largest players' business practices fairer to competitors and less harmful to consumers, which in turn promotes competition and innovation. For example, Apple has been named the most innovative company in the world, “due in part to its creativity in developing features that assist in user privacy and security.”⁷³

Innovation without proper safeguards is reckless, as we have seen time and time again. Innovation just for innovation's sake, or at the expense of privacy, is not something worth striving for. This is the exact problem that the Agency is supposed to address: the un- and under-regulated

⁷² *Id.* at 82.

⁷³ Calli Schroeder, Ben Winters, & John Davisson, *We Can Work It Out: The False Conflict Between Data Protection and Innovation*, 20 Colo. Tech. L. J. 251, 259, citing *Most Innovative Companies Apple*, Fast Company, <https://www.fastcompany.com/company/apple> [<https://perma.cc/DRG7-49XE>] (last visited Mar. 7, 2022).

industry practices that harm consumers. If a practice is built on harming consumers, that practice should be slowed down or halted, and other, less harmful practices should be adopted instead. Innovation should be steered toward practices that protect consumer privacy while providing desirable products and services. This privacy-protective, thoughtful progress is the type of innovation that regulations like the CPPA’s November 2024 proposal should and do incentivize.

III. Cybersecurity Regulations

The previous iteration of the proposed regulations on cybersecurity were strong, as EPIC noted in its February 2025 comments.⁷⁴ While the proposed regulations are still strong, the revisions weaken the requirements. There are four main issues that weaken the proposed regulations and ultimately harm consumer privacy: (1) the regulations remove Board oversight of cybersecurity audits; (2) the regulations no longer require businesses to explain why certain cybersecurity components are not necessary to implement and why other safeguards provide equivalent protections; (3) the definition of “security incident” has been changed from one that “actually or potentially jeopardizes” to one that “actually or imminently jeopardizes” data security, decreasing business readiness to potential security incidents and increasing the potential harm to consumer privacy; and (4) the compliance timelines are pushed back. We suggest that the Agency reinstate the stronger November 2024 requirements.

First, as we stated in the February 2025 comments, requiring the auditor be qualified, objective, and independent is important to ensuring robust cybersecurity audits. Section 7122(a)(3) previously required the auditor to report regarding cybersecurity audit issues directly to the business’s board of directors or governing body, if one exists. Now, the provision requires the highest ranking auditor to report directly to a member of the business’s executive management team

⁷⁴ EPIC CPPA Feb. 2025 Comments.

who does not have direct responsibility for the business's cybersecurity program. Despite the new proposed regulations adding that this structure is "to maintain the auditor's independence," the previous language would have more effectively ensured the auditor's independence by mandating reporting to the board of governing body instead of the executive management team. Further, the original § 7122(f) requirement to submit the cybersecurity audit report to the board of directors or governing body has been watered down to require submission to the executive team with direct responsibility for the business's cybersecurity program. The business management team that directly oversees the business's cybersecurity program may be incentivized to minimize adverse cybersecurity audit findings or issue a negative performance review of the auditor for doing their job. Requiring reporting to the board of the governing body that is incentivized to ensure compliance and is not directly in charge of the auditing team would have encouraged more independent, objective, and robust cybersecurity audits. The CPPA should reinstate the previous language for those provisions.

Second, the new proposed regulations also diminish the scope of the cybersecurity audit. § 7123(b)(2) removes the language that required the audit to document and explain why if any components of a cybersecurity program listed in § 7123(c) is not necessary to the business's protection of personal information and how the safeguards the business does have in place provide at least equivalent security. The components listed in § 7123(c) include important and commonly implemented cybersecurity measures, such as multi-factor authentication, strong passwords, encryption, limiting account privileges, inventory and management of personal information and the business's information system, and secure configuration of hardware and software. If a business is not utilizing any of such cybersecurity components, it should have to explain why and how it implements equivalent or better security, or why such a basic component is not relevant. Instead, the new language allows for gaps in the auditing process, leaving fundamental components of

cybersecurity unaddressed without any explanation as to why they were deemed not applicable. Silence regarding a component signals inadequacy of the business's practices regarding that component. If the regulations are to allow for audits with such gaps, they should also include a presumption that when an incident occurs for which the omitted component could have served as a safeguard, the businesses practices as they related to the omitted component were not adequate, as they were not described in the audit.

Third, in § 7123(c), which outlines the components that the cybersecurity audit must assess, the definition of “security incidents” has changed to allow less proactive assessment of how the business responds to security incidents. The definition of “security incident” was changed from an occurrence that “actually or *potentially*” (emphasis added) jeopardized the security of data, including unauthorized access, destruction, use, modification, or disclosure of personal information, to an occurrence that “actually or *imminently*” jeopardized the security of data. This change narrows the range of potential cybersecurity threats that the audit will assess in terms of how the business manages its responses. Thus, businesses can limit developing incident response measures to highest priority threats—including through documentation of predetermined instructions or procedures to detect, respond to, limit the consequences of, and recover from malicious attacks—while going unprepared for non-imminent potential threats. This would ultimately leave businesses less prepared to respond to incidents and jeopardize consumer privacy in the end. Custodians of consumer data can more effectively mitigate the severity of a potential security incident when the trigger to respond is potential jeopardy rather than imminent jeopardy—and the agency's cybersecurity regulations should reflect that.

Finally, the November 2024 proposal required each business to complete its cybersecurity audit within 2 years of the effective date of the regulations. Assuming that the regulations would have become final in the fall of 2025, cybersecurity audits would have been due for all covered

businesses by fall of 2027. Under the new proposed regulations, the soonest the cybersecurity audits will be completed is April 1, 2028, for businesses with annual revenue over \$100 million. For businesses with annual revenue of \$50 million to \$100 million, reporting would not be required until April 1, 2029, and businesses with annual revenue of less than \$50 million would have until April 1, 2030 to comply. That would give businesses in the last group almost 5 years to comply. This significant delay in compliance increases risks to consumer privacy and is unnecessary given that many businesses already comply with some form of cybersecurity audit.

IV. Conclusion

We thank the CPPA for the opportunity to comment on its modified proposed cybersecurity, risk assessment, and ADMT regulations. We urge the Agency to restore and improve upon the proposed regulations it voted to circulate for public comment in November 2024—scarcely six months ago. In an era where technology-driven threats to the public are growing, California has the opportunity to remain a leading light for privacy, data protection, and AI safeguards. The CPPA must resist Big Tech’s efforts to extinguish that light and further entrench its own alarming power. Californians are counting on you.

/s/ John Davisson
Director of Litigation &
Senior Counsel

/s/ Sara Geoghegan
Senior Counsel

/s/ Kara Williams
Counsel

/s/ Mayu Tobin-Miyaji
Law Fellow

Grenda, Rianna@CPPA

From: Hancock, Jeremy <Jeremy.Hancock@experian.com>
Sent: Monday, June 2, 2025 1:51 PM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: Experian - Revsied CPPA Comments on Proposed ADMT Regulations and Updates to CCPA Regulations 06.02.25.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](#)

Please see the attached comments on behalf of Experian.



555 12th St NW, Suite 504
Washington, DC 20004
www.experian.com

June 2, 2025

Via electronic filing

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

California Privacy Protection Agency:

On behalf of Experian, we submit these comments in response to the California Privacy Protection Agency's ("CPPA") or ("Agency") invitation for comment on the proposed updates to the regulations related to cybersecurity audits, risk assessments, automated decisionmaking technology ("ADMT"), and insurance requirements dated May 9, 2025.¹

We appreciate the Agency's incorporation of revisions we provided during the initial comment period and welcome the opportunity to provide further input on the modified regulations. We remain concerned about the breadth of the proposed regulations with respect to ADMT used for a significant decision and its potential impact on commercial credit reporting. To provide greater clarity and avoid disruptions to business credit, we offer a proposed amendment to the regulations.

As implementing regulations under the California Consumer Privacy Act ("CCPA"), the ADMT proposed regulations are subject to the explicit exemptions under the CCPA including the exemption with respect to activities subject to regulation under the Fair Credit Reporting Act, Section 1681 et seq., Title 15 of the United States Code (1798.145(d)(2)). While the proposed regulations are necessarily subject to exemptions in their enabling legislation, they do not clarify how less fulsome exemptions that are specific to certain consumer rights in that statute would carry over to new ADMT. It is unclear, for example, whether ADMT rights, including the right to opt-out, would apply in the context of commercial credit reporting, particularly when the information involved may qualify as personal information as defined under the CCPA. For example, lenders often use commercial credit reports to make decision about extending loans to a business. These reports may contain information considered as personal information because the information is related to an individual's relationship to a business (such as information about the owner, general partner, or guarantor of the business; contact information for

¹ California Privacy Protection Agency, Notice of Proposed Rulemaking (May 9, 2025), located [here](#).

individuals serving as a director or officer to the business; or senior employees designated as the point of contact for a business). Without further clarification, data vital to extending business credit arguably would need to be excluded from such systems or subject to a new ADMT opt-out. This interpretation could significantly disrupt established credit evaluation practices and create uncertainty for both businesses and service providers.

The CCPA already acknowledges and explicitly safeguards against this potential impact on commercial credit reporting by expressly exempting certain personal information used by commercial credit reporting agencies from the right to delete, the right to opt out of sales, and the right to opt out of sharing.² This exemption helps ensure that business-related personal information maintained solely in connection with the subject business and not an individual consumer remains available to validate businesses' management and credit histories. This, in turn, supports the availability and extension of new lines of credit to California businesses seeking to grow. This is particularly vital to small and mid-size companies that rely on these services to access credit. However, the proposed ADMT rules, which do not include rights to opt out of sales or sharing, but rather a right to opt out of ADMT used for significant decisions, do not clearly incorporate the CCPA's commercial credit reporting exception.

To address this issue and clarify that a significant decision does not include commercial credit reporting purposes, we suggest adding the language below.

Proposed Amendment:

(ddd) (7) A significant decision does not include the purposes set forth in 1798.145(o).

Failure to clearly extend the CCPA's commercial credit exception to the ADMT opt-out right could have a detrimental impact on California small businesses. Without access to data that verifies a businesses' management and credit histories, businesses of all sizes may struggle to secure capital needed to develop new products, enter new markets, and innovate. Further, removing information from the California market for commercial credit reporting would not only disrupt established commercial lending practices, but could also hinder the provision of insurance, compliance with Anti-Money Laundering and Know-Your-Customer regulatory requirements, fraud prevention, and more. Subjecting commercial credit data to an ADMT opt-out could make it significantly more difficult and costly for businesses to assess potential partners, clients, or vendors.

* * *

² Cal. Civ. Code § 1798.145(o).



Thank you for this opportunity to provide further input into this rulemaking under the CCPA. We look forward to continuing to work with the Agency on these important matters.

Regards,



Elizabeth T. Oesterle
Senior Vice President, Government Affairs

Grenda, Rianna@CPPA

From: Robert Jackson <rjackson@flexassociation.org>
Sent: Monday, June 2, 2025 4:11 PM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: FLEX Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations.pdf

This Message Is From an Untrusted Sender

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

Report Suspicious

Dear CPPA,



Please find the attached public comment regarding "CCPA Updates Cyber, Risk, ADMT, and Insurance Regulations". We appreciate the opportunity to provide input.

Thank you for your consideration.

Sincerely,
Robby Jackson

Director of Outreach and External Affairs | Flex Association

M: [REDACTED]

Visit our [website](#) and follow us:  

Before the
California Privacy Protection Agency

| | | |
|---|---|---------------------------------|
| In the Matter of |) | |
| |) | |
| CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations |) | Comments on Proposed Rulemaking |
| |) | |

COMMENTS OF THE FLEX ASSOCIATION

INTRODUCTION

The Flex Association (“Flex”)¹ respectfully submits these comments in response to the California Privacy Protection Agency’s (the “Agency”) rulemaking on “CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology, and Insurance Companies.”² Flex appreciates the revisions the Agency made to the rules, which addressed some of our concerns with the original draft. But Flex respectfully urges the Agency to address some outstanding issues with the rules by (1) narrowing the rules to remain within the Agency’s privacy mandate and (2) refraining from adopting requirements that would overburden innovation or impede the day-to-day operations of app-based platforms. Such an approach would enable the Agency to promote the privacy rights of Californians while also supporting Flex members in delivering the app-based platform industry’s immense benefits to individual Californians and the state’s economy.

Millions of individuals (including 870,000 Californians as of 2022)—from parents and caregivers to veterans, students, and entrepreneurs—have turned to app-based delivery and rideshare platforms for earning opportunities on their own terms.³ App-based platforms have provided earning opportunities for

¹ The Flex Association (<https://www.flexassociation.org>) (“Flex”) is the voice of the app-based economy, representing America’s leading app-based rideshare and delivery platforms and the people who count on them. Our member companies—DoorDash, Grubhub, HopSkipDrive, Instacart, Lyft, Shipt, and Uber—help provide access to crucial goods and services to customers safely and efficiently, offer flexible earning opportunities to workers, and support economic growth in communities across the country.

² California Privacy Protection Agency, Notice of Proposed Rulemaking: Updates to existing CCPA regulations; Cybersecurity Audits; Risk Assessments; Automated Decisionmaking Technology, and Insurance Companies, https://cppa.ca.gov/regulations/ccpa_updates.html.

³ Public First, [U.S. App-Based Rideshare and Delivery: Economic Impact Report](#) (March 2024) (hereinafter “Public First Report”).



App-Based Industry Impact California

► CALIFORNIA | ECONOMIC IMPACT

\$38B

economic impact
for California

870,000

active app-based
workers in California

46%

of Californians have
earned income on
app-based platforms

► CALIFORNIA | CONSUMER VALUE

660M

app-based platform
transactions in California

76%

of Californians have used
app-based platforms
as a customer

nearly
170

app-based transactions
for every ten Californians

workers, including for those that have historically been left on the economic sidelines.⁴ In California alone, app-based platforms contribute \$38 billion annually in economic value—and across the country, the industry generates an additional \$32 billion in revenue for restaurants, grocers, and other local businesses.⁵

⁴ App-based platforms provide opportunities for individuals who are precluded from traditional W-2 employment (whether that be attributable to chronic illness, disabilities, caregiving or parental responsibilities, or other realities) to earn income. A recent study estimates that there are approximately 1.52 million people who choose independent contractor work for this reason. See Shapiro, Robert and Stuttgen, Luke, [The Many Ways Americans Work and the Costs of Treating Independent Contractors as Employees](#) (April 2022).

⁵ Public First Report. The data below is from the Public First Report as well as Morning Consult survey data, both of which are available at flexassociation.org. For further discussion on how app-based platforms operate a three-sided marketplace that unlocks value for consumers (the buyers), local businesses (the suppliers), and workers (who deliver the goods), see [Flex Explainer | How Three-Sided Marketplaces Work for All](#) (2024).

App-based work also boosts entrepreneurial activity, which is especially important to California's creator economy.⁶ These platforms are helping communities to tackle food insecurity,⁷ provide more equitable healthcare,⁸ and recover from natural disasters,⁹ including the wildfires in Southern California this year.¹⁰ App-based platforms are using their scale to innovate and drive progress on sustainability issues, thanks to data-driven initiatives that find ways to reduce emissions, minimize environmental impacts, adopt sustainability practices, and foster partnerships with key stakeholders and local programs.¹¹ App-based platforms have also advanced the safety of earners, communities, and consumers, including via the use of automated technologies.¹²

App-based platforms use data to provide the services that connect millions of consumers, app-based earners, and local businesses every day. This industry takes protecting that information seriously, with commitments to respecting privacy and safeguarding data. In addition, Flex member companies use technology to support and power many day-to-day aspects of their operations, including features that promote safety, efficiency, and sustainability. Tapping the power of data and technology is key to supporting these valuable features and the development of new innovations.

⁶ Rice University found a 7% to 12% increase in entrepreneurial interest after the arrival of rideshare platforms in a community, attributed to the safety net that app-based work provides while people pursue their goals. John M. Barrios et al., [Launching with a parachute: The gig economy and new business formation](#), JOURNAL OF FINANCIAL ECONOMICS (April 2022), Volume 144, Issue 1, 2022.

⁷ See David Downey, [California city first in US to partner with DoorDash to deliver food to hungry households](#), The Mercury News (Nov. 3, 2022); Instacart, [Instacart Launches Community Carts, Enabling Online Grocery Donations to Food Banks Nationwide in Just a Few Taps](#) (Nov. 29, 2022).

⁸ See [Walgreens, Partners with DoorDash and Uber Health to Provide Free Paxlovid Delivery](#) (Oct. 25, 2022) (noting that “[f]ree delivery will help accelerate access to COVID-19 treatment for communities across America with a focus on underserved populations.”).

⁹ Flex Association, [App-Based Platforms | Preparing, Responding, and Recovering from Natural Disasters](#) (2024).

¹⁰ Flex Association, [LinkedIn post](#) (January 2025).

¹¹ Flex Association, [Scaling for Good: How App-Based Platforms Advance Environmental Sustainability](#) (Fall 2024).

¹² Flex Association, [Comments, White House Office of Science and Technology Policy Request for Information](#), May 1, 2023 (hereinafter Flex WH OSTP Comments). (Citing, for instance, how advanced telematics are producing insights that help encourage safer driving behaviors and how “rideshare platforms monitor for instances of unusual activities, such as long stops and route abnormalities. A rider and driver will receive an automatic message should either of these be detected, which will inquire whether help is needed. Riders and drivers can also use an in-app emergency button to call authorities in the event of an emergency, which will allow for sharing of location and trip details. Drivers and riders alike may also allow friends and families to follow their route remotely for an added layer of peace of mind (or just to follow along with their trip).”).

To avoid overburdening the use of technology to make everyday decisions or inhibiting innovation while promoting privacy protections, we respectfully recommend targeted modifications to the Agency’s revised draft of the rules. These modifications would help to ensure that the rules protect the interests of Californians—and the State of California—by fostering safe, productive, and valuable use of data and new technologies like ADMT. Specifically, Flex urges the Agency to:

- A. Narrow the “significant decision” and “ADMT” definitions to cover only truly high-risk decisions that pose a real threat to consumer privacy and exclude scenarios in which a human has oversight over the decision. For example, “significant decision” should be properly scoped as a decision that has a legal or material effect on an individual’s life, such as approving or denying a home loan, and that poses a significant risk to consumer privacy, while “automated decisionmaking technology” should, as the name says, be focused on decisionmaking that occurs without human involvement or oversight.

Day-to-day decisions about contract work are not, and should not count as, “significant.”

- B. Add to the “opt-out” provisions a robust broad exception for processing that is necessary to perform a service requested by the consumer. The “opt-out” requirements pose a serious obstacle to functionality, and the proposed exceptions in § 7221(b) are too narrow and contain requirements too disconnected from consumer privacy protection to fall under the Agency’s mission or serve its purposes.

A. App-Based Platforms’ Use of Technology for Basic, Day-to-Day Functions Are Not “Significant Decisions.”

The Agency should rework proposals that would expansively regulate technologies that many entities, including app-based platforms, use for day-to-day operations, subjecting the basic functions of app-based platforms to burdensome and inapt obligations—without corresponding privacy benefits. The proposed rules would impose requirements on businesses when they use technology to help make “a significant decision concerning a consumer,” and “significant decisions” are defined to include decisions

about “employment or independent contracting opportunities or compensation.”¹³ But the rules would not confine “significant decisions” to events that *may be truly significant* to consumers, like decisions about hiring and firing. Rather, the rules would include uses of ADMT to make those kinds of everyday decisions about “allocation or assignment of work” not on the same plane as a decision to fire a worker, or a decision to deny someone housing, credit, or healthcare.

But that same problem continues to exist for some of the other examples of “employment or independent contracting opportunities or compensation” that remain in this revised draft of the rules. In particular, when it comes to compensation- or benefits-related decisions, the rules still do not distinguish between the truly significant decisions (like choosing the salary to offer a new worker) and the everyday decisions that are not (like performance bonuses, small incentive payments, or other workplace benefits).

As we mentioned in our previous comments, in California alone in a single year, Flex member companies facilitated 660 million transactions.¹⁴ The revised draft of the rules continues to treat every one of those hundreds of millions of transactions—which often last mere minutes—as “significant”, because every one of those transactions necessarily requires calculating an amount of “per-assignment compensation” to offer. Not only that, but many of those individual transactions may consist of a tree of “significant” decisions, with branches for any “bonus” or “incentive compensation” that might go along with each transaction. Offering bonus or incentive compensation is common, because app-based workers—as independent contractors—cannot be told what work to do. Offering a bonus or incentive may be the only way to find a worker willing to agree to take on a job, and under the revised draft, those decisions too—no matter the amount of money involved—are all labeled “significant.” So those 660 million transactions actually involve, under this proposed definition, billions of “significant” decisions. Common sense says that decisions that happen billions of times per year in California alone cannot all be “significant.” It would make little sense to treat day-to-day (and minute-to-minute) decisions about how

¹³ § 7001(ddd)(4).

¹⁴ Public First Report. In addition, 76% of Californians have used app-based platforms as a customer. Flex, [App-Based Industry Impact | California](#).

much to offer a worker to complete a job that often lasts minutes as a “significant decision” on par with using automated technology to make a decision that would deny an individual healthcare or housing.

This is a problem that is not unique to app-based workers. Employees are commonly offered bonuses, incentives, or other “benefits” for routine activities in the workplace, be it on-time rates, sales quotas, production metrics, customer feedback, or hours committed to a project. The calculation and payment of these types of benefits often are automated precisely because they are not significant workplace decisions.

Not only do these kinds of day-to-day decisions fall outside the scope of the truly “significant,” they also do not have any meaningful nexus to consumer privacy. Whether it’s an employer offering incentive payments for employees who meet key sales targets, or an app-based delivery platform offering an extra bonus for each assignment because the consumer demand for deliveries at that moment is outstripping the workers choosing to take on that work, those decisions do not present privacy risks—let alone the significant privacy risks the Agency is tasked with regulating. We urge the Agency to instead focus the ADMT rules on situations with a close nexus to privacy that involve materially consequential, real-world impacts on individuals. Doing so will allow innovation to continue, resulting in better services for consumers and greater economic opportunity for Californians.

B. Allowing Users to “Opt Out” of ADMT Would Impair the Functionality of App-Based Platforms.

The final rules should omit the opt-out requirement as the proposed rule provision allowing users of a service to opt out of ADMT will simply not work in the context of app-based platforms.¹⁵ On app-based platforms, ADMT makes possible—quickly and efficiently—critical features, such as identity verification, connecting users with app-based workers, estimating wait times, inputting taxes/fees, and calculating best routes. Enabling app-based workers or consumers to “opt out of ADMT” will effectively mean opting out of using the platform, or perhaps worse, opting out of features that are instrumental to the

¹⁵ § 7221.

experience they have come to expect and rely upon, including features that promote safety.¹⁶ For example, under the proposed rule, app-based workers could opt out of features like verification, which aids overall safety, or automated route calculation, which aids shorter wait times for consumers, improves efficiency and earning opportunities, and can be leveraged to support sustainability goals by prioritizing routes that are energy efficient.

For example, delivery platforms use technology to estimate the duration of every leg of a given delivery, considering specifics pertaining to merchant partner, time of day, geographic and local realities, and traffic. Automated technologies can process real-time and historical data to estimate the duration of a delivery from start to finish, as well as the duration of every sub-milestone of that delivery (e.g., time it takes to travel to a restaurant, pick up an order, and travel to the consumer). This model allows platforms to account for variables including restaurant preparation speed, restaurant location relative to a potential worker, and on the ground traffic patterns. These calculations help offer workers a delivery that promises the most efficient use of their time. In turn, this enables workers to pick from offers that minimize the time they spend waiting for an order, which allows them to spend more time earning. It also provides users with an accurate estimation of delivery and facilitates efficient service provision, which is good both for California consumers and the California restaurants, local merchants, and other small businesses who have chosen to use these platforms to get their products to consumers. At the same time, use of automated traffic data improves worker safety by providing realistic delivery timeframes that reflect real-time road conditions and the other variables that impact delivery duration.¹⁷

As another example, rideshare platforms rely on ADMT-based methods for matching a driver to a rider that are indispensable to the platform's functionality. These methods have become increasingly efficient, and their development is essential to a platform's ability to compete for workers, consumers, and

¹⁶ Although § 7221(b)(1)(A) provides an exception from the opt-out requirement for safety features, the exception is impracticably narrow, only applying when the feature is "necessary to achieve, and used solely for," the safety purpose, failing to account for how app features typically serve many purposes at once. The uncertainty of when the exception applies could also hinder innovation.

¹⁷ Flex WH OSTP Comments at 4.

businesses.¹⁸ In the early years of app-based platforms, riders and drivers were matched based on the geographically closest available driver. While this approach often worked, some users experienced longer wait times, and the closest did not always mean the most efficient. In response, platforms have deployed ADMT to flexibly assess underlying data such as location, road and infrastructure signals, and traffic patterns to match riders with the most suited driver. These models have resulted in a user experience that has often resulted in drivers earning more by minimizing the wait time between rides while maximizing the ability to match all users in a given area with streamlined and reliable service options. If drivers were to opt out of this allocation system, the functionality of these more efficient and pro-worker platform advances would be jeopardized.

