COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER and
THE CONSUMER FEDERATION OF AMERICA

to the

CALIFORNIA PRIVACY PROTECTION AGENCY

on

Proposed Rulemaking Regarding Cybersecurity, Risk Assessments,
and Automated Decisionmaking Technology

February 19, 2025

The Electronic Privacy Information Center ("EPIC") and the Consumer Federation of America ("CFA") submit 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 commend the Agency for taking steps to protect consumers from the significant privacy harms caused by the use of automated decisionmaking technologies and the processing of personal data without adequate assessment and mitigation of the resulting privacy and security risks. We offer suggestions to help the proposed regulations better safeguard consumer privacy consistent with the Agency's stated objectives.

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

[1] EPIC, *About EPIC* (2022), https://epic.org/about/.

advocating for 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.

CFA is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education. CFA regularly engages state legislators to create algorithmic transparency, accountability, and recourse for victims of discrimination and manipulation.[4]

These comments address the Agency's proposed regulations in three parts: (I) ADMT regulations, (II) risk assessment regulations; and (III) cybersecurity assessment regulations.

---

[2] 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] *See, e.g., CFA Testifies on State AI Legislation Model to Multistate Group of Lawmakers*, Consumer Federation of America (Jan. 27, 2025) https://consumerfed.org/testimonial/cfa-testifies-on-state-ai-legislation-model-to-multistate-group-of-lawmakers/; *CFA Joins Coalition of Advocates Calling for Pro-Consumer Updates to the Colorado Act*, Consumer Federation of America (Dec. 10, 2024) https://consumerfed.org/press_release/cfa-joins-coalition-of-advocates-calling-for-pro-consumer-updates-to-the-colorado-ai-act/.

I. ADMT Regulations

EPIC and CFA commend the Agency for addressing the privacy harms caused by ADMTs and for strengthening related consumer protections. In support of these aims, we set out in this section: (a) the CPPA's clear authority to regulate ADMTs under the CCPA; (b) why regulating ADMTs is necessary to protect Californians' privacy rights; and (c) suggestions to strengthen the ADMT regulations.

a. The CPPA has clear authority to regulate automated decisionmaking technologies.

The CPPA has clear authority to promulgate rulemaking on automated decisionmaking technologies. As the CCPA states, the agency is to "issu[e] regulations…with respect to a business' use of automated decision-making 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]

On top of this clear statutory mandate to promulgate rules about ADMTs, the specific obligations in the proposed regulations are also in line with what other states are doing to regulate ADMTs. Many of the substantive requirements in these proposed regulations are already required under Colorado's AI Act, which businesses will need to comply with next year.[6] Legislators in many other states have already introduced bills based on Colorado's law—or expressed their intent to do so once their states' legislative sessions begin[7]—meaning businesses

[5] Cal. Civ. Code § 1798.185(a)(15) (emphasis added).
[6] S.B. 24-205, 2024 Gen. Assemb., Reg. Sess. (Colo. 2024).
[7] *See, e.g.*, Press Release, *Senate Democrats Announce Caucus Priority Bill Concerning Artificial Intelligence*, Connecticut Senate Democrats (Dec. 20, 2024), https://www.senatedems.ct.gov/senate-democrats-announce-caucus-priority-bill-concerning-artificial-intelligence-2; A.B. A768, 2025-2026 Gen. Assemb., Reg. Sess. (N.Y. 2025); H.B. No. 1709, 89th Leg. (Tex. 2024).

will need to set up processes to comply with similar opt out, risk assessment, and notice requirements. Thus, these proposed regulations will not impose unreasonable or unique burdens on companies, especially those who do business across multiple states, but rather will provide clarity and assurance to California consumers and workers that their rights are protected.

b. Regulating ADMTs is necessary to protect Californians.

Commercial surveillance of consumers is out of control. Consumers today face ubiquitous online tracking through the opaque collection, use, and processing of their data.[8] Commercial surveillance systems enable companies to collect and commodify every bit of consumers' personal data, including sensitive personal data.[9] To participate in today's economy is to have personal data extracted, aggregated, commercialized, and sold—as individuals work,[10]

[8] Comments of EPIC to the FTC Proposed Trade Regulation Rule on Commercial Surveillance & Data Security 7 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM- comments-Nov2022.pdf [hereinafter EPIC FTC Comments on Commercial Surveillance].

