epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@epic.org
https://epic.org

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-Agencys-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 regulations[6] 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 Schecter & 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://cppa.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-pxdx-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 Gedye, *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 gave 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 A*I, 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 comments[59] 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 than 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 to 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