Although proposed § 7221(b)(3) provides an exception from the opt-out requirements for when a business is using ADMT for task allocation, unfortunately, there is no opt out exception for promotion, demotion, suspension, and termination, and exceptions remain too narrow, creating operation difficulties and unintended consequences that could harm consumers. Plus, concerns about the “accuracy” of these systems and risks of discrimination do not involve material privacy interests. Requiring vague accuracy and non-discrimination safeguards is unnecessary, inconsistent with the Agency’s mandate and other state laws, and overly burdensome on businesses—like app-based platforms—that use automated task allocation to provide consumers with efficient and reliable services.

The language of this exception is also vague and will likely require additional rulemakings by the Agency to clarify the scope of an accuracy evaluation (i.e., what such an evaluation must cover). This will create further confusion and uncertainty by leading to inconsistent interpretations and applications by similarly situated companies and potentially different outcomes for consumers as they engage with multiple service providers.

¹⁸ See, e.g., Uber, [How does Uber match riders with drivers](#) (hereinafter “Uber, Marketplace matching”); Douriez, Marie and Murphy, James and Staley, Kerrick, Lyft Engineering, [A new Real-Time Map-Matching Algorithm at Lyft](#) (August 11, 2020).

CONCLUSION

Flex welcomes the opportunity to participate in this proceeding. Many of the proposed rules' requirements and definitions are overly broad, prescriptive, and impractical, making them impossible or unworkable to implement in the app-based platform context without seriously undermining the services' functionality and benefits to users. The Agency should reevaluate its proposals to consider impacts on this important segment of the economy and to ensure that the benefits of app-based platform services can continue to be enjoyed by Californians today and in the future.

Respectfully submitted,

/s/ Robert Jackson

Robert Jackson

Director, External Affairs

Flex Association

<https://www.flexassociation.org/>

June 2, 2025

Grenda, Rianna@CPPA

From: Gebriel Saleh <[REDACTED]>
Sent: Monday, May 19, 2025 11:09 AM
To: Regulations@CPPA
Subject: NOTICE OF MODIFICATIONS TO PROPOSED TEXT (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations)

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](#)

Good Morning!

I had a quick question regarding the proposed regulations in regards to the scope of ADMT, or Automated Decisions-Making Technology. Would the following example fall under the scope/definition of ADMT?

- Suppose a fuel delivery company utilizes AI to monitor truck driver routes, stops and behavior, and automatically flags them for further supervision review - would this fall under the definition of ADMT?

Thank you so much for your clarification, and I'm looking forward to your response!

Best Regards,
Gebriel Saleh
Undergraduate Student | Department of Economics
University of California, Davis
[REDACTED]

Grenda, Rianna@CPPA

From: Wexler, Emma A <EWexler@gibsondunn.com>
Sent: Monday, June 2, 2025 4:56 PM
To: Regulations@CPPA
Cc: Beringer, Ashlie
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: June 2 Gibson Dunn Comment on Proposed CCPA 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

Please find attached comments on the CCPA Updates, Cyber, Risk, and ADMT Regulations.

Thank you,

Emma Wexler
Associate Attorney

T: +1 650.849.5222
EWexler@gibsondunn.com

GIBSON DUNN
Gibson, Dunn & Crutcher LLP
310 University Avenue, Palo Alto, CA 94301-1744

This message may contain confidential and privileged information for the sole use of the intended recipient. Any review, disclosure, distribution by others or forwarding without express permission is strictly prohibited. If it has been sent to you in error, please reply to advise the sender of the error and then immediately delete this message.

Please see our website at <https://www.gibsondunn.com/> for information regarding the firm and/or our privacy policy.

California Privacy Protection Agency
Attn: Legal Division – Public Comment Regarding CCPA Updates, Cyber, Risk, and ADMT
Regulations
2101 Arena Blvd.
Sacramento, CA 95834
regulations@coppa.ca.gov

June 2, 2025

To the Leadership Team and Board of the California Privacy Protection Agency:

We write on behalf of Gibson, Dunn & Crutcher LLP's Privacy, Cybersecurity, and Data Innovation; Artificial Intelligence; and Tech and Innovation practice groups.¹ We appreciate the Agency's work and thoughtful response to the comments and concerns raised in response to the prior draft of the CCPA regulations on risk assessments and automated decisionmaking technology ("ADMT"). The May 9, 2025 Draft ("May 9 Draft") represents a substantial improvement over the prior version in many respects, addressing several of the concerns raised in our prior letter dated February 19, 2025 (attached for reference).

Although significantly improved, the May 9 Draft creates a few new issues that raise potentially significant concerns that we urge the Agency to address. Our comments and recommendations below are in line with the recent steps the Agency has taken to better strike the balance between furthering its mission of protecting consumer privacy and security without unduly burdening innovation and growth in California. These recommendations would clarify the law for California businesses and ensure the regulations stay true to the intent behind the CCPA² and the grant of authority to promulgate the regulations.

First, we recommend further clarifying that profiling qualifies as automated decisionmaking only to the extent it replaces human decisionmaking. The May 9 Draft defines ADMT to mean "any technology that processes personal information and uses computation *to replace human decisionmaking or substantially replace human decisionmaking.*"³ After defining the criteria for evaluating whether a technology "substantially replace[s] human decisionmaking," the regulations go on to state that "ADMT includes profiling."⁴ As currently drafted, the regulations could be

¹ We offer these comments on our own behalf, and our views may not reflect the views of all our clients.

² As amended by the California Privacy Rights Act ("CPRA").

³ Modified Text of Proposed Regulations (Cal. Priv. Prot. Agency, May 9, 2025) (hereafter May 9 Draft), § 7001, subd. (e) (emphasis added).

⁴ *Id.* at § 7001, subd. (e)(2).

misinterpreted to suggest that all profiling should be deemed ADMT whether or not it replaces human decisionmaking—that is, whether or not a profiling activity actually meets the definition of ADMT.

That cannot be the effect, because, as discussed in our prior comment, the authority granted to the Agency is limited to regulating “automated decisionmaking,” namely, decisions *not* made by humans.⁵ Necessarily, then, the regulation of profiling under the ADMT portion of the regulations is subject to the limitations contained in the enabling grant. Indeed, the plain language and structure of the enabling law authorizing the Agency to regulate ADMT makes clear that “profiling” is a type of ADMT, not an extra, freestanding topic for regulation. Specifically, the provision instructs the Agency to “[i]ssu[e] regulations governing ... automated decisionmaking technology, *including* profiling.”⁶ The law thus treats profiling as a *subset* of automated decisionmaking, not as a standalone ground for regulation. Further, the same provision references “automated decisionmaking technology, including profiling” as “decisionmaking processes, which reinforces that “profiling” only qualifies as ADMT to the extent it is used to make automated, non-human decisions. In other words, “profiling” is only within the scope of the enabling grant (and thus, the regulations) if it otherwise qualifies as ADMT.

We therefore believe the Agency intended the reference to profiling in Section 7001(e)(2) to track the statutory language: to be illustrative, but not override the statutory definition or extend the ADMT portion of the regulations to cover things that are not ADMT. That is, the intent of the draft regulations cannot be—and the draft regulations are not authorized—to subject everyday human-led business practices (like generating automated reports of employee performance for human-led year-end reviews or of financial information for human-led profiling by loan officers) to the extensive requirements that apply to ADMT, such as an opt-out (or human appeal).⁷

Because Section 7001(e)(2) could be misinterpreted, however, we propose that the Agency explicitly state that profiling is ADMT only to the extent it replaces or substantially replaces human decisionmaking, consistent with the approach taken in the subsection that immediately follows, which identifies several types of technology that are not ADMT “provided that they do not replace human decisionmaking.”⁸

Specifically, we propose the following clarifying revision:

- (1) Section 7001(e)(2): “ADMT includes profiling that replaces or substantially replaces human decisionmaking.”

⁵ See Gibson Dunn Comment on Proposed CCPA Regulations at pp. 3–6.

⁶ Civ. Code § 1798.185, subd. (a)(15) (emphasis added).

⁷ May 9 Draft, § 7221.

⁸ *Id.* at § 7001, subd. (e)(3).

Second, we strongly recommend **restoring the fraud exception to the requirement to provide opt-out rights from ADMT to fulfill the statutory purpose of protecting the personal information of Californians**. One of the core purposes of the CCPA and CPRA amendments is to strengthen the security of personal information and the systems where personal information is stored.⁹ This is reflected in various exceptions to the regulations, where specific requirements could hinder rather than advance data security by creating opportunities for abuse by malicious actors. For example, we commend you for clarifying that when businesses respond to a request to access ADMT, they need not provide information that would compromise efforts to keep user information secure.¹⁰ At the same time, the May 9 Draft inexplicably removes—without comment or explanation—the provision from the prior draft establishing that consumers could not opt out of ADMT used solely for “security, fraud prevention, or safety purposes.”¹¹ That exception is critical to the protection and security of personal data and related business systems, and we recommend restoring it as previously written. Indeed, we are not aware of *any* comments that suggested removing this exception wholesale from the regulations in the prior round of comments or any reason that could justify doing so.

Automated decisionmaking technology is an essential tool for preventing fraud that accomplishes nothing when fraudsters or hackers may freely opt out of it. In recent years, governments and businesses have witnessed increasingly sophisticated attempts to infiltrate their systems to steal money and user information.¹² These accelerating threats require an equally sophisticated response, including the use of innovative automated tools to detect and respond to potential events and thwart criminals. Requiring businesses to offer an opt-out to malicious actors defeats the

⁹ See Gibson Dunn Comment on Proposed CCPA Regulations at pp. 2-3, 7.

¹⁰ *Id.* at § 7222, subd. (c).

¹¹ Proposed Text of Regulations (Cal. Priv. Prot. Agency, Nov. 2024), § 7221, subd. (b)(1) included the following exception:

“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.”

¹² See, e.g., Dilanian et. al., “*Easy Money*”: *How international scam artists pulled off an epic theft of Covid benefits* (Aug. 15, 2021) NBC News, <https://www.nbcnews.com/news/us-news/easy-money-how-international-scam-artists-pulled-epic-theft-covid-n1276789>; Kelly, *Fake Job Seekers Are Exploiting AI To Scam Job Hunters And Businesses* (Apr. 11, 2025) Forbes, <https://www.forbes.com/sites/jackkelly/2025/04/11/fake-job-seekers-are-exploiting-ai-to-scam-job-hunters-and-businesses>.

point. Would-be criminals could easily avail themselves of any opt-out, undermining the efficacy of systems designed to prevent fraud and protect personal data. And the contemplated other alternative—giving everyone the right to a human appeal—makes no sense in the context of fraud and security prevention. One of the main points of using ADMT for these applications is because humans are vulnerable to fraudulent conduct like social engineering that automated systems are less likely to be fooled by.¹³ Further, automated fraud detection tools can have substantial benefits to consumers beyond protecting their accounts and information: they can reduce false positives by taking a more nuanced view of what constitutes a suspicious transaction and thus reduce the cost of anti-fraud measures, resulting in cost savings to consumers.¹⁴

In fact, the Agency itself previously recognized the importance of the fraud and security exception, noting that it is “necessary to preserve businesses’ ability to protect themselves and consumers” and “consistent with similar exemptions in the existing right to limit the use of sensitive personal information.”¹⁵ Similarly, service providers are granted a right to use consumer personal information for security and fraud prevention under the existing regulations,¹⁶ and businesses can use personal information provided for request verification purposes for security or fraud prevention.¹⁷ Other States, recognizing these concerns, cabin any right to opt out of ADMT with an exception for security procedures, consistent with the prior drafts of the ADMT regulations.¹⁸

¹³ Chitrakar, *Redefining email security with LLMs to tackle a new era of social engineering* (Nov 19, 2024) Microsoft,

<https://techcommunity.microsoft.com/blog/microsoftdefenderforoffice365blog/microsoft-ignite-redefining-email-security-with-llms-to-tackle-a-new-era-of-soci/4302421>.

¹⁴ Reddy et al., *Effective Fraud Detection in E-Commerce: Leveraging Machine Learning and Big Data Analytics* (Jun. 2024) 33 Measurement: Sensors,

<https://www.sciencedirect.com/science/article/pii/S2665917424001144>; *How machine learning works for payment fraud detection and prevention* (Jan. 23, 2025) Stripe, <https://stripe.com/resources/more/how-machine-learning-works-for-payment-fraud-detection-and-prevention>; Business Wire, *Riskified Unveils Adaptive Checkout: AI Fraud Prevention That Maximizes Ecommerce Conversion Rates* (Mar. 5, 2025) Fintech Futures, <https://www.fintechfutures.com/press-releases/riskified-unveils-adaptive-checkout-ai-fraud-prevention-that-maximizes-ecommerce-conversion-rates>.

¹⁵ California Privacy Protection Agency, Initial Statement of Reasons (Nov. 2024) at p. 87.

¹⁶ Cal. Code Regs., tit. 11, § 7050, subd. (a)(4).

¹⁷ *Id.* at § 7060, subd. (d).

¹⁸ For example, the Virginia Consumer Data Privacy Act: “nothing in this chapter shall be construed to restrict a controller’s or processor’s ability to . . . [p]revent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity” (Va. Code Ann., § 59.1-582, subd. (A)(7)). All other comprehensive state privacy laws include an exception for security and fraud prevention similar to Virginia’s. See also, e.g., Colo. Rev. Stat. Ann., § 6-1-1304, subd. (3)(a)(X); Conn. Gen. Stat. Ann., § 42-524, subd. (a)(9); 6 Del. C., § 12D-110, subd. (a)(9); Ind. Code, § 24-15-8-1, subd. (a)(7); Iowa Code Ann., § 715D.7, subds. (1)(g)-(i); Ky. House Bill No. 15 (2024 Reg. Sess.), § 8, subd. (1)(i); Md. Code Ann., Com. Law, § 14-4712, subds. (a)(9), (10); Minn. Stat. Ann., § 325O.09, subd. (a)(7); Mont. Code Ann., § 30-14-2816, subd. (1)(i); Neb. Rev. Stat., § 87-1126, subd. (1)(g), (h); N.H. Rev. Stat., § 507-H:10, subd. (I)(i); NJ Rev. Stat., § 56:8-166.15, subd. (a)(9); Or.

And the CCPA itself contains both an exception to the right to delete for “security and integrity” purposes,¹⁹ and a broad exception to various obligations to “defend legal claims,” which would include legal claims pertaining to alleged fraudulent activity.²⁰

Given the Agency’s recognition of the importance of the fraud and security exception and the numerous related exceptions to other requirements in the CCPA, we believe the omission of the exception in the current draft may have been an oversight. Nevertheless, the May 9 Draft enumerates the exceptions to the right to opt out of ADMT in Section 7221(b) but does not include any exception for fraud, security, or safety applications, leaving California businesses in the perilous position of having to guess whether critical defensive uses of technology are subject to these requirements. To encourage effective countermeasures to a rising tide of consumer threats and ensure parity with other jurisdictions that do not require loopholes for equivalent requirements, we request that the Agency restore an explicit fraud, security, and safety exception to ADMT opt-outs.

To do otherwise would also conflict with federal law. Under the Cybersecurity Information Sharing Act of 2015 (“CISA”), “a private entity may, for cybersecurity purposes, operate a defensive measure that is applied to” its own (or on request, another’s) “information system” to protect “rights or property.”²¹ This law applies “[n]otwithstanding any other provision of law”—that is, it preempts state laws to the contrary.²² CISA thus guarantees private businesses the right to deploy defensive measures—including automated decisionmaking systems—to prevent security breaches and fraud.²³ The May 9 Draft, by requiring an opt-out that would undermine the efficacy of certain defensive measures, would impede private businesses from exercising this federally guaranteed right. Unless the final regulations are updated to restore the fraud, security, and safety exception, they will conflict with federal law and be preempted in at least some, if not all, cases. To forestall this conflict, the fraud exception should be restored.

Third, the definition of “significant decisions” should be limited to decisions that are actually material. We appreciate that the Agency has substantially narrowed the definition of “significant decision” to better align the regulations with the CCPA and reduce the extensive burdens these regulations will impose on California businesses. But it still encompasses instances of immaterial

Rev. Stat. § 646A.572, subd. (3)(e), (f); R.I. Gen. Laws, § 6-48.1-7, subd. (o)(9); Tenn. Code, § 47-18-3309, subd. (a)(7); Tex. Bus. & Com. Code Ann., § 541.201, subds. (a)(6), (7); Utah Code, § 13-61-304, subds. (1)(h), (i).

¹⁹ Civ. Code, § 1798.105, subd. (d)(2).

²⁰ Civ. Code, § 1798.145, subd. (a)(1)(E).

²¹ 6 U.S.C. § 1503, subd. (b)(1).

²² *Id.*

²³ A “defensive measure” is any device that “detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability” (6 U.S.C. § 650, subd. (9)).

or trivial conduct that do not have significant impacts on consumers at all, let alone significant impacts on privacy.

The CCPA directs the Agency to issue risk assessment and cybersecurity regulations when businesses' "processing of consumers' personal information presents a *significant* risk to consumers' privacy or security."²⁴ The May 9 Draft states that the use of ADMT "for a significant decision concerning a consumer" "presents a significant risk to consumers' privacy."²⁵ The current definition of "significant decision," however, puts the regulations out of step with both the statutory text and other regulatory regimes. Because the regulations, as drafted, sweep in various decisions that are not "significant," the regulations impose undue burdens on businesses that will stifle economic growth with no discernable benefit to consumer privacy.

For example, as it stands, the definition of significant decisions includes decisions that result in the provision or denial of "healthcare services," which is defined broadly to mean "services related to the diagnosis, prevention, or treatment of human disease or impairment."²⁶ Some of those decisions would be "significant," like denying healthcare coverage to treat a serious condition. But by sweeping in any services "*related to*" the "prevention or treatment of human disease or impairment," the regulations would reach too far, and could include, for example, automated scheduling of gym sessions recommended by a physical therapist.

Similarly, the regulations include a variety of types of compensation and incentives within the scope of "employment or independent contracting opportunities or compensation."²⁷ Some, like an employee's salary or hourly rate, are likely to be significant employment decisions. But again, this provision reaches too far. Treating as "significant" any type of decision about any type of "benefit" sweeps in even minimal or insignificant types of compensation, such as gift cards or discounts businesses might use to reward an employee for hitting a sales target or getting positive customer feedback. So too with the "allocation or assignment of work," "per-assignment compensation" or "incentive compensation." The use of automation to route a particular assignment to an employee who may have the most capacity at a given time, for example, or calculate how to apply an employee's salary or compensation formula to an individual task, is a minor decision that should not be subject to the same extensive regulatory scheme as a decision to fire or demote them.

The May 9 Draft regulations would regulate a broader category of decisions than existing laws, including laws specifically addressing the use of automated decisionmaking in the workplace. The Civil Rights Council, in its own recently released automated decisionmaking regulations, limited

²⁴ Civ. Code, § 1798.185, subd. (a)(14) (emphasis added).

²⁵ May 9 Draft, § 7150, subd. (b)(3).

²⁶ *Id.* at § 7001, subd. (ddd)(5)

²⁷ *Id.* at, § 7001, subd. (ddd)(4)(B).

its definition of “Employment Benefit” to significant impacts to employment, including only training programs that “lead[x] to employment or promotions,” for example.²⁸ And the Colorado AI Act defines “consequential decision” as a “a decision that has a *material* legal or *similarly significant effect* on the provision or denial to any consumer of” certain categories, including employment or employment benefits.²⁹

To avoid a patchwork of inconsistent regulatory obligations and overburdening businesses with risk assessment obligations even when ADMT is used for immaterial decisions—and keep these regulations within the scope of the authorization—the Agency should revise its definition of “significant decisions” to focus, as other laws and regulations do, on material conduct. We suggest:

(1) adding the following language to Section 7001(ddd): “‘Significant decision’ means a decision that results in **a material or similarly significant effect on** the provision or denial of financial or lending services, housing, education enrollment or opportunities, employment or independent contracting opportunities or compensation, or healthcare services,” and

(2) revising Section 7001(ddd)(4)(B) as follows:

“Employment or independent contracting opportunities or compensation” means:

(A) Hiring;

(B) **For employees³⁰, assignments that materially impact hiring, promotion or compensation;** ~~Allocation or assignment of work for employees; or salary, wage, or bonuses, hourly or per assignment compensation, incentive compensation such as a bonus, or another benefit (“allocation/assignment of work and compensation”);~~

²⁸ “Employment Benefit” includes “hiring, employment, promotion, selection for training programs leading to employment or promotions, freedom from disbarment or discharge from employment or a training program, compensation, provision of a discrimination-free workplace, and any other favorable term, condition or privilege of employment” (Final Unmodified Text of Proposed Employment Regulations Regarding Automated-Decision Systems (Civ. Rights Council, Mar. 17, 2025), § 11008, subd. (i)).

²⁹ Colo. Rev. Stat., § 6-1-1701, subd. (3) (emphasis added).

³⁰ As drafted, Section 7001(ddd)(4)(B) appears to exclude from its scope allocation or assignment of work for independent contractors only, while including “per assignment compensation” for both independent contractors and employees. For the reasons discussed, neither the allocation or assignment of work nor per-assignment compensation rise to the level of a significant decision and should not be included in scope of ADMT decisions. To the extent that they are included in revised form, however, the regulations should make clear that both allocation/assignment of work and compensation (which are grouped together as a single defined term in Section 7001(ddd)(4)(B)) are “significant decisions” in the employment context only, but not for independent contractors. Otherwise, the Agency’s appropriate decision to

(C) Promotion; and

(D) Demotion, suspension, and termination.

Fourth, **the requirement of an attestation under penalty of a perjury by a company executive in both the cybersecurity and risk assessment provisions (Sections 7124(d)(4) and 7157(b)(5)) should be removed.** Requiring that cybersecurity audit reports or risk assessment be signed under penalty of perjury is excessive and incongruous with the contents and structure of those documents and will have the effect of weakening the purpose behind this requirement.

Take the risk assessment requirements. Many of the components of a risk assessment do not involve any factual information or, if they do, require significant judgment calls and evaluations in an evolving and novel technological landscape that are not appropriate for an attestation under penalty of perjury. Businesses “must conduct a risk assessment to determine whether the risks to consumers’ privacy from the processing of personal information outweigh the benefits to consumer, the business, other stakeholders, and the public from that same processing.”³¹ The risk assessment must identify “the logic of the ADMT;” “benefits to the business, the consumer, other stakeholders, and the public” in non-generic terms; and “negative impacts to consumers’ privacy,” including (if applicable) economic, reputational, and/or psychological harms.³² The nuanced balancing and judgment that flows from these requirements necessarily will be the product of collaboration across numerous stakeholders, with different perspectives and views on the risks, benefits, and tradeoffs of ADMT. No individual can reasonably attest, under penalty of perjury, to an assessment that requires diverse participation and viewpoints, or that the Agency will agree with how they have weighed the risks and benefits, given the inherent subjectivity in such balancing. And with respect to ADMT specifically, describing the “logic” of the ADMT may, in some contexts, be an impossible task because, in many cases, the logic is just “a long list of numbers.”³³ The cybersecurity audit report similarly must contain an explanation as to “why assessing [certain] policies, procedures, and practices; using [certain] criteria; and examining [certain] specific evidence justif[ies] the auditor’s findings.”³⁴ Such subjective assessments should not be subject to criminal penalties through a penalty of perjury provision.

Moreover, requiring an “executive” to attest will impoverish the quality of the risk assessments and their efficacy, since businesses will be compelled to protect their executives through

exclude numerous individual tasks in an independent contractor setting from the scope of “significant decisions” would be effectively undone by sweeping “hourly or per assignment compensation” relating to those tasks back into the regulations.

³¹ May 9 Draft, § 7152, subd. (a).

³² *Id.* at § 7152, subd. (a)(3)-(6).

³³ Anthropic, *Mapping the Mind of a Large Language Model* (May 21, 2024), <https://www.anthropic.com/research/mapping-mind-language-model>.

³⁴ May 9 Draft, § 7123, subd. (e)(1).

conservative drafting that avoids comment on fluid issues or subjects of debate. Executive attestations are a rare requirement reserved for only the most serious contexts where information can be validated in an objective manner.³⁵

To that end, the attestation requirement should be struck in its entirety. At most, these provisions should be revised to require only a written submission by an individual familiar with and accountable for the cybersecurity audit or risk assessment process confirming that the audit or assessment was completed consistent with the draft regulations.

* * *

We appreciate this opportunity to share some of our remaining concerns and hope that the Agency will revise the proposed regulations in line with the specific recommendations above.

³⁵ For example, the Sarbanes Oxley Act requires an executive to attest to the accuracy of financial statements for public companies as a condition of issuing registered publicly-traded securities. (See 15 U.S.C. § 7241.)

Respectfully submitted,



Ashlie Beringer

Partner

Co-Chair of the Privacy, Cybersecurity and Data Innovation Practice Group



Jane Horvath

Partner

Co-Chair of the Privacy, Cybersecurity and Data Innovation Practice Group



Cassandra Gaedt-Sheckter

Partner

Co-Chair of the Artificial Intelligence Practice Group

Attachment

California Privacy Protection Agency
Attn: Legal Division – Public Comment Regarding CCPA Updates, Cyber, Risk, and ADMT
Regulations
2101 Arena Blvd.
Sacramento, CA 95834
regulations@coppa.ca.gov

February 19, 2025

To the Leadership Team and Board of the California Privacy Protection Agency:

We write on behalf of Gibson Dunn & Crutcher LLP's Privacy, Cybersecurity and Data Innovation, Artificial Intelligence, and Tech and Innovation practice groups. Gibson Dunn is subject to the California Consumer Privacy Act and advises clients in many industries on the continuously evolving regulation of data, privacy, cybersecurity, and artificial intelligence. While we offer these comments on our own behalf, and our views may not reflect the views of all our clients, our team includes several former executives at technology companies, and our collective experiences give us unique insight into the practical implications of regulations targeting data practices and technology.