[9] *Hearing before the Innovation, Data, and Com. Subcomm. of the H. Comm. on Energy & Com.*, 119th Cong. (2024) (testimony of John Davisson), https://epic.org/wp-content/uploads/2024/09/EPIC-Testimony-FTC-Sept2024.pdf.

[10] *See, e.g.*, *Workplace Privacy*, EPIC (2023), https://epic.org/issues/data-protection/workplace-privacy/; Benjamin Wiseman, Fed. Trade Comm'n, Remarks of Benjamin Wiseman at the Harvard Journal of Law & Technology on Worker Surveillance and AI (Feb. 8, 2024), https://www ftc.gov/system/files/ftc_gov/pdf/Jolt-2-8-24-final.pdf.

eat,[11] pray,[12] study,[13] socialize,[14] browse the internet,[15] seek medical care,[16] plan families,[17] educate children,[18] exercise political freedoms,[19] or simply move about the world.[20] These

[11] *See* Nicole Ozer & Jay Stanley, *Diners Beware: That Meal May Cost You Your Privacy and Security*, ACLU (July 27, 2021), https://www.aclu.org/news/privacy-technology/diners-beware-that-meal-may-cost-you-your-privacy-and-security.

[12] *See, e.g.*, Press Release, Fed. Trade Comm'n, *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations* (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

[13] *See, e.g.*, *Student Privacy*, EPIC (2023), https://epic.org/issues/data-protection/student-privacy/; Press Release, Fed. Trade Comm'n, *FTC Says Ed Tech Provider Edmodo Unlawfully Used Children's Personal Information for Advertising and Outsourced Compliance to School Districts* (May 22, 2023), https://www ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ed-tech-provider-edmodo-unlawfully-used-childrens-personal-information-advertising; Julia Angwin, *The Big Business of Tracking and Profiling Students*, The Markup (Jan. 15, 2022), https://themarkup.org/newsletter/hello-world/the-big-business-of-tracking-and-profiling-students; Elizabeth Laird & Maddy Dwyer, Center for Technology and Democracy, *Off Task: EdTech Threats to Student Privacy and Equity in the Age of AI* (2023), https://cdt.org/insights/report-off-task-edtech-threats-to-student-privacy-and-equity-in-the-age-of-ai/.

[14] *See, e.g.*, Press Release, Fed. Trade Comm'n, *FTC Investigation Leads to Lawsuit Against TikTok and ByteDance for Flagrantly Violating Children's Privacy Law* (Aug. 2, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law; Fed. Trade Comm'n, *A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services* (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf.

[15] Press Release, Fed Trade Comm'n, *FTC Order Will Ban Avast from Selling Browsing Data for Advertising Purposes, Require It to Pay $16.5 Million Over Charges the Firm Sold Browsing Data After Claiming Its Products Would Block Online Tracking* (Feb. 22, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-order-will-ban-avast-selling-browsing-data-advertising-purposes-require-it-pay-165-million-over.

[16] *See, e.g.*, *Health Privacy*, EPIC (2024), https://epic.org/issues/data-protection/health-privacy/; Joseph Cox, *Inside the U.S. Government-Bought Tool that Can Track Phones at Abortion Clinics*, 404 Media (Oct. 23, 2024), https://www.404media.co/inside-the-u-s-government-bought-tool-that-can-track-phones-at-abortion-clinics/; Joseph Cox, *Location Data Firm Offers to Help Cops Track Targets via Doctor Visits*, 404 Media (Dec. 10, 2024), https://www.404media.co/location-data-firm-offers-to-help-cops-track-targets-via-doctor-visits/; Elisa Jillson, *Protecting the Privacy of Health Information: A Baker's Dozen Takeaways from FTC Cases*, Fed. Trade Comm'n: Bus. Blog (July 25, 2023), https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases.