While we appreciate the need for sound regulation, we have significant concerns with the Agency's proposed regulations under the CCPA¹ to govern automated decisionmaking technology ("ADMT"), risk assessments, and cybersecurity audits. As the global epicenter of information technology and artificial intelligence, California has delivered tremendous benefits to society. These benefits are a direct product of Californians' ability to creatively innovate using data and technology. As drafted, however, the proposed rules would impede progress in some of the most promising areas of technological opportunity. They would create headwinds to innovation and stall the engine that has driven so much economic growth in this State.

The net effect of the proposed rules would be to divert resources away from responsible innovation and toward cumbersome and ineffective compliance obligations that do little to protect the privacy and security of Californians. The rules would impose unprecedented burdens on businesses, subjecting them to requirements more onerous than similar regulations in Europe, and putting California out of step with the rest of the country and world. We also fear these regulations would be leveraged to compel a barrage of dense, interruptive disclosures on virtually every commercial

¹ As amended by the California Privacy Rights Act ("CPRA").

website and app, disclosures that promise to at best annoy California consumers and more likely confuse, alarm, and mislead them.

The current proposal also exceeds the CCPA's grant of rulemaking authority. Though the CCPA was written to advance focused privacy and data-security objectives, the proposed regulations instead seek to redress complex social issues from civil rights to economic equity that are simply beyond the statutory mandate. Under the guise of regulating automated decisions, the rules propose to cover everyday decisions made by humans simply because those decisions rely in some part on software.

We thus urge the Agency to revisit these regulations to advance instead the privacy and security objectives that animated the CCPA, while allowing businesses to innovate free from exceptional restrictions that would not benefit any California consumer. We write to highlight our most pressing concerns.

I. The Proposed Regulations Exceed and Are Inconsistent with the Statutory Authorization

The proposed regulations must be consistent with the statute that authorized them.² And they may not vary from or enlarge the statute's terms.³ The proposed regulations do not adhere to these principles in certain foundational respects.

The CCPA was originally enacted in 2018 with the stated goal of ensuring the privacy of Californians' personal information. As discussed in more detail below, the 2020 ballot initiative, Prop. 24, amended the CCPA to further strengthen the privacy and security of personal information – including by creating the CPPA to protect, as the Agency's name implies, Californians' privacy.

This 2020 amendment contains two relevant grants of authority. Section 1798.185(a)(14) authorizes the Agency to:

[I]ssu[e] regulations requiring businesses whose processing of consumers' personal information **presents significant risk to consumers' privacy or security** . . . [to] [p]erform a cybersecurity audit on an annual basis . . . [and to] submit to the California Privacy Protection Agency on a regular basis a risk assessment.⁴

² Gov. Code, § 11342.2 (“No regulation adopted is valid or effective unless consistent and not in conflict with the statute”).

³ *Credit Ins. Gen. Agents Ass'n v. Payne* (1976) 16 Cal.3d 651, 656.

⁴ Civ. Code, § 1798.185, subd. (a)(14)(B) (emphasis added).

And Section 1798.185(a)(15) authorizes the CPPA to:

Issue regulations governing **access and opt-out rights** with respect to a business' use of **automated decisionmaking technology, including profiling** and requiring a business' response to access requests 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.⁵

In several key ways, the proposed regulations stray from these narrow authorizations. They would cover a vast range of technologies, use cases, and perceived harms and would impose unprecedented requirements on virtually every business that uses technology. These requirements do not advance, but instead conflict with, the privacy and security aims of the animating law.

A. The proposed regulations would improperly regulate *human* decisionmaking under a grant of authority to regulate only *automated* decisionmaking

Subsection (a)(15) authorizes the Agency to issue targeted regulations governing “automated decisionmaking technology,”⁶ a term which is not defined in the statute. The Agency has proposed defining “automated decisionmaking technology” as “any technology that processes personal information and uses computation to” do one of three things: “execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking.”⁷

This definition conflicts with the statute. The statutory phrase “automated decisionmaking” is a term of art, first introduced in European privacy regulations, which refers to “a decision based solely on automated processing.”⁸ The same definition results from giving each word in “automated decisionmaking technology” its plain meaning: “Decisionmaking” is “the process or practice of making choices or judgments, esp. after a period of discussion or thought.”⁹ And “automated” means “self-acting or self regulating,” “*without needing human control*.”¹⁰

⁵ Civ. Code, § 1798.185, subd. (a)(15) (emphasis added).

⁶ Civ. Code, § 1798.185, subd. (a)(15).

⁷ Proposed Text of Regulations (Cal. Priv. Prot. Agency, Nov. 2024) (hereafter Draft Regulations), § 7001, subd. (f) (emphasis added).

⁸ EU General Data Protection Regulation (GDPR), art. 22.

⁹ *Decision-making*, Black's Law Dict. (12th ed. 2024).

¹⁰ *Automated*, Merriam-Webster Dict. (“operated automatically”); *Automatically*, Merriam-Webster Dict. (“done or produced as if by machine . . . having a self-acting or self-regulating mechanism”); *Automated*, Cambridge Dict. (“carried out by machines or computers without needing human control”); *Automated*, Oxford English Dict. (“Converted so as to operate automatically . . . automatic”); *Automatic*, Oxford English Dict. (“self-generated, spontaneous; . . . self-acting; having the power of motion within itself”).

The proposed definition *partially* maps to this plain meaning. One of its three components is “any technology that . . . uses computation to . . . replace human decisionmaking,” which tracks the statutory term. This is an appropriately narrow definition. It may cover, for example, a machine-learning algorithm used by a college to predict the future performance of high school students based on data in their application and then decide, without human input, which students to admit.

But the other two components of the definition do not track the statutory grant of authority. First, the proposed regulations would cover “*executing*” a decision already made by a human. By definition, then, technology in this bucket would not be “making” a decision and so fall outside the authorization. For example, if a law firm decides that associates who work above a certain number of hours will receive a bonus, a program that automatically identifies and notifies associates who are above or below that pre-determined threshold is merely executing the decision already made by the firm. It is not, in any meaningful sense, “making” a decision about who will receive a bonus. But the regulations would apparently cover this use case. The statute does not plausibly regulate this use of technology.

Second, the regulations improperly propose to regulate “human decisionmaking” that is “*substantially facilitat[ed]*” by technology. For instance, the regulations stipulate that “generat[ing] a score about a consumer that [a] *human reviewer* uses as a primary factor to make a significant decision” would be regulated.¹¹ By its own admission, then, this third proposed definition does not regulate “automated” decisionmaking.¹² Nothing in the CCPA authorizes regulating *human* decisions simply because they are aided or informed by technology.¹³ In fact, in recent decades, a significant amount of human decisionmaking has been “substantially facilitated” by “the output of . . . technology.” Take an entity that consults a medical diagnostic to help determine whether someone is eligible for a clinical trial; or a business that consults a review website’s algorithm when choosing what plumber to hire, but ultimately has a human make the final call. Nobody would naturally say that these examples involve “*automated* decisionmaking,” even if an automated process informs a decision that is ultimately made.¹⁴

¹¹ Draft Regulations, § 7001, subd. (f)(2).

¹² See *Southwest Airlines Co. v. Saxon* (2022) 596 U.S. 450, 457–58 (describing “meaning-variation canon” as “where [a] document has used one term in one place, and a materially different term in another, the presumption is that the different term denotes a different idea”).

¹³ “Facilitating” just means “mak[ing] easier” or “help[ing] bring (something) about.” (See *facilitate*, Merriam-Webster Dict.). Like “executing,” “facilitating” does not involve the making of any decisions.

¹⁴ The Agency’s proposed regulations governing the opt-out rights, and specifically the exemptions, underscore this problem. As an initial matter, this “human appeal” exception and the other exemptions in the proposed regulations are unmoored from the statutory purpose of advancing privacy and security, focusing instead on issues like accuracy, fairness, and discrimination. And the human appeal exception in particular demonstrates the overbreadth of the Agency’s definition of ADMT: If a decision is subject to human review, then it is, by definition, not automated; it is ultimately being made by a human. Yet the exception applies only to certain types of decisions, when a human appeal should remove a decision from

Although the draft regulations propose to exempt technologies akin to a “calculator,” this limitation does not do anything. In the same breath, the regulations provide that calculators and the like *are* covered if used to “execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking.”¹⁵ Since that is just the definition of ADMT reprinted, the “calculator” exception does not change the scope of the regulations’ coverage. And indeed the regulations are replete with supposed examples of “automated decisionmaking technology” that work exactly like calculators. For example, the regulations offer as an example of ADMT “a business’s use of a spreadsheet to run regression analyses” on employees’ performance records.¹⁶ But many calculators have a regression function.¹⁷ It is even possible to calculate a regression on a four-function calculator (or even by hand), using just addition, subtraction, multiplication, and division.¹⁸ If regressions count as ADMT, the purported exclusion of “calculators” cannot mean very much. Likewise, Section 7150(c)(1) contends that the regulations would apply when a rideshare platform assigns rides to drivers, even though rideshare platforms typically allocate work based on human-specified geospatial formulas that calculate which driver is closest to the customer, rather than any sort of automated decision.¹⁹ The lack of real difference between the technologies explicitly included and purportedly excluded under the regulations suggests that in practice, virtually all forms of computation will be covered. Because the CCPA authorizes regulations only of automated decisionmaking, however, these regulations go well past their authorized scope.

Another tell that the regulations exceed the statutory mandate is that their definition of “automated decisionmaking” is out of step with how that term is used internationally. As noted, Europe recognizes that “automated decisionmaking” does not cover decisions that involve humans. Article 22 of the General Data Protection Regulation (“GDPR”), on “Automated Individual Decision-Making, Including Profiling” covers “decisions based *solely* on automated processing.”²⁰

the scope of the regulations entirely. This further demonstrates that the definition of ADMT is overbroad and strays beyond the statutory mandate.

¹⁵ Draft Regulations, § 7001, subd. (f)(4).

¹⁶ Draft Regulations, § 7001, subd. (f)(4).

¹⁷ *Solution 11918: Calculating and Graphing a Linear Regressions on the TI-83 Plus*, Texas Instruments Knowledge Base (accessed January 31, 2025), <https://education.ti.com/en/customer-support/knowledge-base/ti-83-84-plus-family/product-usage/11918>.

¹⁸ Bobbitt, *How to Perform Linear Regression by Hand*, Statology (May 8, 2020).

¹⁹ Patent No. US12086897, *Dynamic Optimized Reassignment of Providers at Geohash Level*, Applicant: Lyft, Inc., February 3, 2020,

<https://patentimages.storage.googleapis.com/ee/e5/49/b80dd99269e026/US12086897.pdf>; Patent No. US20200072622A1, *Determining Matches Using Dynamic Provider Eligibility Model*, Applicant: Lyft, Inc., February 3, 2020,

<https://patentimages.storage.googleapis.com/4a/3d/da/1a310f2e188a4a/US20200072622A1.pdf>.

²⁰ GDPR, art. 22 (emphasis added); see also GDPR, recital 71.

Similarly, the U.K. government, in its guidance on the U.K. version of the GDPR, explains that “automated decision-making is the process of making a decision by automated means *without any human involvement*.”²¹ Brazil’s equivalent law similarly equates “automated decision[s]” with “decisions made solely based on automated processing.”²² To interpret California’s law to extend to human decisionmaking using technology would be incongruous and wrong.

The proposal to regulate human decisionmaking – as opposed to an “automated decision” based “solely on automated processing” – thus exceeds the grant of authority that supports the regulations. The references to “executing” and “substantially facilitating” human decisions should be removed from the proposed regulations, and the regulations should be modified to exclude examples, like in Sections 7001(f)(4) and 7150(c)(1)–(2), that do not involve the making of decisions solely by automated technology.

B. There is no basis in the statute for keying the regulatory requirements off the overly broad category of “significant decisions”

The proposed rules extensively regulate businesses that use automation to make any “significant decision,” which the Agency defines to include decisions without any connection to the privacy concerns that establish its authority to regulate here. The category of “significant decisions” is instead defined to cover much of the economy with no privacy tether at all: any decision “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).”²³ When a business uses automation to make a significant decision as the proposed regulations define that term, it must conduct a risk assessment, issue a pre-use notice, and (unless it meets certain exceptions) offer consumers the right to opt out of ADMT and a right of access.

The throughline across these supposedly “significant” decisions is plainly not privacy (and the regulation barely purports to have that theme); it is that these decisions arguably involve a socially important industry. For example, the regulations would govern remote software used to proctor a college-admissions test that processes a consumer’s IP address. Examples like this are covered

²¹ Information Comm’r’s Off., What is Automated Individual Decision-Making and Profiling? (accessed Jan. 31, 2025),

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/>.

²² Lei Geral de Proteção de Dados (LGPD), Art. 20, Official Journal of the Brazilian Government (August 14, 2018).

²³ Draft Regulations, § 7220, subd. (a)(1).

because the Agency considers educational admissions to be important, not because they implicate privacy concerns in any real sense.

But there is no basis in the statute to have these sweeping requirements turn merely on whether a decision is “significant,” without any tether to the statute’s focus on data privacy and security. The CCPA is a *privacy* law, not an all-purpose regulator of automation applications perceived to be socially important. Prop. 24 was titled the “California *Privacy* Rights Act.”²⁴ And the resulting law is about data privacy from top to bottom. The law mentions “privacy,” “security,” and “personal information” more than 500 times, but “automated decisionmaking” only once, in a single sentence.²⁵ That sentence is one subsection of one subsection out of Prop. 24’s 31-section, over-20,000-word ballot initiative.²⁶ It is implausible that in this single sentence, California voters intended to authorize a new legal framework for regulating automated decisionmaking entirely disconnected from privacy concerns.²⁷ There is nothing in the CCPA to support the idea that the agency is now empowered to enforce it as a general consumer-protection or anti-discrimination statute.²⁸

The CPRA’s enactment history further confirms what was (and was not) on California voters’ minds when they approved Prop. 24. As the public debated the law, the *only* concerns presented to them involved privacy and security.²⁹ The ballot guide explained that Prop. 24 sought to “amend[] consumer privacy laws.”³⁰ The Attorney General’s official summary promised that the

²⁴ Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020).

²⁵ Draft Regulations.

²⁶ Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020).

²⁷ Indeed, these other concerns are already being addressed by other agencies. The California Civil Rights Department has issued its own proposed regulations concerning the use of “automated-decision systems” in potentially discriminatory ways. (Second Modifications to Initial Text of Proposed Modifications to Employment Regulations Regarding Automated-Decision Systems (Civil Rights Council, Jan. 27, 2025), <https://civildrights.ca.gov/wp-content/uploads/sites/32/2025/02/Second-Modifications-to-Proposed-Modifications-to-Employment-Regulations-Regarding-Automated-Decision-Systems.pdf>.)

Such regulations are best left to an agency which has the authority and competence to address discrimination and fairness. The regulations should be narrowed to focus the opt-out right on factors that relate to privacy and security.

²⁸ It is also no answer that subsection (a)(15) authorizes the Agency to regulate automated decisionmaking. That subsection is prefaced and cabined by section 1798.185, subd. (a), which requires all regulations to “further the purposes of this title.” As we have explained, those purposes all relate to privacy. By contrast, Prop. 24’s “purpose and intent” section does not mention automation or AI even once. Thus, subsection (a)(15) authorizes the agency to regulate automated decisionmaking as necessary to promote data privacy and security. It does not grant a freestanding power to regulate ADMT unmoored from those concerns.

²⁹ California Secretary of State, Official Voter Information Guide, November 3, 2020, pp. 66–71, <https://vig.cdn.sos.ca.gov/2020/general/pdf/complete-vig.pdf>.

³⁰ *Id.* at p. 66.

law would let consumers “prevent businesses from sharing personal information,” “correct inaccurate personal information,” and “limit businesses’ use of sensitive personal information.”³¹ It also explained that the Agency would “enforce and implement consumer privacy laws.”³² The Legislative Analyst added that Prop. 24 would “change[] existing consumer data privacy laws” and “provide new consumer privacy rights” concerning the “*sharing* of personal data” and “use of ‘sensitive’ personal data.”³³ He also noted that the CPPA’s authority to “develop[] . . . new regulations” encompassed the power to pass “rules for correcting consumer personal data.”³⁴ And the arguments for and against Prop. 24 focused exclusively on whether the law would “protect . . . personal information” and how it would impact “privacy rights.”³⁵

By contrast, automated decisionmaking and artificial intelligence were not on anyone’s radar. The terms “automated decisionmaking” and “artificial intelligence” do not appear even once in any of the ballot-initiative materials that accompanied Prop. 24.³⁶ Nor did the Legislative Analyst discuss regulating ADMT, much less for decisions involving non-sensitive information. The complete absence “of such a goal . . . [from the] ballot materials” is a strong tell that the law did not enact it.³⁷ Indeed, “[i]f this quite significant consequence were consistent with the most reasonable understanding of Proposition [24]’s purpose . . . one would assume there would be some mention of such a goal elsewhere in Proposition [24].”³⁸ “[E]nactors do not ‘hide elephants in mouseholes.’”³⁹ And here, that simply cannot be a sound principle of statutory interpretation; Prop. 24’s drafters were forbidden from wedging a comprehensive AI bill into their privacy statute. Under California law, “[a]n initiative measure embracing more than one subject may not be submitted to the electors or have any effect.”⁴⁰

It comes as little surprise then that even the primary advocate for and drafter of Prop. 24, Alastair Mactaggart, has also commented on how the draft regulations have improperly strayed from the privacy mandate.⁴¹ At the November 8, 2024 CPPA board meeting, for instance, Mactaggart

³¹ *Ibid.*

³² *Ibid.*

³³ *Id.* at pp. 67–68.

³⁴ *Id.* at p. 68.

³⁵ *Id.* at pp. 7071.

³⁶ Official Voter Information Guide.

³⁷ *Cal. Cannabis Coalition v. City of Upland* (2017) 3 Cal.5th 924, 940.

³⁸ *Ibid.*

³⁹ *Ibid.*

⁴⁰ Cal. Const. art. II, § 8(d); see, e.g., *Cal. Trial Lawyers Assn. v. Eu* (1988) 200 Cal.App.3d 351, 359–360 (provision regulating insurers’ campaign contributions was not related to the initiative’s subject of “spiralling insurance costs”).

⁴¹ Nov. 8 CPPA Bd. Hr’g Tr. pp. 99–103.

reminded the Agency that “we should focus on our privacy mandate” after explaining how the draft regulations exceed their authorized scope.⁴²

A comparison to Europe’s GDPR also shows why the statute does not authorize the regulation of decisions based solely on their “significance.” As we noted in Part I.A, there is some overlap in the language between Prop. 24 and the GDPR. For example, both laws regulate automated decisionmaking – an indicator that the concept should have similar meaning in both jurisdictions. But the converse is also true: When Prop. 24 conspicuously failed to borrow a certain aspect of the GDPR, that is evidence the voters did *not* intend to import this facet of the European regulations. In this vein, it is telling that, whereas the GDPR regulates the use of automated decisionmaking to make “significant[]” decisions, Prop. 24 omitted that phrasing from its provision concerning automated decisionmaking, instead keeping the focus on the narrower domain of privacy.⁴³ Given that the California voters specifically declined to import the “significance” framework, it would be inappropriate for the implementing regulations to reverse course and do just that.

Because the regulations turn on the broad category a business decision falls into, not the degree to which (or even whether) the decision implicates privacy, they are inconsistent with the privacy rationale explicitly stated in Prop. 24 and approved by the voters. And when coupled with the overly broad definition of ADMT, these regulations cover an astoundingly large swath of the economy that Prop. 24 could not have plausibly meant to regulate. The proposed rules plainly exceed their authorization in the CCPA and must instead be revised to cover only decisions with a significant privacy impact.

C. The provisions limiting how a business can advertise to its own customers based on existing data are not authorized by and are inconsistent with the statute

The draft regulations impose far-reaching and unauthorized obligations on first-party “behavioral advertising.” The regulations put a raft of requirements – extensive disclosures, burdensome evaluations, and mandatory opt-out rights – on businesses that engage in so-called “extensive profiling,” which, contrary to the plain meaning of those words, is defined to encompass *all* personalized advertising, including advertising based on data a business *already has* through its own transactions with its customers.⁴⁴ All these requirements may apply to, for example, a retailer that recommends cleaning supplies to a customer who previously bought them, at a point when

⁴² *Id.* at p. 106.

⁴³ See Prop. 24.

⁴⁴ Draft Regulations, § 7001, subd. (g) (“‘Behavioral advertising’ means the targeting of advertising to a consumer based on the consumer’s personal information obtained from the consumer’s activity . . . *within the business’s own distinctly-branded websites, applications, or services.*”) (emphasis added).

those supplies may be running low. But the CCPA does not authorize the extensive regulation of this benign conduct; indeed the voters consciously drew a line between such first-party advertising, which they allowed, and cross-context behavioral advertising, which they explicitly gave consumers the right to opt out of.⁴⁵

Indeed, when voters amended the CCPA, they directly addressed the question of how to regulate advertising, leaving no room for the proposed rules. The CCPA, as enacted by the legislature, permitted businesses to use consumers' personal information for advertising and marketing, and gave consumers the right to opt out only from their data being sold to third parties.⁴⁶ Prop. 24 expanded that opt-out right to cover both the "selling" and "sharing" of personal information. It specifically identified "cross-context behavioral advertising" – that is, advertising "based on the consumer's personal information obtained from the consumer's activity *across businesses, distinctly-branded websites, applications, or services*" – as a type of "sharing."⁴⁷ So while Prop. 24 provided a right to opt out of cross-context behavioral advertising, it did not impose any comparable restrictions on first-party advertising.

Prop. 24's preamble and legislative history further underscore the voters' intent to regulate third-party advertising only. The preamble indicates that voters were focused on the selling or sharing of their personal information with other businesses.⁴⁸ The Legislative Analyst confirmed that one of the key rights created by Prop. 24 was to limit the "*sharing* of personal data."⁴⁹ Similarly, in describing why Prop. 24 added the concept of "sharing" data and created opt-out rights for "cross-context behavioral advertising," Mactaggart explained that Prop. 24 made it "crystal-clear, when it comes to sharing consumer information for cross context behavioral advertising, that the law gives consumers the right to opt out."⁵⁰ On the other hand, he noted that "*first-party data the business has can be used in any way that the business wants with that consumer.*"⁵¹ That was the fundamental balance struck by Prop. 24: consumers were given a right to opt out of *third-party* targeted advertising, but businesses maintained the ability to engage in *first-party* advertising – that is, to advertise to consumers based on information gathered as part of a business's own

⁴⁵ Draft Regulations, § 7001, subd. (g).

⁴⁶ Cal. Assem. Bill No. 375 (2017–2018 Reg. Sess.); Civ. Code, § 1798.140, subd. (d)(4).

⁴⁷ Civ. Code, § 1798.140, subds. (k), (ah)(1).

⁴⁸ Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 2.I ("Consumers should have the information and tools necessary to limit the use of their information to non-invasive, pro-privacy advertising, where their personal information is not sold to or shared with hundreds of businesses they've never heard of, if they choose to do so.").

⁴⁹ California Secretary of State, Official Voter Information Guide, November 3, 2020, pp. 66–71.

⁵⁰ Davis + Gilbert LLP, *Alastair Mactaggart's Privacy Perspective: Past, Present and Where We're Headed* (2022), <https://www.mondaq.com/unitedstates/data-protection/1183432/alastair-mactaggarts-privacy-perspective-past-present-and-where-were-headed>.

⁵¹ *Ibid.*

relationship with a consumer. In adding opt outs and burdensome requirements for first-party advertising, the proposed regulations are fundamentally at odds with the voters' intent in approving Prop. 24.

Nor does the mere use of the word “profiling” in the statute justify the scope of the proposed regulations. In explaining its expansive definition of that word, the Agency points to various other state statutes that also regulate “profiling.” But each of these laws – like the CCPA and Prop. 24 – treats profiling and advertising as distinct concepts. Each law creates a right to opt out of profiling in some circumstances.⁵² And then each law handles advertising with *separate* statutory language, reflecting the universal understanding that “advertising” and “profiling” are distinct practices.⁵³ (And in turn, the “advertising” proscriptions in these statutes unflaggingly cover only “targeted advertising” – a term, much like “cross-context behavioral advertising” in Prop. 24, defined to exclude first-party advertising.)⁵⁴ It is precisely because Prop. 24 was enacted against a legal background in which “profiling” did not cover “advertising” that Prop. 24 needed to separately address advertising. And when it did, it explicitly carved out first-party advertising from opt-out rights.⁵⁵

The Agency has no authority to include first-party advertising in the draft regulations and should remove all references to first-party behavioral advertising.