[17] Sara Geoghegan, *Two Years Post-Dobbs: A Commercial Surveillance Landscape That is Confusing, Complicated, and Harmful to Abortion Seekers*, EPIC (June 25, 2022), https://epic.org/two-years-post-dobbs-a-commercial-surveillance-landscape-that-is-confusing-complicated-and-harmful-to-abortion-seekers/; Suzanne Bernstein, *The Role of Digital Privacy in Ensuring Access to Abortion and Reproductive Health Care in Post-Dobbs America*, EPIC (June 13, 2024), https://epic.org/the-role-of-digital-privacy-in-ensuring-access-to-abortion-and-reproductive-health-care-in-post-dobbs-america/; Lesley Fair, *FTC Says Premom Shared Users' Highly Sensitive Reproductive Health Data: Can it Get More Personal than that?*, Fed. Trade Comm'n: Bus. Blog (May 17, 2023), https://www ftc.gov/business-

sensitive personal data are aggregated into detailed profiles of individual consumers, exposing them to "ever-increasing risks of data breaches, data misuse, manipulation, and discrimination."[21]

The use of ADMTs in significant decisions threatens discriminatory outcomes across industries. Building on top of ubiquitous collection of data, automated decisionmaking technology (ADMT) uses personal data to automate decisionmaking processes that impact Californians' access to health care, education, employment, financial services, and public benefits.[22] ADMTs touch millions of Americans' lives every day. A recent report by TechTonic

guidance/blog/2023/05/ftc-says-premom-shared-users-highly-sensitive-reproductive-health-data-can-it-get-more-personal.

[18] Press Release, Fed. Trade Comm'n, *FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests* (May 31, 2023), https://www ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever.

[19] Zak Doffman, *Black Lives Matter: U.S. Protesters Tracked by Secretive Phone Location Technology*, Forbes (June 26, 2020), https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-blacklives-matter-protesters/; Dell Cameron & Dhruv Mehrotra, *FTC Says Data Brokers Unlawfully Tracked Protestors and US Military Personnel,* Wired (Dec. 2024), https://www.wired.com/story/ftc-mobilewalla-gravy-analytics-orders/; Sam Biddle, *U.S. Marshals Spied on Abortion Protestors Using Dataminr*, The Intercept (May 15, 2023), https://theintercept.com/2023/05/15/abortion-surveillance-dataminr/.

[20] *See, e.g.*, *Location Tracking*, EPIC (2024), https://epic.org/issues/data-protection/location-tracking/; Press Release, Fed. Trade Comm'n, *FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data* (Jan. 9, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data; Jon Keegan & Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, The Markup (Sept. 30, 2021), https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data.

[21] *Hearing before the Subcomm. Consumer Prot. of the H. Comm. on Energy & Com.*, 117th Cong. (2022) (testimony of Caitriona Fitzgerald), https://epic.org/documents/hearing-on-protecting-americas-consumers-bipartisan-legislation-to-strengthen-data-privacy-and-security; EPIC FTC Comments on Commercial Surveillance, *supra* note 8, at 45-55.

[22] Comments of EPIC et al. to Cal. Privacy Prot. Agency, 7–9, 43, (Mar. 27, 2023), https://epic.org/wp-content/uploads/2023/03/EPIC-et-al-comments-CCPA-rulemaking-March-2023-2.pdf.

Justice estimates that virtually all 92 million low-income people in the U.S. have some basic aspect of their lives decided by AI.[23]

While it is often difficult for individuals to identify the prevalence of algorithmic discrimination and unfair decisionmaking in ADMTs, there is abundant evidence that both occur in housing, employment, education, criminal justice, public benefits, health care, and public access to businesses.

In hiring, employers are increasingly using automated screening products that suggest whether or not an applicant is a good candidate based on resumes, LinkedIn profiles, and other materials, and tools that claim to assess biometric data such as facial expressions, tone, and body language to determine whether an applicant may make a good employee.[24] These systems may screen out candidates based on data that relates to their membership within protected classes, such as age, gender, race, or disability.[25] Others assess candidates through recorded video interviews, where AI systems generate transcripts, even though independent research has shown that transcriptions perform worse for Black speakers, speakers whose first language is not English, and speakers with speech or other disabilities.[26] Applicants have little transparency into

[23] Kevin De Liban, *Inescapable AI: The Ways AI Decides How Low-Income People Work, Live, Learn, and Survive*, TechTonic Justice (2024), https://static1.squarespace.com/static/65a1d3be4690143890f61cec/t/673c7170a0d09777066c6e50/1732014450563/ttj-inescapable-ai.pdf [hereinafter "TechTonic Justice Report"].
[24] 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; Will Knight, *Job Screening Service Halts Facial Analysis of Applicants*, Wired (Jan 12, 2021), https://www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/.
[25] Olga Akselrod & Cody Venzke, *How Artificial Intelligence Might Prevent You From Getting Hired*, ACLU (Aug. 23, 2023), https://www.aclu.org/news/racial-justice/how-artificial-intelligence-might-prevent-you-from-getting-hired.
[26] Marissa Gerchick & Olga Akselrod, *The Critical Role of Research in the Fight for Algorithmic Accountability*, Tech Policy Press (Oct. 23, 2024), https://www.techpolicy.press/the-critical-role-of-research-in-the-fight-for-algorithmic-accountability/.