⁵² See, e.g., Va. Code Ann., § 59.1-577, subd. (5)(iii) (providing the ability to opt out of “profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer”); Colo. Rev. Stat. Ann., § 6-1-1306, subd. (1)(a)(I)(C) (similar); Conn. Gen. Stat. Ann., § 42-518, subd. (a)(5)(c) (similar); Del. Code Ann. tit. 6, § 12D-104(a)(6)(c) (similar); Fla. Stat., § 501.705, subd. (2)(e)(3) (similar); Ind. Code, § 24-15-3-1, subd. (b)(5)(C) (similar).

⁵³ See, e.g., Va. Code Ann., § 59.1-577, subd. (5)(i) (providing the ability to opt out of “targeted advertising”); Colo. Rev. Stat. Ann., § 6-1-1306, subd. (1)(a)(I)(A) (similar); Conn. Gen. Stat. Ann., § 42-518, subd. (a)(5)(A) (similar); Del. Code Ann. tit. 6, § 12D-104, subd. (a)(6)(a) (similar); Fla. Stat., § 501.705, subd. (2)(e)(1) (similar); Ind. Code § 24-15-3-1(b)(5)(A) (similar).

⁵⁴ See, e.g., Va. Code Ann., § 59.1-575 (“‘[t]argeted advertising’ does not include . . . [a]dvertisements based on activities within a controller’s own websites or online applications”); Colo. Rev. Stat. Ann., § 6-1-1303, subd. (25) (similar); Conn. Gen. Stat. Ann., § 42-515, subd. (39) (similar); Del. Code Ann. tit. 6, § 12D-102, subd. (33) (similar); Fla. Stat., § 501.702, subd. (33) (similar); Ind. Code, § 24-15-2-30 (similar).

⁵⁵ The Federal Trade Commission distinguishes between first-party data use and third-party data sharing as well, singling out the latter for enforcement. See, e.g., *In re Gateway Learning Corp.* (July 7, 2004), FTC No. 042-3047,

<https://www.ftc.gov/sites/default/files/documents/cases/2004/07/040707agree0423047.pdf>;

In re Chitika, Inc. (Mar. 14, 2011), FTC No. 1023087,

<https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110314chitikaagree.pdf>.

D. The regulations related to “physical or biological identification or profiling” are unauthorized

The draft regulations seek to impose multiple unwarranted requirements on “physical or biological identification or profiling.” The regulations define “physical or biological identification or profiling” to mean “identifying or profiling a consumer using information that depicts or describes their physical or biological characteristics, or measurements of or relating to their body.”⁵⁶ A business who uses “physical or biological identification or profiling” for a “significant decision” or “extensive profiling” must “conduct an evaluation” of its “identifying or profiling to ensure that it works as intended” and “does not discriminate”; and “must implement policies, procedures, and training to ensure” that the “identifying or profiling works as intended.”⁵⁷ The regulations would grant consumers a complete right to opt out of the use of their personal information for any training of ADMT that is capable of being used “for physical or biological identification or profiling.”⁵⁸ These regulations are incompatible with the statute.

To start, although the Agency has apparently proposed these regulations under its Subsection (a)(15) power to regulate “access and opt-out rights with respect to a business’ use of automated decisionmaking technology, including profiling,” the regulations fly past this grant of authority in two ways. For one thing, they regulate far more than access and opt-out rights. They set substantive criteria that “identification or profiling” must satisfy and compel testing and quality-assurance procedures. There is no basis for this substantive aspect of the regulations. The regulations also exceed the statutory requirement that they concern “automated decisionmaking technology, including profiling.” The regulations cover, in addition to profiling, the mere “identifying” of a consumer using biometrics.⁵⁹ “Identifying” is not “profiling.”⁶⁰ The draft

⁵⁶ Draft Regulations, § 7001, subd. (gg).

⁵⁷ Draft Regulations, § 7201.

⁵⁸ Draft Regulations, §§ 7200, subd. (a), 7221, subd. (a)–(b).

⁵⁹ No other comprehensive state law includes “identification” in the definition of “profiling.” See, e.g., Va. Code Ann., § 59.1-575 (“‘Profiling’ means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person’s economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.” Identification does not fall under this definition because identification does not require businesses to “evaluate, analyze, or predict . . . personal aspects” like “health” or “personal preferences,” but rather to verify or confirm one’s identity.); Ind. Code, tit. 24, § 24-15-2-23 (defining profiling as “solely” automated processing but similarly excluding “identification” because it is not an “evaluat[ion], analy[sis], or predict[ion] relating to “personal aspects” like “health records,” “interests,” or “movements”).

⁶⁰ It does not appear that the Agency has tried to justify this regulation under the authority to regulate “automated decisionmaking.” And for good reason: identification does not entail making a decision. When an online grocery store uses a scanner to check the ID of someone buying medicine, or a college’s anti-cheating software automatically verifies the student ID of a remote exam taker, to say that anyone

regulations define “profiling” as processing personal information to “analyze or predict aspects concerning that natural person’s intelligence, ability, aptitude, performance at work, economic situation; health, including mental health; personal preferences, interests, reliability, predispositions, behavior, location, or movements”⁶¹ – in short, predicting someone’s behavior or personal characteristics. Someone’s identity, however, is not a behavior or characteristic. Other parts of the CCPA bolster this distinction between “identifying” and “profiling.” For example, the CCPA grants consumers the right to opt out of certain uses of their biometric information, but not if a business has collected this information “without the purpose of inferring characteristics about a consumer.”⁶² And even the portion of the regulations ostensibly directed at “profiling” exceeds the statutory limit. The statute authorizes at most a right for consumers to opt out of having their data used to profile them – not the right created by the regulations, a right to opt out of having their data used merely to train a technology that theoretically could be used to profile other people.⁶³

The regulations also conflict with the statute by erecting a confusing scheme for regulating biometric information that competes with a different one already created by the statute. The statute already defines a category called “sensitive personal information,” which includes “the processing of biometric information for the purpose of uniquely identifying a consumer.”⁶⁴ The statute then guarantees consumers the right to limit the use of their sensitive personal information.⁶⁵ But this right is highly qualified. Consumers cannot opt out of businesses’ using their data to “improve, upgrade, or enhance the service[s]” they offer.⁶⁶ The statute also authorizes additional rules qualifying this right of consumers in order to protect the “legitimate operational interests of businesses.”⁶⁷

The draft regulations conflict with this carefully balanced scheme. For example, under the draft regulations, a user may opt out of the use of her biometric data to “improve [a business’s] algorithm.”⁶⁸ This is irreconcilable with the statute’s express safe harbor allowing businesses to use sensitive personal information to improve the services they offer. And putting this specific glaring conflict aside, given that the statute already lays out an approach to biometric regulation and does so using a specific statutory term, the statute cannot be plausibly read to authorize the

has made a “decision” would be strained. There has been no judgment or weighing of options; the identifications are no more a “decision” than when a calculator determines whether two values are equal.

⁶¹ Draft Regulations, §7001, subd. (kk).

⁶² Civ. Code, § 1798.121, subd. (d).

⁶³ Civ. Code, § 1798.185, subd. (a)(15).

⁶⁴ Civ. Code, § 1798.140, subd. (ae)(2).

⁶⁵ Civ. Code, § 1798.121.

⁶⁶ Civ. Code, §§ 1798.121, subd. (a), 1798.140, subd. (e)(8).

⁶⁷ Civ. Code, § 1798.185, subd. (a)(18)(C).

⁶⁸ Draft Regulations, §§ 7200, subd. (a), 7221, subd. (a)–(b).

Agency to define a new similar, overlapping term and design a separate scheme of rights associated with that term.⁶⁹

The proposed regulations of “physical or biological identification or profiling” should therefore be removed. At the very minimum, “identification” and “identifying” should be deleted from the definition.

E. The “Pre-Use Notice” requirements are not authorized by the statute

Even though the enabling provision authorizes “regulations governing *access* and *opt-out* rights” for automated decisionmaking, the proposed regulations invent an entirely new category of requirements.⁷⁰ Specifically, businesses engaged in ADMT must provide a “prominent and conspicuous” pre-use notice with extensive information, including: a “plain language explanation of the specific purpose for which the business proposes to use the automated decisionmaking technology”; an explanation of any exceptions to the right to opt out that the business relied on; “information about how the automated decisionmaking technology works,” such as the “logic,” “key parameters,” and “intended output” of the ADMT; and information about the role of humans in the decision.⁷¹

These mandated disclosures conflict with the CCPA. Not only does the statute nowhere mention them, it explicitly handles consumer notice differently. When discussing consumers’ right to “information about [an algorithm’s] logic,” the law specifically couches that right in terms of an “access” request rather than any sort of pre-use notification. Meanwhile, other parts of the law require businesses to give notice, in some form, of what personal information they collect and how it is used “at or before the point of collection”⁷² – but as other parts of the regulations make clear, this flexible requirement can be satisfied by providing consumers with a link to a section of its

⁶⁹ Further illustrating that implausibility is that in addition to conflicting with the statute, the draft regulations conflict sharply with the existing regulations fleshing out limitations on the use of “sensitive information.” Under the existing regulations, businesses have the right to use sensitive information like biometrics to “verify or maintain” the quality of the business’s products and “improve, upgrade, or enhance” their service or device (§ 7027, subd. (m)). By contrast, under the draft regulations, a business may not use biometrics to “improve [its] algorithm” if a user opts out (Draft Regulations, §§ 7200, subd. (a), 7221 subd. (a)–(b)). It is inevitable that having two separate regulations of essentially the same activity will lead to conflicts like this – not to mention unsettle the expectations of businesses that have already invested money complying with the first set of regulations – which is further evidence the statute did not authorize that.

⁷⁰ Civ. Code, § 1798.185, subd. (a)(15).

⁷¹ Draft Regulations, § 7220. While Civ. Code, § 1798.185, subd. (a)(15) authorizes the Agency to issue regulations requiring “meaningful information about the logic involved in those decisionmaking processes,” that is only in connection with “response[s] to access requests,” not a “pre-use notice.”

⁷² Civ. Code, § 1798.100, subd. (a).

privacy policy.⁷³ Elsewhere, the CCPA does expressly require businesses to issue certain “prominent” disclosures, but notably not here.⁷⁴ The legislature and voters thus know how to create a “pre-collection” notice regime, and even created an intricate one. They chose not to authorize the Agency to create yet another.⁷⁵

And for good reason. Especially given the scope of the regulations, users would be bombarded with the proposed pre-use notifications constantly. As detailed in Part II below, copious social-science research confirms that consumers are likely to suffer from this information overload. The California law, correctly interpreted, does not allow this anti-consumer result. The Agency has no authority to include a pre-use notice requirement in the draft regulations and should remove the requirement.

II. The Regulations Are Not Supported by Substantial Evidence

Regulations must be reasonably necessary to implement the statute authorizing them,⁷⁶ and the proposed regulations are not. Although the draft regulations would impose unprecedented burdens on California businesses and consumers, there is not substantial evidence that they are necessary to effectuate the goals of the CCPA. Those goals, as we have noted, were explicit. Prop. 24 states that “the rights of consumers and the responsibilities of businesses should be implemented with the goal of strengthening consumer privacy, while giving attention to the impact on business and innovation.”⁷⁷ The proposed regulations advance many concerns unrelated to privacy and security while impeding innovative product development.

This is why Mactaggart, now a member of the CPPA’s board, has expressed concern about the “overreach” of the draft regulations,” that they “undermine[] privacy rather than protecting it,” and that they mandate obligations inconsistent with the “privacy and security” focus of the statute.⁷⁸ As explained more below, the overly burdensome demands of the regulations are likely to lead

⁷³ Cal. Code Regs., tit. 11, § 7012, subd. (f).

⁷⁴ Specifically, “prominent and robust” notice is required when a business transfers personal information to a third party as part of a “merger, acquisition, bankruptcy, or other transaction” and the third party “materially alters how it uses or shares the personal information.” (Civ. Code, § 1798.140, subds. (ad)(2)(C), (ah)(2)(C).) Third parties are permitted, but not required, to satisfy their notice obligations by “prominently and conspicuously” “providing the required information . . . on the homepage of its internet website.” (Civ. Code, § 1798.100, subd. (b)); Civ. Code, § 1798.130, subd. (a)(5)(C)).

⁷⁵ *Hamdan v. Rumsfeld*, (2006) 548 U.S. 557, 578 (“A familiar principle of statutory construction . . . is that a negative inference may be drawn from the exclusion of language from one statutory provision that is included in other provisions of the same statute.”).

⁷⁶ Gov. Code, § 11342.2 (“No regulation adopted is valid or effective unless . . . reasonably necessary to effectuate the purpose of the statute.”).

⁷⁷ Prop. 24, § 3, subd. (C)(1).

⁷⁸ Nov. 8 CPPA Bd. Hr’g Tr., pp. 99–103.

businesses to divert limited resources from effective privacy protections, resulting in a net reduction in actual privacy and security protections for consumers. As Mactaggart put it, “this just creates a regulatory burden that I think has a negative impact on privacy.”⁷⁹

A. There is no basis for regulating human decisionmaking merely because it is assisted by technology

The Agency has not put forward substantial evidence to support its definition of ADMT, which imposes onerous requirements on uses of technologies that only “execute” or “substantially facilitate” decisions made by humans. California businesses have used algorithms, artificial intelligence, “regression analyses,” “computation,” and other technology to assist with human decisions for decades. As Mactaggart noted, the proposed “definition of ADM[T] includes the use of almost any computerized technology in a way that describes how humans have used computers for 30 or 40 years.”⁸⁰ Businesses have deployed these techniques to execute or inform countless “significant decisions” and instances of “extensive profiling” (as the regulations define those terms), and the use of this technology is essential to California’s economy.⁸¹ Yet the Statement of Reasons does not cite any evidence that decisions executed by technology or substantially facilitated by technology put consumers at a heightened privacy or security risk and must be regulated.

Instead, the Statement merely notes that its definition of ADMT “is informed by other frameworks addressing the use of ADMTs,” including the Biden Administration’s now-rescinded Blueprint for an AI Bill of Rights, an EEOC guidance document, and an academic article that discusses government uses of ADMT.⁸² These policy documents do not support the proposed definition, however, since none defines ADMT to include the mere “execution” or “substantial facilitation” of a human decision or contends that those activities present privacy concerns.⁸³ To the contrary, such a broad scope would put California out of step with other states, including Connecticut,⁸⁴

⁷⁹ Nov. 8 CPPA Bd. Hr’g Tr., p. 106.

⁸⁰ Nov. 8 CPPA Bd. Hr’g Tr., p. 100.

⁸¹ Additional longstanding practices now covered by these regulations include: use of software or programs derived from statistics or other data-processing techniques (§ 7001, subd. (f)(1)); a business’s use of a regression analysis to evaluate employee performances (§ 7001, subd. (f)(4)); a dating app’s provision of geolocation, ethnicity, and medical information from a consumer’s profile to its analytics service provider (§ 7150, subd. (c)(3)); a grocery store’s use of wifi tracking within its stores to observe consumer shopping behavior (§ 7150, subd. (c)(5)); an educational provider’s use of software that automatically screens a student’s work for plagiarism (§ 7220, subd. (d)(3)).

⁸² California Privacy Protection Agency, Initial Statement of Reasons (hereafter ISOR), (July 2024) p. 14.

⁸³ ISOR at p. 14 n.64.

⁸⁴ Conn. Gen. Stat. Ann., § 42-518.

Delaware,⁸⁵ Indiana,⁸⁶ Montana,⁸⁷ Rhode Island,⁸⁸ Maryland,⁸⁹ Texas,⁹⁰ Florida,⁹¹ Nebraska,⁹² Tennessee,⁹³ and New Hampshire,⁹⁴ which all provide a right to opt out of profiling in furtherance of “solely” automated decisions. By producing no evidence of privacy harms stemming from the broader range of activities it seeks to cover, the Agency fails to justify the scope of its regulation.⁹⁵

B. There is no basis to define “significant decisions” and “extensive profiling” to cover everyday uses of technology that pose no privacy concerns

The Statement of Reasons does not contain substantial evidence to support the regulations’ broad definitions of “significant decisions” or “extensive profiling.” In fact, the Statement contains no evidence that the far-reaching scenarios covered by these definitions present any risk to the privacy or security of personal information – much less “substantial evidence” that regulating ADMT in these contexts is necessary.

The Statement offers only high-level explanations for its sweep, without linking the categories the regulations would cover to real privacy concerns. For example, while the Statement cites a generalized concern about the “lack of consumer control over their personal information,”⁹⁶ it does not link this concern to examples of a “significant decision” or “extensive profiling,” and especially not to examples of first-party behavioral advertising. Nor does the Statement attempt to tie this putative privacy harm to any specific ADMT use (let alone the uses that the Agency characterizes as “significant”) or explain why the alleged harms are not adequately addressed by the CCPA and numerous sector-specific laws.⁹⁷

⁸⁵ Del. Code Ann., tit. 6, §12D-104, subd. (a)(6)(c).

⁸⁶ Ind. Code, § 24-15-23.

⁸⁷ Mont. Code Ann., § 30-14-2808.

⁸⁸ 6 R.I. Gen. Laws, § 48.1-5, subd. (e)(4).

⁸⁹ Md. Code Ann. Com. Law, § 14-4605, subd. (b)(7)(iii).

⁹⁰ Tex. Bus. & Com. Code, § 541.001, subd. (24).

⁹¹ Fla. Stat., § 501.702, subd. (25).

⁹² Neb. Rev. Stat., § 87-1102, subd. (25).

⁹³ Tenn. Code Ann., § 47-18-3201, subd. (21).

⁹⁴ N.H. Rev. Stat. Ann., § 507-H:4, subd. (I)(e).

⁹⁵ During the November 8, 2024 CPPA board meeting, Mactaggart stated, “If a human is materially involved in a decision, no opt-out should be required. And . . . again, I think we should focus on our privacy mandate.” (Nov. 8 CPPA Bd. Hr’g Tr., p. 106–107.)

⁹⁶ ISOR at p. 60.

⁹⁷ See Civ. Code, §§ 1798.110, 1798.120. Consumer-privacy concerns are already addressed by existing sector-specific laws. See Health Insurance Portability and Accountability Act, 45 C.F.R., § 164.502; see also Fair Credit Reporting Act, 15 U.S.C., § 1681, subd. (b); see also Equal Employment Opportunity Commission, 29 C.F.R., § 1635.9.

Although a broader policy debate has recently emerged around the potential benefits and harms of fully automated decisionmaking and AI, this debate has not been principally focused on privacy concerns.⁹⁸ Rather, these technologies implicate fairness considerations and broader philosophical questions around the appropriate role of technology in everyday life. This discussion has tended toward the theoretical, emphasizing the potential harms to society if technology is left to its own devices – but with very few examples of real harms related to the Agency’s privacy-and-security mandate.⁹⁹

A comparison to Europe’s GDPR helps underscore why the regulations here are inappropriately broad. The GDPR covers a broader range of applications (though even then, only with respect to *solely* automated decisions), but it does so in order to implement sweeping human-rights objectives. The GDPR frames its purposes in all-encompassing terms: to “serve mankind,” and protect all manner of “freedoms” and “fundamental rights,” ranging from “freedom of expression and information” to “diversity.”¹⁰⁰ And the GDPR is itself grounded in the European Union’s Charter of Fundamental Rights, which enshrines principles such as human dignity, nondiscrimination, and due process.¹⁰¹ It is no surprise, then, that the GDPR covers all manner of decisions with a legal or similarly significant effect.¹⁰² The CCPA, by contrast, was never meant to promote such a diverse array of human-rights or policy priorities, beyond privacy. It does not establish a comprehensive rights-based framework. As detailed above, it was enacted to enhance transparency, provide consumers with greater control over their personal information, and regulate how businesses collect, share, and sell that information.¹⁰³ And thus it cannot carry the weight that the draft regulations seek to put on it.

The references to “behavioral advertising” should be deleted, and as discussed in Part I.B, the regulations should be revised to cover only decisions with a significant privacy impact.

⁹⁸ Krupa and Brandstätter, *UK data reform nurtures innovation but ensures safeguards to ensure EU adequacy, officials say* (November 21, 2024), Mlex, <https://www.mlex.com/mlex/articles/2264157/uk-data-reform-nurtures-innovation-but-ensures-safeguards-to-ensure-eu-adequacy-officials-say> (on UK proposed reform); Kern, *Humans versus machines: Who is perceived to decide fairer? Experimental evidence on attitudes toward automated decision-making* (October 14, 2022), *Patterns*, Vol. 3, Iss. 10, <https://www.sciencedirect.com/science/article/pii/S2666389922002094>.

⁹⁹ Chakravorti, *AI’s Trust Problem* (May 3, 2024) *Harv. Bus. Rev.*, <https://hbr.org/2024/05/ais-trust-problem>.

¹⁰⁰ GDPR, recital 4.

¹⁰¹ *Charter of Fundamental Rights of the European Union* (Dec. 7, 2000) O.J. (C 364).

¹⁰² *Ibid.*

¹⁰³ See Prop. 24.

C. There is no basis to support the burdensome pre-use notice and request-to-access requirements

Similarly, the detailed and burdensome disclosure obligations contained in the proposed regulations are not necessary to protect consumers' privacy or security.¹⁰⁴ To the contrary, substantial evidence demonstrates that mandating extensive "conspicuous" notices in the course of routine consumer interactions would *undermine* privacy and security by overwhelming consumers and leading them to tune out important disclosures. At the same time, the enormous compliance burden on businesses will be a headwind on innovation.

The Agency has not put forward any evidence that the pre-use notices or access rights will help consumers. The Statement's discussion of pre-use notices is bereft of any evidence justifying the invention of this requirement.¹⁰⁵ And its justification of the "request to access" regulations is nearly as sparse. On that score, the Statement points only to consumers' right to access how credit scores are calculated.¹⁰⁶ But discrete information about credit score calculations is a far cry from the detailed disclosures required here.

Worse still, the regulations are likely to backfire for consumers, because the pre-use notice requirements will result in a highly disruptive online experience. Given the staggering proposed coverage of the "automated decisionmaking" regulations, consumers would be bombarded with pre-use notifications constantly. And given the dense list of required information, the notices will be long. Businesses will need to pepper users with numerous detailed categories of information, ranging from the fine details of how the automation works (its "logic" and "parameters") to a non-generic (that is, long) explanation of the purpose behind the automation, to a list of rights.¹⁰⁷ What is worse, users *must* be presented with most of these details before they even interact with the business or product; this is not like a warning label on a microwave that they may exercise autonomy over whether to read. So it is inevitable that many users will be force-fed excessive information they do not want.

Abundant social science confirms the intuition that overloading consumers with this information will be bad for them. Studies show that forcing consumers to view "excessive information" will overwhelm them and "degrade the quality" of their choices.¹⁰⁸ One reason is that "mandated

¹⁰⁴ ISOR at pp. 85, 91–92.

¹⁰⁵ ISOR at pp. 83–86.

¹⁰⁶ ISOR at pp. 91–97 & nn. 141–143.

¹⁰⁷ Draft Regulations, § 7220, subd. (c).

¹⁰⁸ See Latin, *Good Warnings, Bad Products, and Cognitive Limitations* (1994) 41 UCLA L.Rev. 1193, 1214–15, <https://heinonline.org/HOL/LandingPage?handle=hein.journals/uclalr41&div=41&id=&page=>; see also Zheng et al., *How Causal Information Affects Decisions* (2020) 13 Cogn. Res. Princ. Implic.,

disclosure can crowd out useful information” and focus users on irrelevant considerations.¹⁰⁹ For example, an FTC study showed that a “proposed disclosure of brokerage fees” caused consumers to focus overly on those fees, and thus “overestimate the total cost of loans.”¹¹⁰ Mandatory disclosures are also often too complicated for consumers to understand.¹¹¹ And the situation becomes even worse when disclosures accumulate across products: each decreases the effectiveness of every other one, as they “compete[] for . . . time and attention with [each other].”¹¹² “Even if [consumers] wanted to read all the disclosures relevant to their decisions, they could not do so proficiently,” and they will “soon learn their lesson and give up any inclination they may have had to devote their lives to disclosures.”¹¹³ The upshot is that both the “use of encyclopedic warnings” and the “overuse of warnings” “may, in fact, decrease the effectiveness of all warnings.”¹¹⁴ Excessive disclosures may also lead consumers to simply shut down and avoid interacting with covered businesses at all.¹¹⁵

Here, consumers will at best tune out the annoying barrage of similarly sounding pre-use notices they see every day, and at worst be distracted from the details they actually need to know, like the features and price of a product, the admissions criteria of a university, or an employer’s personnel policies. In no way will they benefit. Consider perhaps the closest analogy to the proposed disclosures, the now-ubiquitous cookie banner that websites display to comply with European regulations. The cookie banner has been a consensus failure for consumer privacy and empowerment, because Internet users have been so inundated with the disclosures that they simply disregard them.¹¹⁶

<https://pubmed.ncbi.nlm.nih.gov/32056060/> (documenting a psychological experiment showing that giving consumers certain “information can actually lead to worse decisions”); Dalley, *The Use and Misuse of Disclosure as a Regulatory System* (2007) 34 Fla. St. U. L.Rev. 1090, 1115, <https://ir.law.fsu.edu/lr/vol34/iss4/2/> (describing “information overload” and how an excess of information can lead decisionmakers to make ill-informed decisions).

¹⁰⁹ Ben-Shahar and Schneider, *The Failure of Mandated Disclosure* (2011) 159 U.Penn.L.Rev. 647, 737, <https://www.jstor.org/stable/41149884>.

¹¹⁰ Craswell, *Taking Information Seriously: Misrepresentation and Nondisclosure in Contract Law and Elsewhere* (2006) 92 Va. L.Rev. 565, 584, <https://virginialawreview.org/articles/taking-information-seriously-misrepresentation-and-nondisclosure-contract-law-and/>.

¹¹¹ Ben-Shahar and Schneider at pp. 665–672.

¹¹² *Id.* at p. 689.

¹¹³ *Id.* at p. 690.

¹¹⁴ Schwartz and Driver, *Warnings in the Workplace: The Need for a Synthesis of Law and Communication Theory* (1983), 52 U.Cin.L.Rev. 38, 43.

¹¹⁵ See Craswell at p. 584; Accenture, *The Empowered Consumer* (2024), <https://www.accenture.com/us-en/insights/consulting/empowered-consumer> (finding that in a three-month period, three quarters of consumers “walked away from purchases simply because they felt overwhelmed” by information).

¹¹⁶ See, e.g., Utz et al., *(Un)informed Consent: Studying GDPR Consent Notices in the Field* (2019), <https://arxiv.org/abs/1909.02638> (studying user behavior in reaction to cookie banners and noting the “[r]ecurring theme[]” “that the notices were ‘annoying . . . , so [users] just ignore them out of

The regulations will also be a costly drag on business. Generating the required disclosures for the pre-use notifications and access rights will be an exceedingly complex task. The proposed regulations require an explanation of “the output of the automated decisionmaking technology with respect to the consumer,” “the role the output played in the business’s decision and the role of any human involvement,” and “how the automated decisionmaking technology worked with respect to the consumer.”¹¹⁷ These disclosures will apparently have to be individualized to each consumer. This poses an immense data-governance and retention challenge. Businesses will have to store detailed information regarding every single “significant decision” made using ADMT, and will have to build systems that can, upon request, parse that data to construct a usable individualized response. This is orders of magnitude more challenging than responding to a request to know or a request to correct, under California law, given the inherent complexity of automated processing. Despite that, the regulations do *not* provide any exceptions when compliance would involve “disproportionate effort” – even though similar exceptions exist for requests to correct, delete, or know.¹¹⁸ Maintaining and processing this data for the entire range of “significant decisions” would necessarily stifle the innovative engines that drive California’s economy. But neither the Agency’s statement of reasons nor its economic analysis addresses these concerns.

And there are yet more reasons why the disclosures will hurt the public that the Statement does not grapple with. To start, the regulations would compel businesses to make statements that are confusing and even misleading. Disclosing the “logic” and “key parameters” of an ADMT in “plain language” may often be an impossible task. The most advanced AI models today have *billions* or even *trillions* of parameters. Their internal logic is just “a long list of numbers.”¹¹⁹ Translating these numbers into human-understandable explanations is far from trivial.¹²⁰ The field

frustration”); O. Kulyk et al., *Has The GDPR Hype Affected Users’ Reaction to Cookie Disclaimers* (2020) 6 J. Cybersecurity, <https://academic.oup.com/cybersecurity/article/6/1/tyaa022/6046452> (studying web users’ behavior and concluding that “participants considered the cookie disclaimer as a nuisance” and so “tend[ed] to accept cookie disclaimers blindly to get rid of it”); M. Nouwens et al., *Dark Patterns after the GDPR: Scraping Consent pop-ups and Demonstrating their Influence* (2020), <https://dl.acm.org/doi/10.1145/3313831.3376321> (“[T]he frequency of the pop-ups caused frustration and consent fatigue.”).

¹¹⁷Draft Regulations, § 7222, subd. (b).

¹¹⁸ Draft Regulations, §§ 7022, subd. (b)–(c), 7023, subd. (f), 7024, subd. (h).

¹¹⁹ Anthropic, *Mapping the Mind of a Large Language Model* (May 21, 2024), <https://www.anthropic.com/research/mapping-mind-language-model>.

¹²⁰ See J. Woods, *Machine Learning Interpretability: New Challenges and Approaches* (Mar. 14, 2022)

Vector Institute, <https://vectorinstitute.ai/machine-learning-interpretability-new-challenges-and-approaches/>; See generally R. Dwivedi, *Explainable Ai (XAI): Core Ideas, Techniques, and Solutions* (2023), 55 ACM Computing Surveys, <https://dl.acm.org/doi/10.1145/3561048>.

of research devoted to this task has made promising advances.¹²¹ But even when sophisticated researchers get a handle on how an advanced AI model works, their explanations have been long and jargon-filled.¹²² And researchers have struggled to convert these explanations into a form understandable by non-expert humans.¹²³ So in many circumstances, any “plain language” explanation of the model’s logic will be overly simplistic and misleading. It is never proper for the government to direct a business to mislead its customers.¹²⁴

There is also ample reason to be concerned that such a disclosure regime could be misused to gain access to confidential business or consumer information. For example, it would be plainly inappropriate to compel the admissions office of a private college to disclose the “logic” and underlying “assumptions” of its admissions policy. A university may reasonably want to keep this information private, to prevent prospective students from gaming the system. But if a school implements or informs its admissions decisions in part using an automated system (as colleges fielding hundreds of thousands of applications necessarily will), it now may have to reveal exactly that confidential information.

Worse still, the disclosure requirements can be misused by malicious actors to gain unauthorized access to personal information. An unfortunately common scenario is that malicious actors use social engineering to obtain consumers’ login credentials for a service.¹²⁵ Under a compelled-

¹²¹ See Anthropic, *supra*; K. Wang et al., *Interpretability in the Wild: A Circuit for Indirect Object Identification in GPT-2 Small* (Nov. 1, 2022), <https://arxiv.org/abs/2211.00593>.

¹²² See, e.g., Wang, *supra* (twelve technical pages to explain how a large language model predicted a single word in a sentence).

¹²³ See H. Siu et al., *STL: Surprisingly Tricky Logic (for System Validation)*, (May 26, 2023), <https://arxiv.org/abs/2305.17258>.

¹²⁴ Cf. *Barton v. Neeley* (6th Cir. 2024) 114 F. 4th 581, 592 (explaining that the First Amendment protects the “right to decide what to say and what not to say, and accordingly, the right to reject governmental efforts to require [someone] to make statements he believes are false”), and *Massachusetts Ass’n of Priv. Career Sch. v. Healey*, 159 F. Supp. 3d 173, 199–200 (D. Mass. 2016) (holding that a regulation requiring a business to make misleading statements was subject to heightened scrutiny under the First Amendment).

¹²⁵ See, e.g., Pavur & Knerr, *GDPArrrrr: Using Privacy Laws to Steal Identities*, Blackhat USA (2019), <https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf> (noting that “social engineers can abuse right of access requests as a scalable attack vector for acquiring deeply sensitive information about individuals”); IBM, *IBM Security X-Force Threat Intelligence Index 2024* at p. 9, <https://www.ibm.com/reports/threat-intelligence> (noting that “the focus has shifted towards logging in rather than hacking in, highlighting the relative ease of acquiring credentials compared to exploiting vulnerabilities or executing phishing campaigns”); *Verizon 2023 Data Breach Investigations Report* (2023) at p. 8, <https://www.verizon.com/about/news/media-resources/attachment?fid=65e1e3213d633293cd82b8cb> (noting that “74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering”); Stahie, *Billions of Leaked Credentials Available on the Dark Web*, Bitdefender (2020) (noting 15 billion credentials available on the dark web), <https://www.bitdefender.com/en-us/blog/hotforsecurity/billions-of-leaked-credentials-available-on-the-dark-web>.

disclosure regime, an attacker with these stolen credentials may now be able to learn even more information about his victim by obtaining the inferences a business has made about her and use that ill-gotten information in furtherance of identity theft or targeted phishing attacks. In this way, the regulations may be more harmful to privacy than enhancing of it.

D. There is no basis to require the onerous risk assessments

The Statement does not contain substantial evidence demonstrating that the extremely detailed and burdensome risk assessments are necessary to further consumers' privacy. Per the statute, the purpose of the risk assessment is to evaluate which instances of data processing have elevated "risks to privacy."¹²⁶ But many of the activities that must be addressed by the risk assessment have no impact on privacy at all. For example, the draft regulations would require each business to discuss the "completeness, representativeness, timeliness, validity, accuracy, consistency, and reliability" of its information sources and the "logic" of certain algorithms. None of these requirements bears any relationship to privacy or security concerns. The Statement does not explain otherwise.

Not only is there no evidence that risk assessments are necessary to advancing privacy and security, but the overbroad compliance regime proposed here would undermine privacy and security.¹²⁷ The risk assessments must address dozens of discrete issues. Undertaking such an extensive assessment anytime ADMT is used for a broad category of "significant decisions" would be enormously resource-intensive. Companies throughout the economy would need to divert resources, including engineering talent, away from substantive risk mitigation and toward producing burdensome risk assessments with little relation to privacy or security. The Statement denies any tradeoff with the blanket statement that "risk assessments are cost effective."¹²⁸ But its only source discusses not the regulations here, but the burdens of complying with Europe's GDPR, an entirely different set of requirements. And even with respect to those requirements, the source does not support the point: it acknowledged that the cost of the GDPR's data-protection assessments may already be "prohibitive," particularly for smaller companies that otherwise could

¹²⁶ Cal. Civ. Code, § 1987.1785(a)(14)(b).

¹²⁷ Nov. 8 CPPA Bd. Hr'g Tr. 99 ("With respect to the risk assessments, I think these proposed regulations will make the inclusion criteria for risk assessments so broad that we will end up hurting the cause of privacy, not helping it. The scope of these regulations effectively mandates risk assessments for almost any business using software. This spread will hurt businesses and overwhelm our agency with, I think, largely form paperwork, diminishing our focus – our ability to focus on enforcement. There's no chance we'll be able to review tens and tens of thousands of multi-page risk assessments at this stage with our current resources.").

¹²⁸ ISOR, p. 71–72.

substantially benefit from automation.¹²⁹ The Agency must promulgate regulations that balance the enhancement of privacy with the promotion of innovation, and since the risk-assessment requirements would do little to improve privacy and stifle innovation, the significant cost imposed by risk assessments is unsupported and unnecessary.¹³⁰

E. There is no basis for the rigid cybersecurity audit requirements

The cybersecurity audit requirements are overly simplistic, in both when they apply and what they entail. The Statement of Reasons fails to show that the draft regulations' blunt requirements are necessary or appropriate.

The thresholds for when an audit is required are unjustified. The thresholds are based on blunt indicators, a business's revenue and number of consumers whose data is processed.¹³¹ These simplistic conditions fail to account for how cybersecurity practices and the need for an audit vary across different industries. For example, strict compliance checklists may be appropriate for a mature institution with a predictable workflow, but counterproductive for a software company with a rapidly evolving product and headcount.¹³² The draft regulations could lead to disproportionate compliance costs for businesses without lowering true risks to consumer security. The Statement does not address this concern.

¹²⁹ Iwaya et al., *Privacy Impact Assessments in the Wild: A Scoping Review* (2024), <https://www.sciencedirect.com/science/article/pii/S2590005624000225>.

¹³⁰ The risk assessments, as envisioned by the proposed regulations, also run afoul of the First Amendment. Courts have repeatedly rejected recent attempts to require disclosures about a company's use of technology and its opinions on whether and how this use maps to ambiguous and often pejorative characterizations. The Ninth Circuit made this point twice in just the last year while striking down remarkably similar California laws. In one case, the law demanded, akin to the present regulations, that certain website operators report on whether "the design of the[ir] online product . . . could harm children" in various specific ways. (*NetChoice v. Bonta* (9th Cir. 2024) 113 F. 4th 1101, 1109.) The requirement was invalid because it compelled "covered businesses to opine on potential harm" of their product outside the context of any specific transaction. In the other case, the State compelled businesses to "implicitly opin[e] on whether and how certain controversial categories of content should be moderated." (*X Corp. v. Bonta* (9th Cir. 2024) 116 F. 4th 888, 901.) Yet this request too was invalid, because the government had no authority to make a company offer "opinions about and reasons for" its policies. The only difference here is that there is nothing "implicit" about what the new regulation asks for. It flat-out tells companies to express an opinion on whether or not their technology fits within the vague and value-laden categories in the regulations and, if so, the merits and drawbacks of their own policies. But this is well past the range of speech that a government can legitimately compel.

¹³¹ Draft Regulations, § 7120.

¹³² Wallace, *The Importance of Cybersecurity by Industry*, <https://www.uscybersecurity.net/the-importance-of-cybersecurity-by-industry>; Cristiano and Prenio, *Regulatory approaches to enhance banks' cyber-security frameworks* (2017), <https://www.bis.org/fsi/publ/insights2.pdf>.

And when audits are required, the mandated components are problematically rigid. The particular approaches that work in one industry or for one particular size of business may backfire elsewhere.¹³³ Moreover, the detailed cybersecurity audit requirements set forth in the regulations – including dozens of discrete requirements – would, at best, introduce a box-checking exercise and, at worst, distract businesses from focusing on actually optimizing security and keeping sensitive information safe.¹³⁴

III. The Proposed Regulations Lack Clarity

Regulations must be easy to understand and follow,¹³⁵ and “due process also requires that regulations be written with sufficient clarity so that those subject to the law can understand what is required or prohibited.”¹³⁶ But complying with the proposed regulations will require herculean guesswork. The regulations leave California businesses to puzzle over whether and when the regulations apply and, if they do, how to comply.

First, the **definition of ADMT** is troublingly vague. The flexible terms “execute,” “substantially facilitate,” and “key factor” provide little guidance to businesses about what qualifies as ADMT. It may be difficult to assess whether a particular output of a technology plays a “substantial” or “key” role in a decision, particularly when the technology merely informs human decisionmaking; there may be no agreed-upon way to quantify the weight that a factor plays in a human decision. The examples only compound this indeterminacy. Section 7001(f)(2) states that ADMT “substantially facilit[es] human decisionmaking” when it is used “to generate a score about a consumer that a human reviewer uses as a primary factor to make a significant decision.” But in Section 7001(f)(4), the regulations indicate that using technology to “calculate” a “score that [a] manager will use to determine which [employee] will be promoted” is not even a use of ADMT. The regulation appears to discern between “generating a score” for the purpose of guiding a human

¹³³ Etoom, *Strategising cybersecurity: Why a risk-based approach is key* (2023), <https://www.weforum.org/stories/2023/04/strategizing-cybersecurity-why-a-risk-based-approach-is-key/>; Boehm et al., *The risk-based approach to cybersecurity* (2019), <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity>.

¹³⁴ Marotta and Madnick, *Convergence and divergence of regulatory compliance and cybersecurity* (2021), https://doi.org/10.48009/1_iis_2021_10-50 (“regulatory compliance can negatively affect cybersecurity”); Sjouwerman, *5 Reasons Why Compliance Alone Is Not Efficient at Reducing Cyber Risks* (2022), <https://www.corporatecomplianceinsights.com/compliance-not-enough-cybersecurity-risk/>; Internet Security Alliance, *Cyber Regulations Are Counter-Productive to True Security* (2021), <https://isalliance.org/cyber-regulations-are-counter-productive-to-true-security/>.

¹³⁵ Gov. Code, § 11349, subd. (c); *FCC v. Fox Television Stations, Inc.* (2012) 567 U.S. 239, 253 (same under Due Process clause).

¹³⁶ See *FCC v. Fox Television Stations, Inc.* (2012) 567 U.S. 239, 253.

decision and “calculating a score” for that same purpose, but without any meaningful explanation of how the two are different.

Section 7001(f)(4) likewise creates confusion as to what “technology” is in scope. It alternately says that “calculators,” “spreadsheets,” and “similar technologies” are *not* ADMT, then asserts that the “use of a spreadsheet to run regression analyses” *is* ADMT if used by humans evaluating job performance, but then says that it is *not* ADMT if it “merely . . . organize[s] human . . . evaluations.” As we noted above, the distinction between “regressions” and “calculators” is wholly unclear, and a business has little hope at guessing which side of the line its software falls on. The Agency’s attempt to explain the regulation only adds confusion because “the language of the regulation conflicts with the agency’s description of the effect of the regulation.”¹³⁷ These artificial distinctions underscore the unworkability and ambiguity of the proposed definition of ADMT.

Second, the term “**significant decision**” also lacks clarity. The specific categories that count as “significant” are problematically vague. For example, what does it even mean for a decision to “result[] in access to, or the provision or denial of . . . criminal justice”? The regulations do not say, beyond offering the single example of the “posting of bail bonds.” Suppose a security firm guarding a semiconductor factory uses an AI tool to decide which visitors must go through extra screening. Since the security screening could theoretically discover evidence of a crime and lead to a prosecution, does the company’s use of AI fit the definition? It is likewise unclear what decisions count as affecting “housing.” If a college assigns roommates using software that considers students’ personal preferences, does it have to conduct a risk assessment and offer an opt-out? Or does housing extend only to the purchase or lease of real property? And what counts as an “essential good or service”? The regulations provide a handful of examples (groceries, medicine, hygiene products, or fuel) but what else should be considered “essential” and how is that decided? Is Internet access essential? Cultural opportunities? Firearms? And even if a good is unequivocally “essential,” which decisions affect “access” to it? Do the regulations cover every single transaction related to that good (for example, a grocery store’s denying a consumer access to one particular foodstuff on one occasion)? Or does a decision count only when it wholesale excludes a consumer from the good (like if the only utility company that services a consumer’s home disconnects the power)? The proposed definition of “significant decision” creates more questions than it answers.

¹³⁷ Office of Administrative Law, OAL Review for Compliance with the Six Substantive Standards of the Administrative Procedure Act, § 3.03 (Apr. 2023), <https://oal.ca.gov/wp-content/uploads/sites/166/2023/04/OAL-Review-for-6-APA-Standards.pdf>.

Third, the proposed **pre-use notice** and **right to access** regulations likewise fail to explain how those disclosures would function. The pre-use notice and any response to a request to access may not “describe the purpose in generic terms” and must include information about the logic, key parameters, and output of the ADMT, which must be in “plain language.” But, as discussed above, automated decisionmaking technology, including artificial intelligence, often involves dynamic and constantly evolving, highly technical systems that can consider hundreds of inputs of variable weights that lead to a range of different outputs. And businesses may be constantly tweaking and testing their technology to optimize for different circumstances or to account for changes in the marketplace. And as discussed above, translating any given iteration of an ADMT system into plain English may be an impossible task. The regulations provide no guidance on how to provide accurate and digestible information given this highly complex backdrop.

* * *

We appreciate this opportunity to share some of our concerns with the Agency and hope that the Agency will revise the proposed regulations to focus on the privacy and security concerns expressed by the People of California in approving Prop. 24.

Respectfully submitted,



Ashlie Beringer

Partner

Co-Chair of the Privacy, Cybersecurity and Data Innovation Practice Group



Jane Horvath

Partner

Co-Chair of the Privacy, Cybersecurity and Data Innovation Practice Group



Cassandra Gaedt-Sheckter

Partner

Co-Chair of the Artificial Intelligence Practice Group

Grenda, Rianna@CPPA

From: Elizabeth Banker <bankere@google.com>
Sent: Monday, June 2, 2025 4:58 PM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: Final Google Comments on CCPA Regs 6022025.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](#)

Please accept the attached comments from Google with regard to: CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations.

Thank you for your attention to this matter.

Best,
Elizabeth

--



Elizabeth Banker [she/her]
Government Affairs & Public Policy
bankere@google.com | 415.523.0142

June 2, 2025

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

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

To whom it may concern:

Google appreciates the California Privacy Protection Agency's ("Agency") thoughtful and calibrated approach reflected in its Modified Text of Proposed Regulations related to automated decisionmaking technology, risk assessments, and other updates to the existing regulations released for public comment on May 9, 2025 (herein "Modified Proposed Regulations").

In our initial comments, we urged the Agency to craft regulations with three goals in mind, each of which was echoed by members of the Board and voices of the community throughout the rulemaking to date:

1. Prioritize clarity around obligations under the statute over introducing new, additional obligations not expressly required by the law;
2. Provide flexibility where possible about how to comply with the law in a manner that prioritizes substance over form; and
3. Seek to align rules with existing national and global standards to facilitate consumer understanding and promote privacy-preserving business practices.

We thank the Agency for its diligent attention to these goals and to the issues previously raised by Google and others in preparing the Modified Proposed Regulations, which reflect critical updates – including seeking to scope ADMT-specific obligations to processing that presents risk of harm to consumers and bringing risk assessment obligations in line with those imposed in other jurisdictions while still protecting consumers' privacy.

While the Modified Proposed Regulations reflect substantial progress toward addressing these goals, we agree with CalChamber and others in the business community that the Agency should continue to be mindful of Governor Newsom and the state legislature's efforts to regulate automated processing systems and should consider further narrowing its proposed regulations (such as by removing training altogether and substantially paring back ADMT-specific access obligations). In our comments, we have chosen to focus on a narrower set of concerns and proposed changes where we believe the regulations would benefit from further clarity, flexibility, and alignment with other legal frameworks. Below, we explain these concerns and suggest corresponding changes, grouped under three topics: 1) the definition of ADMT; 2) the types of processing that trigger risk assessment obligations; and 3) procedures for conducting and submitting risk assessments.

1. ADMT definition

By limiting ADMT-specific obligations to decisions that do not involve human review and that are used to make significant decisions, the Modified Proposed Regulations appropriately pare back the scope of ADMT obligations to be in line with legislative intent, similar legal frameworks adopted around the globe, and sound policy goals. However, the statement in § 7001(e)(2) that ADMT “includes profiling” could cause some confusion and potentially undermine these goals, particularly given the broad definition of “profiling” (which is *not* limited to profiling for significant decisions¹). Accordingly, we suggest that the Agency clarify the ADMT definition to explain that it includes “profiling” only to the extent that profiling is used to make a decision with significant effects. This clarifying change will advance business understanding; without it, businesses may face uncertainty over whether even banal processing activities, such as personalizing the content shown to consumers using solely data collected in a first-party context, require adherence to the ADMT-specific obligations set forth in the regulations.

Suggested Changes:

Revise § 7001(e)(2) as shown: “ADMT includes profiling **when used to make a significant decision.**”

2. Risk Assessment Triggers

a. Sensitive Locations

The Revised Proposed Regulations appropriately narrow the scope of processing concerning observation of consumers in public places to “sensitive locations.” Google applauds this change, which advances sound policy goals and aligns with other privacy laws that, for example, prohibit collecting information about visits to reproductive care facilities for purposes of inferring health interests about consumers or showing them ads on the basis of such visits.² However, the regulations should make clear that in order to trigger risk assessment obligations, the business must actually identify a consumer as visiting a sensitive location and use information about that sensitive visit for profiling purposes. Without that change, companies that process precise location information for any purpose could risk coming in scope, particularly given the proximity that sensitive locations often share with non-sensitive ones (e.g., a large office building that contains an OBGYN clinic, retail shops, restaurants, and offices for dozens of companies). Moreover, some location data may not be precise enough to identify a user in a sensitive location but rather be in the proximity of such location. While we appreciate the Agency expressly carving out processing for delivering goods or providing transportation, other routine processing that presents no risk of harm to consumers (such as providing directions or navigation functionality to a doctor’s office without making any health-related inference from

¹ Modified Proposed Regulations § 7001(ii).

² See e.g., Wash. Rev. Code Ann. § 19.373.030 (West 2025); Conn. Gen. Stat. Ann. § 42-526 (West 2025).

such processing, noting a visit to a pet store to infer interest in pets when such store happens to be next to a doctor's office, or processing a request for "cafes near me" from a consumer sitting in a doctor's office) could come into scope without further revisions. In addition, while much of the definition of "sensitive location" set forth in the Modified Proposed Regulations is clear and in line with other legal frameworks, the definition includes some vague references such as "legal services offices" and "educational institutions" that are not clear and are out of line with such norms. Google recommends that the Agency revise this definition to ensure that the regulations remain focused on harm avoidance and make businesses' obligations clear.

Suggested Changes:

§ 7150(b)(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 **known or inferred** presence in a sensitive location. "Infer or extrapolate" does not include a business using a consumer's personal information **to make inferences that do not relate to the sensitivity of the location, such as solely to provide goods or services requested by the consumer, to deliver goods to, or provide directions to or transportation for, that consumer at a sensitive location. For example, a consumer's presence in a sensitive location is not "known or inferred" by a business if:**

- (A) The business infers an interest in pets based on a visit to a pet store that happened to be next to an urgent care facility; or**
- (B) The business provides a service regardless of location sensitivity, such as to deliver goods, provide directions or transportation to a sensitive location, and does not infer sensitive personal information based on that consumer's presence at a sensitive location.**

§ 7001(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.~~

b. *Physical or Biological Identification or Profiling*

The Revised Proposed Regulations have narrowed the scope of ADMT training activities that trigger the obligation to conduct a risk assessment, but should go further as noted by CalChamber in their submission. We would like to particularly highlight that the draft still contemplates the need to conduct risk assessments for training of ADMT systems outside of systems that 1) make significant decisions or 2) are used for physical or biological identification of consumers through an overly broad definition of "physical or biological identification or profiling" that can be read to contemplate use of emotion recognition even when not used to make a significant decision nor to identify or recognize a consumer. While Google agrees that emotion detection systems should be subject to risk assessment obligations when used to make significant decisions such as related to employment (as the example set forth in § 7150(c)(1)

contemplates) or to identify consumers, there is no basis to require such an assessment when technology is not used for such purposes. We suggest the clarifying changes below to align the regulations with legislative intent and similar privacy frameworks.

Suggested Changes:

§ 7150(b)(6): Processing the personal information of consumers, which the business intends to use to train an ADMT 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, 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.

§ 7001(ee): "Physical or biological identification ~~or profiling~~" means 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 **to identify or infer a consumer's identity**. This includes using biometric information, vocal intonation, facial expression, and gesture **for such purposes** ~~(e.g., to identify or infer emotion)~~. This does not include processing **of** physical or biological characteristics **for a purpose other than** ~~that do not identifying, and cannot reasonably be linked with,~~ a particular consumer.

§ 7001(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.

3. Procedures for Conducting and Submitting Risk Assessments

a. Stakeholder Participation

Google recognizes the flexibility the Agency has provided businesses in conducting risk assessments contemplated by the Modified Proposed Regulations. However, the draft seems to contemplate both involvement and documentation of a potentially broad spectrum of individuals -- obligations that would add substantial burden on businesses and the Agency with little or no corresponding consumer benefit. For example, § 7151(a) the Modified Proposed Regulations states that individuals 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 all individuals who provided the information for the risk assessment, barring only legal counsel from this obligation. In large organizations, countless 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 would take enormous time and resources and would not add to the veracity of the risk assessment, because some may not have a complete picture and others will have overlapping information. Instead, 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 may include, for example, an individual who has the authority to participate in deciding whether the business will initiate the processing that is the subject of the risk assessment.

Suggested Changes:

§ 7151(a): **Individuals who are primarily responsible for** ~~A business's 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** business's risk assessment process for that processing activity. For example, an individual who **is primarily responsible for** determining the method by which the business plans to collect consumers' personal information for one of the processing activities in section 7150, subsection (b), must **facilitate the provision of** that information to the individuals conducting the risk assessment.

§ 7152(a)(8): Identify and document in a risk assessment report the individuals who **have authority to participate in deciding whether the business will initiate the processing that is subject to** ~~provided the information for~~ the risk assessment, except for legal counsel who provided legal advice.

b. Risk Assessment Submissions

Google appreciates the Agency's recognition of the burden its prior draft regulations would have imposed both on businesses and on the Agency and its efforts to address those burdens while still protecting consumers, in particular by removing the obligation to submit an "abridged" risk assessment. By and large, the information the Agency contemplates businesses providing in the Modified Proposed Regulations appropriately strikes this balance. However, the Modified Proposed Regulations continue, in places, to prioritize form over substance and would impose substantial burden with little, if any, corresponding consumer benefit. First, the proposed requirement in § 7157(b)(4) for businesses to document and submit information about whether the risk assessment involved the processing of each of the categories of personal information and sensitive personal information set forth in the CCPA would add needless paperwork challenges and would be out of line with the requirements of other privacy laws, which while covering the same sorts of personal information and sensitive personal information, do not refer to the same categories as does the CCPA. Second, 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 somehow link each risk assessment and update thereto to individual processing activities notwithstanding that processing activities may cross over multiple risk assessments and a single risk assessment may cover multiple processing activities. Third, 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). Here too, minor revisions to the Modified Proposed Regulations would bring them in line with requirements of similar frameworks and help prioritize substance over form.

Suggested Changes: Strike § 7157(b)(4) and § 7155(a)(2) in their entirety and edit § 7157(b)(3) as shown: “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).~~”

* * * * *

We appreciate the opportunity to provide comments on the Modified Proposed Regulations, and we look forward to continued collaboration with the Agency on these important issues.

Sincerely,

Will DeVries
Director, Regulatory Affairs - Privacy Advisory

Grenda, Rianna@CPPA

From: Angel Lin <angel.lin@greenlining.org>
Sent: Friday, May 30, 2025 3:39 PM
To: Regulations@CPPA
Cc: Monica Palmeira; Rawan Elhalaby
Subject: Greenlining Institute's Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: Greenlining Comment to the CPPA Re Rulemaking .pdf

This Message Is From an External Sender

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

Report Suspicious

Greetings,

I am submitting public comment on behalf of The Greenlining Institute regarding the proposed text for CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations. Please reach out for any questions or requests for additional information.

Best,
Angel Lin

--



Angel Lin
Tech Equity Fellow
Email: angel.lin@greenlining.org
Pronouns: she/her
[Twitter](#) | [LinkedIn](#) | [Website](#)

June 2, 2025

Tom Kemp

Director, California Privacy Protection Agency
400 R Street, Suite 350
Sacramento, CA 95811

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

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

The Greenlining Institute (“Greenlining”) appreciates the opportunity to provide comment to the California Privacy Protection Agency (“CPPA” or “Agency”) on proposed regulations for the California Consumer Privacy Act (“CCPA”), Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (“ADMT”), and Insurance Companies. Greenlining’s advocacy is rooted in our commitment to advance a more just economy for communities of color, where we work towards a future where race is never a barrier to opportunity. In order for us to arrive at this future, we recognize that it is imperative for the regulatory agencies governing our emergent technologies to be empowered with the rules and authority to meaningfully protect consumers’ rights.

California voters recognized this as well. In 2020, the majority of voters declared that the information asymmetry between consumers and businesses was inequitable. As a result, they voted in favor of Proposition 24, creating the very CPPA that sits here today. Californians have trusted the Agency with the responsibility of protecting and strengthening their privacy rights against potentially predatory industry practices. The CPPA promised it would work to give consumers *meaningful control* over how their information was used.

Unfortunately, today’s iteration of the proposed regulations does the opposite. Rather than drafting rules that target the harms arising from the largely unregulated use of consumer data—specifically inaccurate or biased automated decision making—the CPPA may have been influenced to soften their previously proposed language to render itself effectively toothless against industry abuses. Wholesale adoption of industry arguments only reinforces the very power asymmetry that Californian voters sought to eliminate in the first place with Proposition 24. We are concerned that the most recently proposed language may indicate the CPPA is prioritizing industry motives over reasonable consumer protections.

In order to reaffirm the CPPA’s commitment to consumer protection, we recommend taking the following actions specific to the definition of ADMT and how risk is being assessed. We also support comments from our partners at ACLU California Action, Privacy Rights Clearinghouse, Consumer Federation, Epic, and the Electronic Frontier Foundation on issues specific to civil rights and other key constituencies.

Proposed Definition of ADMT Still Leaves Consumers Vulnerable to Algorithmic Bias

The proposed decision to change the definition of ADMT from a technology that will “substantially *facilitate*” human decisionmaking to one that will “substantially *replace*” human decisionmaking is a clear attempt to exempt major ADMT use cases from this regulation. These edits, and the subsequent explanation of “substantially replace,” imply that any automated decision-making process that includes the bare minimum of human involvement is somehow free from risk.

In many major use cases where ADMT is used in tandem with human-in-the-loop decision making, algorithmic discrimination still takes place. For example, in automated home valuation programs, Black homeowners living in formerly redlined neighborhoods are consistently given home appraisals 21-23% lower than similar white homeowners.¹ In hiring processes where AI-enabled recruitment and interview technologies are used, applicants with ‘Black-sounding names’ are placed at a disadvantage.² In loan-lending, when algorithms generate interest rates, Black applicants end up with interest rates that are 5.6% higher than their white counterparts.³

In each of these cases where algorithms inflict major, life-impacting harm, human involvement still exists: licensed appraisers sign off on automated valuations before presenting them to homeowners; HR executives make final hiring decisions based on AI-filtered candidate pools; and loan officers approve applications with algorithmically-determined interest rates. Humans remain involved in nearly all cases where algorithmic bias causes the most severe harm, yet this ruling fails to address or minimize the documented discrimination we have witnessed over the past decade. The presence of human oversight has not prevented these systematic patterns of bias from occurring.

Automation Bias Still Leads to Algorithmic Bias

Industry lobbyists may also make the argument that incorporating human oversight into automated decision-making processes renders additional regulatory intervention unnecessary, arguing that human reviewers can effectively identify and correct biased algorithmic outputs. This position assumes that human actors possess both the technical expertise and institutional awareness needed to recognize problematic decisions and intervene appropriately. Unless the entirety of California’s workforce is suddenly imbued with a deep understanding of algorithmic infrastructure and decades of robust experience in their respective industries overnight, this assumption does not hold water.

In practice, many automated systems are deployed in emerging use cases where established expertise may not exist, or are overseen by personnel who lack the specialized knowledge required to effectively audit algorithmic outputs. The average human reviewer—whether a customer service representative, loan

¹ <https://www.naacpldf.org/appraisal-algorithmic-bias-racial-discrimination/>

² <https://ojs.aaai.org/index.php/AIES/article/view/31748/33915>

³ <https://www.sciencedirect.com/science/article/abs/pii/S0304405X21002403>

officer, home appraiser, or HR staff member—typically receives minimal training on the technical aspects of the automated systems they're supposed to oversee. It is unrealistic to expect average users to possess the domain expertise necessary to identify subtle forms of bias or systematic errors that require intervention. The burden of this expectation should fall onto developers.

Furthermore, as artificial intelligence becomes the new workplace standard, the risk for automation bias grows. When confronted with ADMT-generated outputs, human users—both novice and expert—will often over rely on the algorithms' provided decision, rather than trusting their own judgement.⁴ Research shows that this automation bias is more likely to take place when the generated outputs adhere to preexisting stereotypes about groups and social identities, like race and gender; irresponsible systems that leave the door open for complacency and automation bias are more likely to harm communities of color.⁵

Combatting automation bias requires deliberate product design, decision-making transparency, and reasonable guidelines about the volume of tasks that the users are expected to complete. The proposed regulations offer developers no mandate to implement these components into their ADMT. Without an explicit mandate, companies use ADMT to maximize the output of their employees without regard for the harms of automation bias. For example, when the health insurance company Cigna implemented ADMT in their claims-approval process, doctors spent an average of 1.2 seconds scanning patient cases before "reviewing" each request.⁶ Former Cigna doctors testified that the system was used to quickly deny claims without any substantive medical review.

Developers and industry lobbyists may try to argue that these ADMT are less discriminatory than humans and, therefore, humans *should* have less oversight in major decision-making processes. Whether or not these claims are true, the fact of the matter is that a biased or inaccurate ADMT can create significantly more harm at mass scale than one bad human decision-maker. In the case of Cigna, after policyholders appealed their denied requests, it was revealed that the ADMT had an 80% error rate—an oversight that was rubber stamped by the 1.2 seconds of menial "human involvement."

With only the vague definition of "human involvement" proposed in sections § 7001.e.1.A-C, companies are given immense discretion as to what bare minimum human involvement can look like. The proposed regulations also fail to provide any specification as to what it would mean for a human actor to "know how to interpret and use the technology" or "review and analyze the output of the decision." There are no benchmarks listed about the human actor being able to articulate the ADMT's decisionmaking logic, identify biases and vulnerabilities in the data, recognize flawed target variables and mitigation strategies. In its current state, the proposed regulations assume these humans are qualified simply by virtue of being there. This is self-regulation in its most irresponsible and vague form.

⁴ <https://journals.sagepub.com/doi/10.1177/0018720810376055>.

⁵ <https://academic.oup.com/jpart/article/33/1/153/6524536?login=false>

⁶ <https://apnews.com/article/cigna-california-health-coverage-lawsuit-4543b47cd6057519a7e8dc6d90a61866>

In the event that the CPPA retains this proposed definition of ADMT, we urge the agency to develop a more rigorous definition of "human involvement" that accounts for and mitigates the well-documented risks of automation bias.

The Board should align with the existing California definition of automated decisionmaking systems, which more appropriately captures systems that can cause harm to consumers and workers. The "Alternative 1" definition from the April 4, 2025 board meeting,⁷ aligns with existing state definitions of automated systems, and would capture harmful systems that the current narrow definition excludes. For example, an AI system that generates hiring and interview recommendations based on applicant profiles—even if a human reviewer technically makes the "final" decision—would be covered under this definition but could easily escape regulation under the draft definition if a company claims minimal human review exempts them from the definition of ADMT.

If the Board proceeds with the current definition, it must ensure that "human involvement" is truly meaningful rather than perfunctory. The current definition's requirements are insufficient to prevent companies from implementing token human oversight. The proposed regulation should require that human reviewers have sufficient resources, and time, in addition to authority, to meaningfully review automated decisions. The Board should incorporate this language requiring that human involvement be substantive, not merely procedural. The text should read:

- (1) 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.
- (2) 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, including a thorough description of the technologies' decisionmaking logic provided by the developer; and
 - (C) Have the sufficient authority, resources, and time to make or change the decision based on their analysis in subsection (B).

Consumers Deserve Notice of Adverse Significant Decisions

Consumers ought to receive additional notice and access to an ADMT when they are subject to an adverse significant decision. This is the bare minimum for establishing consumer protection against biased ADMT and meaningful control over sensitive data. We urge the CPPA to restore § 7222.k.1-3 and codify this right.

⁷ 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 processes personal information and is used to assist or replace discretionary human decisionmaking and materially impacts consumers.

Adverse significant decision notifications are essential to minimizing the effects of algorithmic discrimination. When individuals are denied a job, loan, housing, or public benefit due to an automated system, clear notice ensures they understand that an algorithm played a role and enables them to assess whether the decision was fair or lawful. Without notice, affected individuals have no way to identify potential bias, request an explanation, or contest the outcome—effectively stripping them of due process. These are protections that similar data disclosure rules, such as the Fair Credit Reporting Act, offer consumers.⁸ Adverse significant decision notifications should be the baseline of consumer protection.

Moreover, notice requirements promote accountability among system developers and deployers by creating a feedback loop incentivizing them to monitor for discriminatory outcomes and improve system fairness. In policy terms, notice is not only a matter of transparency but a necessary condition for oversight, equitable treatment, and the enforcement of civil rights in the digital age.

We urge the CPPA to restore § 7222.k.1-3 and empower consumers' fundamental right to notice, as laid out in the expectations of Proposition 24.

Conclusion

California has the opportunity to lead the nation in establishing meaningful protections against algorithmic bias. We respectfully urge the CPPA to strengthen, rather than weaken, these critical consumer safeguards by maintaining robust notification requirements, rejecting overly narrow definitions that exclude consequential automated systems, and recognizing that true consumer protection requires transparency and accountability—not merely the presence of humans who may defer to biased algorithmic outputs.

The stakes are too high, and the evidence of harm too clear, to retreat from the comprehensive approach that these regulations originally promised. We ask the CPPA to prioritize consumer protection over industry convenience and ensure that California's regulations fulfill their intended purpose of preventing algorithmic discrimination.

With Regards,

Angel Lin
Tech Equity Policy Fellow

Mobile: [REDACTED]
Email: angel.lin@greenlining.org
Pronouns: she/her

⁸ <https://www.consumercomplianceoutlook.org/2013/second-quarter/adverse-action-notice-requirements-under-ecoa-fcra/>

Grenda, Rianna@CPPA

From: Marie-Charlotte Roques-Bonnet <mariecharlotte@idside.eu>
Sent: Monday, May 12, 2025 6:51 AM
To: Regulations@CPPA
Subject: ID side comments - CCPA regulation update - ADMT & opt-out signals
Attachments: File Attachment: CCPA PUBLIC CONSULTATION IDside-Comments2-May2025.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 teams,

ID side is grateful for the chance to contribute to the formal public consultation for modifications to the text of proposed regulations for updates to existing CCPA regulations, cybersecurity audits, risk assessments, automated decisionmaking technology (ADMT), and insurance companies.

Thanks a lot for your time and interest in envisaging the set of additional comments attached.

Best regards,

Dr Marie-Charlotte BOUQUET
ID side Principal & Product Lead



ID side comments to CCPA PUBLIC DRAFT on the
“PROPOSED TEXT (CCPA Updates, Cyber, Risk, ADMT, and Insurance
Regulations)”

May 12, 2025



1. Our Organization in a nutshell

ID side is a French independent start-up created in 2019, right after the adoption of the GDPR in EU, by 3 associates: an expert in Privacy ([Marie-Charlotte Roques-Bonnet](#), 20 years' experience), an expert in Security ([Alain Pannetrat](#), 20 years' experience) and a Data visualisation expert ([Damien Bouquet](#), 15 years' experience).

We created ID side with the objective to give control back to internet users over commercial targeting online, empower them to set their privacy Choices in few clicks & **share their specific commercial interests seamlessly online**. Our goal is to foster ethically & environmentally sustainable business models and facilitate qualitative exchanges between individuals and the Companies they trust or like.

The objective of ID side is also to help anyone effectively set their choices online (i.e. regarding Privacy, Safety, commercial preferences or Artificial Intelligence) and exercise their privacy rights seamlessly and automatically.

After years of Research and patenting our Tech, including in the US, we decided in 2024 to shift our main focus from a tool automatically sharing our reasonable expectations regarding “Cookie banners” (see our PoC on [idside.eu](#) / and the page [idside.eu/cookies](#)) to:

- Designing the second prototype for our “Personal Data Choices Management Platform” with the view of “sandboxing” it;
- launching a new “personal and private marketplace” -to be rolled out in February- so that individuals can easily set their commercial & algorithmic preferences (ID side app on iOS and Android).

On the long-run, ID side promotes an alternative and user-centric approach to online commercial targeting that we call the **Light Web**. In 2020, online commercial personalisation & ad targeting worked as follows:

- My data is collected online 24/7.
- It is sold so that ads get better directed to me.
- Companies sell such data without giving me control.

With ID side, and the Light Web model, individuals are empowered to take control over their data & ads displayed to them. They decide:

- How they want personal data to be collected online (our cookie banners extension).
- By Whom, When and How they want to be targeted (our personal & private marketplace).

- Which Companies they want to create a trusted relation with.

In conclusion, our Research, Proof of Concepts (auto-filling of cookie banners) and latest prototypes (a personal and private marketplace) promote the **Light Web**, that is to say a digital business model in which there are less data collected “in my back”, I have more control on targeting & ads and companies unleash the benefits of an alternative **ethically & environmentally sustainable model**.

2. Why is it relevant for ID side to contribute to CCPA Public consultation?

ID side team has a sound expertise in data protection and struggles to advance digital fundamental rights' state of the art tools -specifically with regards to individual-choices-automatic-sharing-online. Its [“Personal Data Choices Management Platform”](#) is designed to empower internet users to share opt-out signals about any individual choice or right (regarding Privacy, AI, safety or any other right) and their commercial preferences (into brands, products, sectors), which is part of the mechanisms that could be relevant to this consultation.

Separately, our team noted in “7025. Opt-out Preference Signals” (a) (2) that *“The configuration or disclosure does not need to be tailored only to California or to refer to California”*. In the light of our germinating exchanges with DAA about Webchoices 2.0 Token ID, we considered it was relevant to share about our Technology and prototypes.

3. Consultation scope & specific provisions at stake

ID side team recognizes the significance of the consultation and the CCPA's role in advancing tech-enabled privacy rights globally and in practice. We also express appreciation for the opportunity to provide additional comments specifically about “Opt-out preference signals” and consumer consent & rights online.

Our contribution will mainly focus on:

1. Definition (1).
2. Sharing of preferences signal online: “7025. Opt-out Preference Signals”, and specifically (c)(1), (c) (2) and example D.

4. Our additional comments

A. Definitions: “Physical or biological identification or profiling”

While we appreciate the effort to clarify these terms, we urge the CPPA to clearly differentiate between **“profiling”** and **“physical or biological identification”** in the final rulemaking, as they are distinct concepts with different privacy implications. To avoid ambiguity, the CPPA should **separately define** “physical or biological identification” (biometric recognition) and “physical or biological profiling” (emotion/gesture analysis).

Indeed, the definition of **“Profiling”** is clearly set by CCPA (§ 1798.140(ai)) as *“any form of automated processing performed on personal information to evaluate certain personal aspects relating to a natural person, including to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.”*

Profiling is inherently **predictive and evaluative**, focusing on behavioural, economic, or personal traits rather than direct physical or biological measurements.

On the contrary, the definition of "Physical or Biological Identification" relies on the automated recognition, authentication, or verification of an individual's identity based on measurable, intrinsic physical or biological characteristics, such as fingerprints, facial geometry, iris patterns, voiceprints, DNA, or other biometric data. Unlike profiling (which infers traits, behaviors, or preferences), identification serves to uniquely distinguish or confirm a specific person, typically by comparing captured data against a stored template or reference record. This process does not include predictive analysis or evaluation of personal aspects unrelated to identity confirmation.

In a nutshell, **identification** (e.g. biometric authentication) and **profiling** (e.g. emotion inference) serve fundamentally different purposes. **Identification verifies or recognizes an individual**, while **profiling infers characteristics or behaviors**.

WE therefore encourage CCPA teams to clarify that **profiling under CCPA § 1798.140(ai)** pertains to behavioral predictions, whereas **biometric identification** (e.g., facial recognition for access control) is a separate use case and ensure consistency with existing CCPA definitions to prevent overlap that could create compliance uncertainty.

B. Consumer Preferences: 7025. Opt-out Preference Signals.

1/ As set in c) 1., *"The business shall treat the opt-out preference signal as a valid request to opt-out of sale/sharing submitted pursuant to Civil Code section 1798.120 for that browser or device and any consumer profile associated with that browser or device, **including pseudonymous profiles**".* We believe there is no easier method than Personal data Choices Management Platforms (PDCMPs) -which are based **on pseudonymous profiles**- to help individuals share their preferences seamlessly and access it easily.

To uphold meaningful consumer control, privacy preferences (e.g., opt-outs from sale/sharing, biometric data restrictions) must persist across websites, devices, and platforms—ensuring choices travel with the individual, not the browser or IP address. However, to prevent circumvention via tracking tactics like fingerprinting or reverse-engineering identities, these preferences should be linked to **strong pseudonymized identifiers** (e.g., cryptographic tokens or rotating, non-PII-based keys). Such identifiers must be: (1) **unique to the user** but not reveal raw identity data, (2) **resistant to linkage** with other datasets (e.g. via salting or zero-knowledge proofs), and (3) **revocable** to mitigate re-identification risks. This approach balances portability with security, closing loopholes that allow covert profiling while respecting user intent.

Critically, pseudonymized identifiers provide robust safeguards to prohibit correlating identifiers with behavioral data, mandatory transparency about their use, and technical constraints preventing cross-context accumulation. By anchoring privacy choices to these identifiers, regulators can foster interoperability (e.g. across CCPA's opt-out signals and Global Privacy Control) without enabling surveillance-by-default.

Therefore, we would respectfully recommend that the draft would strengthen the added value of pseudonymisation as follows: *"The business shall treat the opt-out preference signal as a valid request to opt-out of sale/sharing submitted pursuant to Civil Code section 1798.120 for that browser or device and any consumer profile associated with that browser or device. **We recommend strong pseudonymisation techniques would be used, notably to avoid reverse-tracking & fingerprinting and to promote a secured user-centric approach**".*

2/ Regarding § 2) ("*... However, if the consumer does not respond, the business shall still process the opt-out preference signal as a valid request to opt-out of sale/sharing for that browser or device and any consumer profile the business associates with that browser or device, **including** pseudonymous profiles*"), we reiterate our previous comment and suggest there would be a recommendation such privacy signals would be associated with a strong pseudonymisation feature -so that reverse-tracking or fingerprinting would be impeded.

We respectfully suggest that the text would be amended as follows: ("*... However, if the consumer does not respond, the business shall still process the opt-out preference signal as a valid request to opt-out of sale/sharing for that browser or device and any consumer profile the business associates with that browser or device. **We recommend strong pseudonymisation techniques would be used, notably to avoid reverse-tracking & fingerprinting and to promote a secured user-centric approach***".

3/ Our final comment concerns Example D ("*Ramona participates in Business P's financial incentive program where she receives coupons in exchange for allowing the business to pseudonymously track and share her online browsing habits with marketing partners. Ramona enables an opt-out preference signal on her browser and then visits Business P's website. Business P knows that it is Ramona through a cookie that has been placed on her browser but also detects the opt-out preference signal. Business P may ignore the opt-out preference signal and notify Ramona that her opt-out preference signal conflicts with her participation in the financial incentive program and ask whether she intends to withdraw from the financial incentive program. If Ramona does not affirm her intent to withdraw, Business P may ignore the opt-out preference signal and place Ramona on a whitelist so that Business P does not have to notify Ramona of the conflict again.*").

The CPPA's example of Ramona's conflict between her opt-out signal and participation in Business P's financial incentive program highlights a critical flaw in current privacy choice architectures: fragmented, context-dependent controls that force users to manually reconcile conflicting preferences across systems.

ID side's observation is that some of the frictions explored by CPPA in few examples could be resolved by adopting a Personal Data Choices Management Platform (or DMP) -as conceptualized in WIPO Patent US392996960, which would empower users with:

1. Unified Preference Portability

Individuals' privacy choices (i.e. opt-outs, financial incentive participation) should follow them via a user-centric, cryptographically secured identifier decoupled from cookies or device-specific trackers to ensure consistency across all businesses. For sure, a platform-based approach would automatically reconcile conflicts (i.e. suspending tracking under an opt-out while preserving coupon eligibility) without requiring repeated user intervention.

2. Dynamic Consent Management

Instead of whitelisting individuals (which risks degrading their upcoming choices), digital service providers could query their real-time, context-aware preferences via the platform. For example, if one's default preference prioritizes privacy over incentives, the opt-out would apply immediately. If one wishes to temporarily permit tracking for targeted benefits or discounts, the platform could log this as a time-bound exception—transparently documented and revocable at will.

3. Anti-Fingerprinting Protections

Few examples rely on cookies (a re-identifiable tracker) to recognize individuals, undermining the pseudonymity promised by some loyalty programs. A zero-knowledge proof system (as suggested in

the patent) could verify one's eligibility for incentives without exposing their identity or browsing history to businesses or partners.

To operationalize this, the CPPA could usefully:

- Mandate interoperability between opt-out signals (e.g. GPC) and financial incentive programs via standardized APIs, preventing businesses from forcing users into "choice conflicts."
- Require cryptographic non-linkability for pseudonymous identifiers, ensuring that individuals cannot be re-identified or tracked across contexts.
- Prohibit whitelisting as a default, as it perpetuates dark patterns by silently preserving tracking unless the user affirmatively acts.

5. High-level Takeaways

A Personal Data Choices Management Platform would transform privacy from a burdensome series of opt-outs into a seamless, user-controlled experience aligning with the CCPA's goal of meaningful consumer control. ID side would finally like to emphasize two crucial points.

1. User-Centric Privacy by Default (Reversing the Current Logic)

ID side solution is promoting a truly **user-centric** approach because it operates **cross-platform** and fundamentally **reverses the current privacy paradigm**. Today, individuals must repeatedly assert their preferences (e.g. opt-out signals) across countless websites, forcing them into reactive battles against tracking. In contrast, ID side's system shifts the burden to **companies**, which must proactively check a user's **default, portable privacy choices** before processing data—effectively enforcing "privacy by default" at scale. This architecture ensures that Ramona's preferences (e.g. "no sale of data") are **automatically respected everywhere**, eliminating the need for whitelisting, cookie-based conflicts, or coercive "choice fatigue" tactics.

2. Strong Pseudonymisation via Encryption: The Only Viable Path Forward

ID side's encryption-based pseudonymisation is the **only technically robust method** that empowers users **without introducing new tracking risks**. Unlike cookies, device fingerprints, or probabilistic identifiers—which can be reverse-engineered or linked across contexts—**cryptographic identifiers** (e.g., zero-knowledge tokens) allow businesses to verify eligibility (e.g., for financial incentives) **without ever accessing raw personal data**. This ensures one can participate in programs like loyalty programs **without** exposing their browsing history or enabling re-identification. Without this level of protection, even "pseudonymous" systems become vectors for surveillance. Our understanding of individual and tech-enabled Privacy signals is that encryption is a non-negotiable feature to ensure **real control and real privacy in the digital environment**.

APPENDIX 1 - Additional background & information on ID side and the “Personal Data Choices Management Platform” (DMP) designed by ID side

Additional background & information on ID side and the DMP designed by ID side

ID side solution is architected to technically empower internet users and share their by-default choices wherever they browse (such choices could be Privacy, Safety, AI or commercial ones). Our patent was filed in February 2020 and is available [here](#).

Inspired by recital 68 of the GDPR and article 12 of the GDPR, this tool is shaped to empower internet users in practice, specifically in IoT, Data Spaces, metaverse and AI-enabled environments. Our R&D now focuses on how our tool could empower individuals regarding “AI agents”.

Reminder: ID Side’s technology allows internet users to broadcast their default privacy choices to information technology providers. Conversely, it also allows these information technology providers to ask specific internet users to grant them an exception to these default privacy choices, through a “Contact Box” mechanism. To enable this to work, information technology providers need a way to indirectly identify a specific internet user within the ID side system, so that these requests for an exception are routed to the correct individual. ID Side’s technology relies on a pseudonymous identifier to make this possible in API calls. This approach creates a potential unexpected privacy risk: this pseudonymous identifier could be used by information technology providers to indirectly track users, somewhat like using a device address. ID Side counters this risk by using cryptographic mechanisms that make the pseudonymous identifier change continuously, rendering it useless as a tracking tool.

Online consent: How can it be made valid in practice?

Online consent cannot be reduced to a binary choice. It relies on the scope of “what” should be consented to, “why” it matters specifically to individuals, “when,” and more broadly, “how” it is provided. Far from being a black-or-white assessment, to be valid, consent should be legally offered, meaning in accordance with applicable fairness, transparency and accountability principles, under Recital 32 of the [EU General Data Protection Regulation](#) referring to a “*freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her.*”

Valid consent should be rooted in, or at least aligned with, the reasonable expectations of individuals, i.e., neither distorting nor constraining individuals’ will to accept or reject one or several optional data processing options, on the top of strictly necessary ones.

[...]

Online, no individual can humanly read, assess, or signify agreement freely when using currently available consent tools. The load of related requests remains so high, and the act of consent is so cumbersome -reading applicable provisions, finding appropriate settings, ticking opt-out boxes, checking specific provisions, identifying how to change or withdraw consent - that no informed and free consent exists. This author’s standpoint is that online consent today is neither legally valid nor implementable simply because we use far too many services.

As mentioned earlier, in May 2020, the EDPB [clarified](#) how consent should be requested. The opinion clarifies few interesting points focusing on the “freely given” parameter.

- **Imbalance of power.** Is the service provided to individuals unique or so dominant that there is no real possibility to disagree? In this case, individuals “*will have no realistic alternatives to accepting the processing.*”
- **Conditionality.** Is the agreement separated from any other term? It corresponds to a “*situation of “bundling” consent with acceptance of terms or conditions, or “tying” the provision of a contract or a service to a request for consent to process personal data that are not necessary for the performance of that contract or service, is considered highly undesirable.*”
- **Granularity.** Is the request for agreement specific to a limited set of data processing activities? Consent “*should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes.*”
- **Detriment.** Would disagreement have a negative impact on individuals or block benefits at stake? As specified by the EDPB, “*examples of detriment are deception, intimidation, coercion or significant negative consequences if a data subject does not consent*”; individuals shall have “*a free or genuine choice about whether to consent*” and not suffer any such significant negative consequences.

[...]

In April 2024, EU data protection authorities agreed large online platforms should implement consent or pay models relating to behavioral advertising in a way that constitutes valid and, in particular, freely given consent. A core takeaway from the European Board is that, according to them, “[in] most cases, it will not be possible for large online platforms to comply with the requirements for valid consent if they confront users only with a binary choice between consenting to processing of personal data for behavioural advertising purposes and paying a fee.”

[...]

A lingering debate on the validity of consent results from user experience considerations. Setting dark patterns or lack of transparent or intelligible information aside, the question to address is: Can humans validly consent to all requests coming their way?

Far from being a purely legal matter, consent is a practical ratio to frame: [available time / human capacity] -or put differently: a pragmatic consideration of the time and attention that individuals can actually dedicate to online privacy monitoring in real life in order for consent to be deemed as valid. For instance, consent management platforms ask everyone to grant consent when entering a website and willing to access specific content. Widely spread, these mechanisms also help data controllers demonstrate they collected explicit agreement for personal data to be processed. They do not guarantee individuals are empowered to freely consent.

Why so? First, consent is requested at a given time, potentially as a take-it or leave-it choice, and as a pre-condition for individuals to access the content or service they are interested in - somehow forcing users' choices based on interest or convenience considerations. Second, they do not allow users to share their by-default reasonable expectations, nor do they have their primary choices automatically updated or seamlessly shared as they browse -somehow carving a one-time consent into digital stone! Third, the tool does not permit “qualitative” consent nor gives control to individuals -because consent must be provided immediately and “as is.”

Finally, consent management platforms do not streamline consent fatigue nor reduce the illimited number of consent requests coming our way. They do not check individual reasonable expectations nor enquire about by-default choices before sending requests. Consent is both the entry point and the endpoint. Wouldn't it be fair though if everyone's reasonable expectations were considered by default before any consent request were sent our way?

What online consent should be

To reassess state-of-the-art consent (GDPR Recital 32), a Nov. 2024 [article](#) by Lorrie Cranor stresses that, globally, “notice and consent” does not work as is and should be given “*the legal and technical support it needs.*”

On the tech front, Cranor acknowledges the significant steps taken in the U.S. to empower individuals in practice, specifically providing them with appropriate tech tools. From the binary approach of “do not track” to the current [Global Privacy Control](#) in California “*which allows users to turn on a setting in their browser (or browser extension) that transmits a GPC signal to automatically opt out of websites selling or sharing their personal information,*” she writes that “*for the first time privacy laws are requiring websites to respect automated privacy signals such as GPC.*”

California law sets a new cornerstone for regulating valid consent, and a crucial landmark has been set to respect individuals' right to share automated privacy signals and have them automatically complied with. Since the adoption of the GPC and, after that, the settlement of the [Sephora case](#) in August 2022, such right factually and amicably entered into force.

Outside the EU, California/US internet users are the first to enjoy the right to an actionable automated privacy signal tool, giving them real opt-out control. The California Privacy Protection Agency is the

DPA leading the charge on this tech-enabled consent framework and was created four years ago. Despite being a new DPA, it somehow sets the tone on how individual fundamental rights should be enforced in practice in a tech-enabled world.

On the legal front, the need is clearly identified too and announced by GPC model. It is all about giving individuals the chance to seamlessly share their reasonable expectations online and switch from consent collection tools such as consent management platforms to user-centric privacy choices tools, such as personal data choice management platforms.

[...]

In short, this "notice and consent 2.0" empowers everyone to take control over commercial processing and personalization online, as they proactively share automated privacy signals wherever they browse seamlessly.

So why don't we validly consent online yet?

The tech is there. Few legal provisions in California already made the point that, in a tightly limited timeframe, user-centric automated privacy control practices can be fostered and enforced. What we need now is a global, consistent and game-changing regulatory positioning. Cranor stressed, *"We need IoT devices that send and receive standardized privacy signals to well-designed user agents. We need enforceable penalties for data collectors that fail to honor automated signals or manipulate users into consenting to data practices. And, importantly, we need strong baseline privacy regulations [...]"*.

Conspicuously, valid consent blockers, whatever they are, are not tech ones anymore. As of today, the main blocker to valid consent appears to be regulatory latency - the time for regulators to adapt regulation to state-of-the-art tech practices from CMPs to PDCMPs.

Things will move fast now. One year ago, the Directorate-General for Communications Networks, Content and Technology in the EU Commission recommended exploring signals from personal data choice management platforms under the [cookie pledge](#) draft principle H. Indeed, for consent to be valid in practice, what most innovative and accountable companies need is support in showcasing what kind of user-centric personal data choices management platforms could help serve trusted personalised ads and services. Since 2024, the [Digital Advertising Alliance](#) started exploring cross-services [signal-based mechanisms](#) similar to those designed in EU and subject to patent application. So, let's all move discussion forward diligently and determine what a consistent tech-enabled consent mechanism should look like in the U.S., the EU and globally.

Grenda, Rianna@CPPA

From: Austin Heyworth <austin@heygovt.com>
Sent: Monday, June 2, 2025 12:16 PM
To: Regulations@CPPA
Subject: Internet Works - CPPA ADMT Rulemaking Comments
Attachments: CPPA ADMT - Internet Works Comments - 6.2.25.docx.pdf

This Message Is From an Untrusted Sender

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

Report Suspicious

CPPA team,

Please find attached comments on behalf of [Internet Works](#) for the open comment period on the revised proposed regulations.

Thank you for considering.

Austin Heyworth

(626)818-6322

Austin@heygovt.com





Internet.Works

June 2, 2025

VIA EMAIL TO:

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

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

Dear Board Members:

Internet Works (IW) is a trade association of diverse members working together to right-size technology policy, especially for middle tech companies, and promote trust and safety online. Our goal is to ensure our users are represented in important policy conversations and that state and federal policies continue to promote innovation, protect freedom of expression, and maintain choice in products and services. Our trade association is composed of 22 companies, all of which directly support millions of small businesses and entrepreneurs, with a substantial number based in California.

We appreciate the CPPA's recent revisions to the ADMT and risk assessment regulations, which represent meaningful progress toward reducing compliance burdens—especially for small and medium-sized tech companies. Narrowing the scope of ADMT to tools that “substantially replace” rather than “facilitate” human decision-making, and limiting applicability to “significant” decisions, helps protect core platform functions from disproportionate regulation. Excluding common practices like first-party behavioral advertising and removing references to “artificial intelligence” reflect a thoughtful response to concerns about overreach. Similarly, eliminating the “abridged” risk assessment submission and narrowing the range of covered processing activities will ease compliance costs and complexity. These changes support a more balanced and scalable regulatory framework that recognizes the operational realities of smaller platforms.

Narrow the Definition and Scope of “Automated Decision-Making” and “Significant Decision”

We recognize the progress made in refining the definition of ADMT, however, the

proposed rules still sweep in routine, low-risk tools such as calendar assistants, content filters, and internal document generation. These tools are designed to support—not replace—significant human decisions and should not be regulated alongside consequential systems for lending, housing, or employment. In particular, the current language in § 7001(e)(1)(B) requiring human review of all “relevant” information is vague and likely unworkable.

We recommend ADMT be more narrowly defined as:

“Final decisions that are made solely or fully with machine learning technology and result in legal or similarly significant effects—such as access to credit, housing, education, insurance, or other essential services.”

We recommend “legal or similarly significant effects” be defined as:

“A decision made by the business that results in the provision or denial by the business of financial and lending services, housing, insurance, education enrollment, criminal justice, health care services, or access to basic necessities, such as food and water.”

In particular, we are concerned with the subdefinition of “financial and lending services” under what constitutes a “significant decision” as included in the most recent draft. This is the first time we’ve seen such a broad construction of “financial or lending services” in any statute or regulation to date, and its adoption would have far-reaching and unintended consequences. This would encompass common tools such as peer-to-peer payment apps, money transfer features, and digital wallets—none of which involve a judgment or evaluation of a consumer’s eligibility or worthiness for financial services. This would create a broad right to opt out of automated functionality that is a core feature to how many services operate. In practice, consumers who opt out of an ADMT used to transmit or exchange funds would likely be opting out of using the service entirely. To that end, we suggest revising the definition as follows:

“Financial or lending services” means the extension of credit or a loan.

Limit Risk Assessment Requirements to Actual High-Risk Use

We urge the Board to avoid finalizing prescriptive risk assessment mandates while two pieces of related legislation are still working their way through the Legislature. Definitions like “significant risk” and triggers such as training an ADMT—even if it is never deployed—go well beyond the statutory mandate and intent. We encourage the Agency to clarify that risk assessments apply only when ADMTs are used in consequential decisions affecting consumers. Moreover, references to profiling based on “sensitive locations” must distinguish between routine uses (e.g., geofencing for store locations) and invasive surveillance. Granular reporting mandates, including disclosing ADMT “logic,” threaten trade secrets and impose excessive burdens without improving consumer protection. Aligning with interoperable, risk-based models would support stronger outcomes.

Realign Consumer Transparency Provisions

While we support transparency, pre-use notices and access rights must be tailored to significant decisions with real consumer impact so as not to lead to user fatigue because of the excessive prevalence of those options. As written, § 7200(b) would apply retroactively to tools no longer in use, and § 7220(a) appears to apply even where no access or opt-out rights are triggered.

We recommend:

- Limiting pre-use notice and access requirements to consequential uses of ADMT.
- Narrowing opt-out provisions to specific high-risk use cases rather than a general opt-out, which may mislead users or disrupt helpful functionality.
- Restricting access requests under § 7222 to adverse decisions affecting the consumer making the request.
- Lastly, the provisions that require explanation for the “logic” of complex ADMTs are not only impractical but risk confusing consumers and exposing proprietary information. These disclosures should instead focus on actionable outcomes and consumer rights.

Economic Impact Underestimated and Uneven

We recognize and appreciate the CPPA’s efforts to revise the proposed regulations in a way that significantly reduces projected compliance costs—by an estimated 64%—by addressing some of the most excessive and duplicative requirements identified in earlier drafts. These revisions mark meaningful progress in making the rules more workable and responsive to stakeholder feedback. However, even with these cost reductions, the overall burden of compliance remains substantial—particularly for small and medium-sized platforms and developers. The CPPA’s own regulatory impact assessment still estimates significant compliance costs, which could disproportionately impact smaller businesses that lack the legal and engineering resources of larger platforms. These costs risk stifling innovation, reducing competitiveness, and creating barriers to entry in the digital economy.

We urge the CPPA to continue refining the economic impact analysis and consider phased implementation timelines, size-based thresholds, or alternative compliance paths that preserve the rules’ objectives while mitigating the unintended consequence of discouraging competition and job growth. To avoid creating a regulatory environment that favors only the largest firms, we encourage the CPPA to adopt tiered penalties based on the severity and intent of noncompliance, recognizing the difference between inadvertent issues and willful violations.

Internet Works thanks the Board for the opportunity to provide our comments on this proposal. We would be happy to make ourselves available for a meeting to discuss these important issues with you further. We look forward to working with you and your staff and supporting California as a home to the technology industry.

Respectfully submitted,



Peter Chandler

Executive Director, Internet Works

<https://www.theinternet.works/>



Grenda, Rianna@CPPA

From: Celeste Wilson <cwilson@lbchamber.com>
Sent: Thursday, May 29, 2025 11:36 AM
To: Regulations@CPPA
Subject: LBACC | Public Comment on Revised Draft Regulations on Automated Decisionmaking Technology
Attachments: 5_29_2025_CPPA Regulations Revision Comments_LBACC.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,

My name is Celeste Wilson, I am the Long Beach Area Chamber of Commerce's (LBACC) Government Affairs Manager.

Please find attached LBACC's written comment on the revised draft regulations for Automated Decisionmaking Technology. While we appreciate the CPPA's continued commitment to California's business community, we are still concerned with some of the overly broad and burdensome regulations the draft includes, as well as the exodus of the fraud prevention tools exemptions.

Thank you in advance for your consideration of our position.

All the best,

--

Celeste Wilson

Government Affairs Manager

[Long Beach Area Chamber of Commerce](#)

1 World Trade Center Ste 101

Long Beach, CA 90831

Direct: 562-435-9594

Cell: 530-588-4984

Email: cwilson@lbchamber.com



The Long Beach Business Organization since 1891

Catalyst for business growth, Convener of leaders and influencers, and a Champion for a stronger community

May 29, 2025

Subject: Public Comment on Revised Draft Regulations on Automated Decisionmaking Technology

To whom it may concern,

On behalf of the Long Beach Area Chamber of Commerce (The Chamber), representing nearly 900 members, I am writing to express our appreciation of the California Privacy Protection Agency's willingness to revise the proposed regulations on Automated Decisionmaking Technology (ADT), but express continued concern with the overly broad and burdensome regulations that remain in the latest draft.

While the latest draft includes several helpful and positive revisions (such as removing restrictions on customer-targeted advertising or the allowance for businesses to withhold trade secrets) that demonstrate significant responsiveness to stakeholder concerns, the remaining provisions still pose significant operational and financial burdens to California businesses – especially small and mid-sized employers. According to the state's own estimate, this revised version would still cost California businesses over \$1.2 billion – just in the first year.

Despite revisions to the definition of “automated”, the rules still appear to apply to many common business tools that are neither autonomous nor decision-making. For example, software used by employers to help track and analyze its workers' performance – such as tracking and analyzing sales figures, safety incidents, or even something basic such as whether or not they are regularly late to work – could fall under the regulation's scope. This interpretation stretches the definition of “automated decisionmaking” to include standard workplace tools and performance metrics, which have little to do with consumer privacy.

Lastly, we urge the agency to reinstate the previously included exemption for fraud prevention tools. As drafted, businesses could be required to allow consumers or employees to opt out of systems designed to detect fraud or prevent malicious activity. That undermines the purpose of such tools and creates significant security concerns. Restoring this common-sense exception is essential to maintaining fraud prevention capabilities.

Thank you for considering our comments.

Sincerely,

A large black rectangular redaction box covering the signature area.

Jeremy Harris
President & CEO
Long Beach Area Chamber of Commerce

Grenda, Rianna@CPPA

From: csw833 [REDACTED]
Sent: Monday, May 12, 2025 10:42 AM
To: Info@cppa
Subject: Please do not scale back/abandon CCPA's rule making process
Attachments: CCPA-Open-Letter.pdf

Categories: To Legal

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 CCPA:

As a consumer I am very concerned about the CPPA's decision to abandon or scale back the CCPA's rule making process. I have noticed an alarming trend with websites I visit. They have an enormous amount of personal information businesses have collected about me that I would never authorize. I support and am attaching the April 15, 2025 letter sent to you from the ACLU, the CA Nurses Association, the Electronic Frontier, the Electronic Privacy Information Center and all organizations who signed this letter and have asked you "to adhere to the current California privacy law and continue with the current rule making process as directed by the CCPA ...". Consumers need stronger privacy protections and I urge you to protect them.

Sincerely,

Lynne Licari

Sent with [Proton Mail](#) secure email.

April 15, 2025

California Privacy Protection Agency
2101 Arena Boulevard
Sacramento, CA 95834

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

We the undersigned organizations and individuals are writing to express our deep concern about recent pressure on the California Privacy Protection Agency (CPPA) to abandon or significantly scale back its current CCPA rulemaking process. At a time when our country's consumer- and worker-protection infrastructure is under threat, we strongly urge the board and agency to adhere to the intent of California's privacy law and proceed with the rule-making process as directed by the state's voters. The agency has proper democratic authority to protect Californians from privacy harms; it should use it.

Digital and data-driven technologies can make life better for Californians. We know that establishing a common-sense foundation for the collection and use of our data by these technologies can unlock their potential and build trust for consumers and workers who use these technologies. But technology broadly, and algorithmic systems specifically, can also magnify and expand threats to consumer and worker rights and safety, if robust protections are not put into place throughout the data collection and algorithmic ecosystem.

We're at a critical juncture. If we don't act quickly, companies choosing to use these powerful tools could build barriers instead of bridges—furthering an unequal society for Californians where some prosper, while others are locked out of jobs, homes, healthcare, education, and equity and dignity. As these systems grow in their ubiquity, they must meet a high standard that respects people's rights and ensures that they can be used safely and without harm. The choices we make today will determine whether these data-driven technologies empower us or deepen existing divides.

In 2022, voters in California passed Prop 24, which continued a proud tradition of protecting people's privacy that stems all the way back to 1972, when the right to privacy was enshrined in the state constitution. Since then, the rapid development of data-driven technologies has necessitated new laws and regulations to ensure the continued protection of this right. Prop 24 was a critical point in this history. It added to the privacy rights of consumers and workers by amending the California Consumer Privacy Act, empowering the CPPA to develop new regulations around cyber security, impact assessments, and automated decisionmaking systems. This regulatory authority carries the promise of ensuring that the law stays in step with developments in the collection and use of personal data. Since then, the CPPA's board and staff have been steadfastly moving through several rounds of rule-making to fulfill their charge. Importantly, dozens of organizations representing hundreds of thousands of workers and consumers have weighed in repeatedly throughout the rulemaking process to express their support for the board's efforts to establish common sense guidelines for the use of our data in algorithmic systems.

But recently, we have seen escalating pressure on agency staff and board members to abandon or restrict the scope of rulemaking so significantly that it would fail to fulfill the agency's statutory mandate. This pressure has come in multiple forms. Starting last year, public comments by business

representatives at agency hearings uniformly attacked the rule-making process as overreach, and in particular targeted the ADMT rulemaking for elimination. Then in February, 18 state legislators wrote an open letter to the agency demanding that the agency “redraft all [its] regulations.” This suggestion, for the agency to start from scratch, represents a fundamental misunderstanding of the agency’s legal authority and the nature of the harm facing Californians from algorithmic decisionmaking systems. And in January, CPPA board member Vinhcent Le—a champion of ensuring consumer and worker protections under the law—was unceremoniously removed from his position.

The arguments we’ve heard in public hearings from the business community, claiming that the board is exceeding its mandate and should defer to the legislature and Governor, represent many of the same groups that are simultaneously opposing efforts to regulate automated decisionmaking systems in the California legislature. This is part of a larger effort to block the will of the voters and input from thousands of consumers and workers, all to protect some of the largest and most profitable corporations in history from a common sense foundation of transparency and accountability over their use of our personal data.

In short, we are seeing an anti-democratic assault on a state agency and its staff that are working diligently to implement and enforce the country’s premier privacy law. This is an effort to block the implementation of critical privacy rights for California’s consumers and workers.

We therefore strongly urge the CPPA board and agency to adhere to California’s privacy law and continue with the rule-making process as directed by the CCPA. Voters have been very clear that they want their information fully protected—and that includes future-proofing the CCPA by developing regulations around cybersecurity, harm identification and mitigation, and algorithmic systems. What’s at stake are highly consequential decisions impacting access and equity in our communities and our workplaces.

At the federal level, we are witnessing an assault on the very fabric of government, including its agencies, staff, and regulations. California therefore has a critical role to play in modeling the democratic rule of law for the rest of the country. The successful completion of the current rule-making process by the CPPA, without interference and undue influence, would set an important example.

Sincerely,
The signed organizations and individuals

Organizations:

American Civil Liberties Union California Action
American Federation of Musicians Local 7
Athena Coalition
California Federation of Labor Unions, AFL-CIO
California Nurses Association
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Gig Workers Rising
IBEW 569

Los Angeles Alliance for a New Economy (LAANE)

MediaJustice

National Employment Law Project

National Union of Healthcare Workers

Oakland Privacy

PowerSwitch Action

SAG-AFTRA

SEIU California

Strippers United

Tech Oversight California

TechEquity

TechTonic Justice

The Resilience Labs

UDW/AFSCME Local 3930

UFCW Western States Council

Upturn, Inc.

Working Partnerships USA

Worksafe

Writers Guild of America West

Individuals (organizations listed for identification purposes only):

Annette Bernhardt, UC Berkeley Labor Center

Christina Chung, Center for Law and Work, UC Berkeley Law School

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

Grenda, Rianna@CPPA

From: Mohmad Sharif Jamali <noreply@adv.actionnetwork.org>
Sent: Tuesday, May 20, 2025 4:57 AM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations

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](#)

CPPA CPPA CPPA,

I strongly urge the CPPA to adopt its proposed regulations for businesses using automated decisionmaking technologies that would protect Californians' safety, privacy, and informed consent.

These common sense rules are a vital intervention for consumer protection and human rights as unaccountable algorithms increasingly influence our housing, education, employment, and basic freedoms. These rules should reflect the needs of everyday people to be protected from discrimination and data scraping, not Big Tech's appetite for profiting from our personal info.

Please stand strong, defend our rights to algorithmic transparency and accountability, and adopt the amended regulations.

Mohmad Sharif Jamali
mohmadsharifjamali@gmail.com

,

Grenda, Rianna@CPPA

From: Nick Meyer <nick@networkadvertising.org>
Sent: Monday, June 2, 2025 2:58 PM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: NAI Comment on CCPA Updates 6.2.2025.docx.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 Ms. Sanders,

Attached are the NAI's comments on the CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations, as modified on May 9, 2025.

Please let us know if anything else is needed. Otherwise, have a wonderful day!

Best,
Nick

Nick Meyer
Counsel, Compliance & Policy
The NAI
409 7th Street, NW, Suite 250, Washington, DC 20004
P: 408.394.9612 | nick@networkadvertising.org



June 2, 2025

Submitted via electronic mail to regulations@coppa.ca.gov

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

Re: Public Comment on CCPA Updates, Cybersecurity Audits, Risk Assessments, ADMT, and Insurance Companies

To the California Privacy Protection Agency:

On behalf of the Network Advertising Initiative (“NAI”),¹ thank you for the opportunity to comment on the modified proposed regulations regarding CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (“ADMT”), and Insurance Companies under the California Consumer Privacy Act (the “Proposed Regulations”).² The NAI appreciates both the continued commitment the California Privacy Protection Agency (the “Agency”) has shown to provide transparency and the opportunity to submit written comments throughout this rulemaking. The NAI is generally supportive of the changes the Agency has made to date for the Proposed Regulations, including the following: (1) removing the “Behavioral Advertising” definition from the Proposed Regulations as this decision will avoid confusing consumers without limiting their ability to opt out of Cross-Context Behavioral Advertising; (2) removing references to “extensive profiling”; (3) removing the “remains deleted” language as doing so avoids inconsistencies with existing deletion-request requirements to permanently and completely erase data; (4) removing language that would require an ADMT opt-out be treated as a deletion request; and (5) adding language to clarify that businesses must evaluate their use of ADMT to ensure it does not *unlawfully discriminate* based on protected characteristics.³ The NAI

¹ The NAI is a non-profit, self-regulatory association dedicated to responsible data collection and use for digital advertising. The NAI has been a leader in this space since its inception in 2000, promoting the highest voluntary industry standards for member companies, which range from small startups to some of the largest companies in digital advertising. The NAI’s members are providers of advertising technology solutions, and include ad exchanges, demand side platforms, supply side platforms, as well as other companies that power the digital media industry. Our member companies help digital publishers generate essential ad revenue, advertisers reach audiences interested in their products and services, and ensure consumers are provided with ads relevant to their interests. Earlier this year, the NAI launched its new Self-Regulatory Framework Program (the “NAI Framework”) to promote strong privacy practices for NAI members engaged in behavioral advertising. See *NAI Self-Regulatory Framework*, <https://thenai.org/self-regulatory-framework/>.

² California Privacy Protection Agency Proposed Text, Cal. Code Regs. tit. 11 (updated May 9, 2025) (hereinafter “Proposed Regulations”).

³ See Proposed Regulations at § 7001(g) (removed “Behavioral Advertising” definition); § 7150(b)(3)(B)(iii) (removed “Extensive Profiling”); § 7022(b)(1) (removed “remains deleted” language); § 7221(n)(1) (removed

provided comments on several of these topics and appreciates the Agency's willingness to engage with constructive comments.⁴

We now offer additional comments before the Proposed Regulations are made final, set out in more detail below.

- The Agency should further streamline consumer disclosures by clarifying that the pre-use notice may be presented as part of the notice at collection.
- The Agency should align its proposed definition of "sensitive location" with established treatments of that concept in Federal Trade Commission (FTC) enforcement actions and the NAI's self-regulatory standards.

I. The Proposed Regulations should clarify that the information required for an ADMT "pre-use" notice may be presented through a link that meets the CCPA's existing "notice at collection" requirements.

Consumers benefit most from transparency into how businesses process personal information about them—whether through ADMT or otherwise—when that transparency is provided in a way that is as simple and streamlined as possible.⁵ When consumers are presented with multiple notices through different links, there is a significant risk that consumers may be confused or overwhelmed and, as a result, forgo reading important disclosures that could impact how they choose to exercise their privacy rights. As initially proposed, the regulations would have introduced this risk by requiring businesses to post an ADMT pre-use notice separately from the notice at collection already required by CCPA.⁶

The Proposed Regulations now under consideration ameliorate that risk, as they appear to permit businesses to bundle the information the Proposed Regulations would require in an ADMT Pre-use notice with the information businesses are already required to include in a "notice at collection" under the CCPA,⁷ as consumers are best served by a single, easy-to-read notice that explains the data processing taking place.⁸ The NAI is supportive of this change.

language requiring ADMT opt-out be treated as a deletion request); § 7152(a)(6)(A) (added "unlawfully discriminate" language).

⁴ The Network Advertising Initiative, Comment Letter on Proposed Rule on CCPA Updates, Cybersecurity Audits, Risk Assessments, ADMT, and Insurance Companies (Feb. 19, 2025), <https://thenai.org/nai-comments-on-ccpa-updates-cyber-risk-admt-and-insurance-regulations/>.

⁵ See generally Cal. Code Regs. tit. 11 § 7003(a) ("Disclosures and communications to consumers shall be easy to read and understandable to consumers. For example, they shall use plain, straightforward language and avoid technical or legal jargon.").

⁶ California Privacy Protection Agency Proposed Text, Cal. Code Regs. tit. 11 (proposed Nov. 22, 2024) § 7220(b)(2) ("The Pre-use Notice must... [b]e presented prominently and conspicuously to the consumer before the business processes the consumer's personal information using automated decisionmaking technology[.]") (emphasis added).

⁷ See California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100(a) (hereinafter "CCPA"); Cal. Code Regs. tit. 11 § 7012.

⁸ See Proposed Regulations at § 7220(a).

However, the Agency can avoid potential ambiguity that remains under the Proposed Regulations concerning the pre-use notice requirements by further clarifying that the information required in a pre-use notice can be presented in a manner consistent with the existing CCPA requirements regarding notice at collection.

The existing CCPA regulations provide illustrative examples of how a business may make the *notice at collection* readily available to consumers, including one example indicating that a business may “post a conspicuous link to the notice on the introductory page of the business’s website and on all webpages where personal information is collected.”⁹ These illustrative examples are extremely helpful for businesses seeking to comply with the CCPA’s notice at collection requirements; however, comparable illustrative examples are absent from the Proposed Regulations for a pre-use notice. If the Agency’s objective is to permit businesses to include the information that will be required for a pre-use notice through a link that already satisfies the CCPA’s requirements for *notice at collection*, providing illustrative examples for how a business may achieve this would be useful. One illustrative example the Agency could include is the following:

“When a business uses ADMT as set forth in section 7200 and has posted a conspicuous link to its Notice at Collection on the introductory page of the business’s website and on all webpages where personal information is collected, the business may provide a Pre-use Notice in its Notice at Collection.”

The NAI recommends that the Agency adopt this illustrative example, or another that aligns with the Agency’s intentions as to how a business may satisfy the pre-use notice requirement.

II. The Proposed Regulations should align the definition of “Sensitive Locations” with the NAI’s definition of “sensitive points of interest.”

Not all location data carries the same level of sensitivity to consumers. In some cases, using location data to associate a consumer with a particular location or point of interest (POI) may create a heightened risk of harm if those data are misused. The NAI therefore supports the Agency’s inclusion of a definition for *Sensitive Locations* in the Proposed Regulations and the associated requirement for businesses to conduct a risk assessment when associating a consumer with a Sensitive Location.¹⁰

However, the NAI recommends that the Agency amend the definition of Sensitive Locations in the Proposed Regulations to align it more closely with the NAI’s existing definition of “sensitive POIs”¹¹ as

⁹ Cal. Code Regs. tit. 11 § 7012(c)(1).

¹⁰ See Proposed Regulations at § 7001(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.”) (quotations removed); § 7150(b)(5) (requiring a business to conduct a risk assessment when “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.”).

¹¹ See *NAI Precise Location Information Solution Provider Voluntary Enhanced Standards* (2024), <https://thenai.org/wp-content/uploads/2025/03/NAI-Precise-Location-Information-Solution-Provider-Voluntary-Enhanced-Standards.pdf> (hereinafter, “NAI Enhanced Standards”).

well as the definitions of Sensitive Location used by the FTC in connection with recent enforcement actions dealing with location data.¹² Amending the definition in the Proposed Regulations would promote two important objectives. First, it would tailor the definition more closely to risks of harm. As it stands, the proposed definition is both too broad when it includes locations that are not likely to increase the risk of harm; and incomplete when it omits categories of locations that may pose those risks. Second, it would promote uniformity and help businesses adopt a common standard for when a location or other point of interest is sensitive.

1. *Aligning the definition of “Sensitive Location” in the Proposed Regulations with the NAI’s definition of sensitive POIs will more closely track the risk of harm.*

The NAI has been a longstanding leader in promoting strong location data privacy practices across the digital advertising industry. Since 2022, the NAI has encouraged adoption of its *Precise Location*

¹² See Federal Trade Commission, *In the Matter of X-Mode Social, Inc. and Outlogic, LLC*, F.T.C. Docket No. C-4802, Decision and Order (April 11, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf, (“Sensitive Locations means locations within the United States associated with: (1) medical facilities (e.g., family planning centers, general medical and surgical hospitals, offices of physicians, offices of mental health physicians and practitioners, residential mental health and substance abuse facilities, outpatient mental health and substance abuse centers, outpatient care centers, psychiatric and substance abuse hospitals, and specialty hospitals); (2) religious organizations; (3) correctional facilities; (4) labor union offices; (5) locations of entities held out to the public as predominantly providing education or childcare services to minors; (6) associations held out to the public as predominantly providing services based on racial or ethnic origin; or (7) locations held out to the public as providing temporary shelter or social services to homeless, survivors of domestic violence, refugees, or immigrants.”); *In the Matter of InMarket Media*, F.T.C. Docket No. C-4803, Decision and Order (April 29, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/InMarketMedia-DecisionandOrder.pdf, (“Sensitive Location means: (1) sexual and reproductive health care providers, offices of mental health physicians and practitioners, residential mental health and substance abuse facilities, outpatient mental health and substance abuse centers, psychiatric and substance abuse hospitals, offices of oncologists, and offices of pediatricians; (2) religious organizations; (3) correctional facilities; (4) labor union offices; (5) locations held out to the public as predominantly providing education or childcare services to minors; (6) locations held out to the public as predominantly providing services to LGBTQ+ individuals such as service organizations, bars and nightlife; (7) locations held out to the public as predominantly providing services based on racial or ethnic origin; (8) locations held out to the public as predominantly providing temporary shelter or social services to homeless, survivors of domestic violence, refugees, or immigrants; or (9) locations of public gatherings of individuals during political or social demonstrations, marches, and protests.”); *In the Matter of Gravy Analytics, Inc. and Venntel*, F.T.C. Docket No. C-4810, Decision and Order (Jan. 13, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/212_3035_-_gravy_analytics_final_consent_package_without_signatures.pdf, (“Sensitive Locations means locations within the United States associated with: (1) medical facilities (e.g., family planning centers, general medical and surgical hospitals, offices of physicians, offices of mental health physicians and practitioners, residential mental health and substance abuse facilities, outpatient mental health and substance abuse centers, outpatient care centers, psychiatric and substance abuse hospitals, and specialty hospitals); (2) religious organizations; (3) correctional facilities; (4) labor union offices; (5) locations of entities held out to the public as predominantly providing education or childcare services to minors; (6) associations held out to the public as predominantly providing services based on racial or ethnic origin; (7) locations held out to the public as providing temporary shelter or social services to homeless, survivors of domestic violence, refugees, or immigrants; or (8) military installations, offices, or buildings.) (quotations removed) (hereinafter “ Relevant FTC Decisions.”)

Information Solution Provider Voluntary Enhanced Standards, which includes restrictions on processing location data associated with Sensitive Points of Interest (“SPOIs”).¹³ The NAI’s goal in putting forth categories of POIs that count as sensitive was to enable responsible uses of location data while limiting or eliminating certain uses of location data that pose a heightened risk of harm if misused. In developing categories of SPOIs, the NAI relied a set of key factors that weigh the risk of harm, especially: (1) the reasonable privacy expectations of consumers; (2) the risk of harm to consumers (including both likelihood and severity of harm); and (3) the risk of societal harms, even when individual consumers may not be affected.

In weighing these factors, the NAI determined that the following POIs should be considered sensitive:

- Places of religious worship
- Correctional facilities
- Places held out to the public as involving engagement with explicit sexual content, material, or acts
- Places held out to the public as predominantly providing education or childcare services to minors
- Domestic abuse shelters, including rape crisis centers
- Welfare or homeless shelters and halfway houses
- Dependency or addiction treatment centers
- Medical facilities that cater predominantly to sensitive conditions, such as cancer centers, HIV/AIDS, fertility or abortion clinics, mental health treatment facilities, or emergency room trauma centers
- Places held out to the public as primarily providing refugee or immigrant services, such as refugee or immigration centers and immigration services
- Credit repair, debt services, bankruptcy services, or payday lending institutions
- Military bases
- Temporary places of assembly such as locations or venues at the time(s) when political rallies, marches, or protests are taking place
- Places held out to the public as primarily serving individuals who identify as LGBTQ+, including gender-affirming care and transgender-specific medical services

Notably, some of these categories of SPOIs are absent from the definition of “Sensitive Location” in the Proposed Regulations. For example, the NAI determined that data associating a consumer with a point of interest that holds itself out as primarily serving individuals who identify as LGBTQ+ poses a heightened risk of harm to the consumer, and hence qualifies as an SPOI. This has been borne out in specific cases where location information about an individual has been used to associate that individual with gay bars, leading to adverse impacts to that individual.¹⁴ Updating the proposed definition of “Sensitive Location”

¹³ See NAI Enhanced Standards at 3.

¹⁴ See, e.g., *Pillar Investigates: USCCB gen sec Burrill resigns after sexual misconduct allegations* (Jul. 20, 2021), <https://www.pillarcatholic.com/p/pillar-investigates-usccb-gen-sec> (“According to commercially available records of app signal data obtained by The Pillar, a mobile device correlated to Burrill emitted app data signals from the location-based hookup app Grindr on a near-daily basis during parts of 2018, 2019, and 2020 — at both his USCCB

to include locations held out as serving LGBTQ+ populations and other categories of POIs classified as sensitive by the NAI will increase the likelihood that businesses conducting risk assessments will identify circumstances where their processing of location data could result in an increased risk of consumer harm.

However, the Agency should also consider cases where an overbroad classification of benign points of interest as “Sensitive Locations” unnecessarily burdens businesses without mitigating any meaningful risk of harm. For example, the proposed definition of Sensitive Location currently includes all *educational institutions*.¹⁵ This may include locations that do not appear to pose any special risk of consumer harm, such as universities and professional schools that serve populations of adults. However, the NAI recognizes that some educational institutions serve children – a more vulnerable population – and that associating a particular consumer device with presence at that type of location could be used to infer that an individual is a child. To account for this risk, the NAI determined that while treating *all* educational institutions as SPOIs would be overbroad, including as SPOIs all “[p]laces held out to the public as predominantly providing education or childcare services to minors”¹⁶ accounts for the relevant risk to children. This is true not only for educational institutions for children (such as elementary schools) but also for daycare facilities or amusement facilities that are intended to be occupied by children.

By adopting these more nuanced distinctions, the Proposed Regulations can promote a risk analysis framework that balances the need to protect consumers with the goal of preserving beneficial uses of location data and avoiding undue burden to businesses. While we recognize that adopting the NAI’s categories of SPOIs would in some cases narrow which locations would be considered “sensitive” (such as the example above for educational institutions), the Agency should also keep in mind that consumers would still retain the baseline protections and rights afforded to consumers by the CCPA, including the right to limit the use of sensitive personal information when precise geolocation information is being used.¹⁷

The FTC enforcement actions dealing with sensitive locations also align with the NAI’s definition of SPOIs on many of these categories, further demonstrating their utility to address the risk of consumer harm.¹⁸

office and his USCCB-owned residence, as well as during USCCB meetings and events in other cities.”) (“an analysis of app data signals correlated to Burrill’s mobile device shows the priest also visited gay bars.”).

¹⁵ See Proposed Regulations at § 7001(aaa).

¹⁶ See *NAI Enhanced Standards* at 2.

¹⁷ See, e.g., CCPA at § 1798.121 (consumers’ right to limit use and disclosure of sensitive personal information); § 1798.140(ae) (defining “Sensitive personal information” to include precise geolocation).

¹⁸ The following categories are defined as “sensitive locations” or cited as “prohibited uses” of location data by both the NAI *Enhanced Standards* and the relevant FTC enforcement actions: places of religious worship; correctional facilities; locations held out to the public as predominantly providing services to LGBTQ+ individuals such as service organizations, bars and nightlife; locations of public gatherings of individuals during political or social demonstrations, marches and protests; medical facilities providing treatment for substance abuse and mental health; family planning centers; domestic violence shelters; homeless shelters; refugee or immigration centers; and locations held out to the public as predominantly providing education or childcare services to minors. See *NAI Enhanced Standards* at 2; Relevant FTC Decisions, *supra* note 12.

2. *Aligning the definition of “Sensitive Location” in the Proposed Regulations with the NAI’s definition of sensitive POIs will promote a uniform standard.*

This Agency has a unique opportunity to craft definitions and rules that will be used as guideposts for other regulatory bodies and policymakers around the world. As with all privacy concepts that will be applied in laws and regulations across jurisdictions, uniformity helps promote business adherence to those rules and to set consumer expectations for how their personal information will be handled by businesses. By updating the definition of “Sensitive Location” in the Proposed Regulations to more closely align with treatments of that concept by the FTC and the NAI, the Agency can help promote those important goals.

The tables included at the end of this comment letter as Exhibit A illustrate how the definition of Sensitive Location as currently proposed diverges from other treatments of the concept discussed above.

When treatments of the same concept diverge widely across jurisdictions, this makes it difficult to set consumer expectations for privacy and increases the cost and complexity for businesses building compliance programs to address those concepts, including for sensitive locations. We therefore recommend the Agency align its definition of Sensitive Locations with the existing NAI categories of SPOIs.

In summary, the NAI supports the requirement in the Proposed Regulations for a business to conduct a risk assessment if the business profiles a consumer based on presence at a Sensitive Location. However, the Agency should update its definition of Sensitive Location to align with the NAI’s categories of SPOIs to better track the risk of harm presented by associating a consumer with a given point of interest, and to promote uniformity for businesses implementing safeguards around the processing of personal information that may be used to associate consumers with particular points of interest.

III. Conclusion

Thank you for your continued commitment to public involvement and transparency in this important rulemaking process concerning automated decisionmaking technology. If we can provide any additional information, or otherwise assist your office as it continues to engage in the rulemaking process, please do not hesitate to contact Tony Ficarrota, General Counsel, NAI (tony@thenai.org); or David LeDuc, Vice President, Public Policy, NAI (david@thenai.org).

Respectfully submitted,

Leigh Freund
President and CEO
Network Advertising Initiative (NAI)

Exhibit A

| Identity and Association-Based Locations | | | | | | |
|--|-------------------------|-------------------------------------|------------------------------|---------------------------------|---------------------------|---|
| Sensitive Point of Interest | NAI VES | FTC Outlogic/X-Mode | FTC InMarket | FTC Mobilewalla | FTC Gravy | CPPA ADMT Draft Regulations |
| Places of religious worship, religious organizations | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Places that could infer an LGBTQ+ identification (e.g. locations held out to the public as predominantly providing services to LGBTQ+ individuals such as service organizations, bars and nightlife) | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Venues that Could Infer Engagement with Explicit Sexual Content, Material, or Acts | ✓ | | | | | |
| Correctional Facilities | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Identity and Association-Based Locations | | | | | | |
| Sensitive Point of | NAI VES | FTC Outlogic/X | FTC InMarket | FTC Mobilewalla | FTC Gravy | CPPA ADMT Draft |

| Interest | | -Mode | | | | Regulations |
|--|---|-----------------------|---|---|---|-----------------------------|
| Labor Union Offices | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Racial/Ethnic Service Organizations | | ✓ | ✓ | ✓ | ✓ | |
| Temporary places of assembly (such as political rallies, marches, or protests) during the times the rallies, marches, or protests take place; political activity | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Military Bases, Installations, Offices, or Buildings | ✓ | | | ✓ | ✓ | |
| Political party offices | | | | | | ✓ |

| Health-Related Facilities | | | | | | |
|--|-------------------------|-------------------------------------|------------------------------|---------------------------------|---------------------------|---|
| Sensitive Point of Interest | NAI VES | FTC Outlogic/X-Mode | FTC InMarket | FTC Mobilewalla | FTC Gravy | CPPA ADMT Draft Regulations |
| Medical facilities (in general) | | | | | | |
| Medical facilities/ doctor's offices | | ✓ | ✓ | ✓ | ✓ | ✓ |
| General medical and surgical hospitals | | ✓ | | ✓ | ✓ | ✓ |
| Specific types of medical facilities | | | | | | |
| Specialty Hospitals | | ✓ | | ✓ | ✓ | |
| Locations treating substance abuse disorders (e.g. Offices, Residential, Outpatient, Hospitals, Dependency or Addiction Treatment Centers) | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Offices of physicians | | ✓ | | ✓ | ✓ | ✓ |
| Offices of Oncologists/ Cancer Centers | ✓ | | ✓ | | | |
| Health- Related Facilities | | | | | | |

| Sensitive Point of Interest | NAI VES | FTC Outlogic/X-Mode | FTC InMarket | FTC Mobilewalla | FTC Gravy | CPPA ADMT Draft Regulations |
|---|-------------------------|-------------------------------------|------------------------------|---------------------------------|---------------------------|---|
| Specific types of medical facilities | | | | | | |
| Offices of Pediatricians | | | ✓ | | | |
| Facilities catering to HIV/AIDS | ✓ | | | | | |
| Family Planning Centers (e.g. sexual and reproductive health care providers, fertility or abortion clinics) | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Mental Health-Related Facilities (e.g. Offices, Residential, Outpatient, hospitals) | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Emergency Room Trauma Centers | ✓ | | | | | |
| Urgent Care Facilities | | | | | | ✓ |
| Community health clinics | | | | | | ✓ |
| Pharmacies | | | | | | ✓ |

| Facilities Serving Vulnerable or Protected Populations | | | | | | |
|--|-------------------------|-------------------------------------|------------------------------|----------------------------------|---------------------------|---|
| Sensitive Point of Interest | NAI VES | FTC Outlogic/X-Mode | FTC InMarket | FTC Mobilewall a | FTC Gravy | CPPA ADMT Draft Regulations |
| Domestic Abuse/ Violence Shelters (including rape crisis centers) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Homeless Shelters (including welfare shelters and halfway houses) | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Refugee or Immigration Centers and Immigration Services | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Locations held out to the public as predominantly providing education or childcare services to minors/ Places primarily intended to be occupied by children under 16 | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Food pantries | | | | | | ✓ |
| Housing/ emergency | | | | | | ✓ |

| shelters | | | | | | |
|--|-------------------------|-------------------------------------|------------------------------|----------------------------------|---------------------------|---|
| Facilities Serving Vulnerable or Protected Populations | | | | | | |
| Sensitive Point of Interest | NAI VES | FTC Outlogic/X-Mode | FTC InMarket | FTC Mobilewall a | FTC Gravy | CPPA ADMT Draft Regulations |
| Educational institutions | | | | | | ✓ |
| Legal services offices | | | | | | ✓ |

| Financial Vulnerability Indicators | | | | | | |
|------------------------------------|-------------------------|-------------------------------------|------------------------------|----------------------------------|---------------------------|---|
| Sensitive Point of Interest | NAI VES | FTC Outlogic/X-Mode | FTC InMarket | FTC Mobilewall a | FTC Gravy | CPPA ADMT Draft Regulations |
| Credit repair | ✓ | | | | | |
| Payday lending institutions | ✓ | | | | | |
| Debt services | ✓ | | | | | |
| Bankruptcy services | ✓ | | | | | |