an employer's hiring practices, including when an automated tool is used, let alone when it may be discriminating against them.[27]

Employers are also increasingly monitoring employees through technologies that track, assess, and evaluate workers, including by tracking time spent completing tasks, web browsing, messages sent to coworkers, duration of meetings, keystroke frequencies, and even biometric data.[28] As of 2023, over 50% of large U.S. employers across a wide array of industries—such as call centers, finance, health, retail, and caregiving—had adopted some form of emotion recognition to assess employees.[29] Companies producing such technology promise that their systems will reduce absenteeism, improve communication and productivity, support decision-making and creativity, promote employee well-being, and identify employees at risk of quitting, patterns of workplace relations, and even security risks.[30] In reality, emotion recognition systems have not been shown to be accurate or unbiased. Instead, they pose significant harm to a worker's privacy, dignity, autonomy, and job security through intrusive surveillance and flags by the ADMT indicating when workers are unfocused, not friendly enough, or suffer from mental health conditions.[31]

---

[27] *Id.*; Dave Schmidt & Breanna Timko, *EEOC Settles First AI Hiring Bias Lawsuit*, JD Supra (Aug. 25, 2023), https://www.jdsupra.com/legalnews/eeoc-settles-first-ai-hiring-bias-6261293/; Complaint of EPIC, *In re HireVue* (Nov. 6, 2019), https://epic.org/documents/in-re-hirevue/.

[28] Veena Dubal, *On Algorithmic Wage Discrimination*, 123 Col. L. Rev. 129 (2023); Merve Hickok & Nestor Maslej, *A Policy Primer And Roadmap On AI Worker Surveillance And Productivity Scoring Tools*, AI Ethics 3, 673–687 (2023), https://link.springer.com/article/10.1007/s43681-023-00275-8; Diego Areas Munhoz, '*Robot Bosses' Spur Lawmaker Push to Police AI Job Surveillance*, Bloomberg Law (Sept. 8, 2023), https://news.bloomberglaw.com/daily-labor-report/robot-bosses-spur-lawmaker-push-to-police-ai-job-surveillance.

[29] Nazanin Andalibi, *Emotion-Tracking AI on the Job: Workers Fear Being Watched—and Misunderstood*, The Conversation (Mar. 6, 2024), https://theconversation.com/emotion-tracking-ai-on-the-job-workers-fear-being-watched- and-misunderstood-222592.

[30] Scott Monteith, Tasha Glenn et al., *Commercial Use of Emotion Artificial Intelligence (AI): Implications for Psychiatry*, 24 Current Psychiatry Reports at 206 (2022).

[31] Comments of EPIC to Dutch DPA on Emotion Recognition Prohibition under EU AI Act, 19-22 (Dec. 17, 2024), https://epic.org/documents/epic-comments-to-dutch-dpa-on-emotion-recognition-prohibition-under-eu-ai-act/.

In healthcare, insurers and healthcare providers have relied on ADMTs to make decisions that often lead to discriminatory outcomes and arbitrary denials of coverage. ProPublica's recent report on United Health's reliance on an algorithm to identify "outliers" in receiving mental health treatment illustrates that UnitedHealth used the system's outputs to deny coverage and harass mental healthcare providers to limit reimbursements.[32] Racial bias has been shown in models used to assist in providing care, including assessing whether a vaginal birth is safe for patients,[33] diagnosis through chest x-rays,[34] and determining the level of patient need during triage.[35]

ADMTs are also deployed in many stages of criminal justice systems, including policing, bail, sentencing, and parole. Predictive policing tools use historical policing data, which reflects a history of racist policing practices, and dispatch police to the same historically heavily policed areas, resulting in more over-policing of BIPOC neighborhoods.[36] Deployment of systems like ShotSpotter—which installs sound sensors that purport to detect gunshots and report them to the police, but, in reality, has high false alarm rates—in mainly low-income communities of color

[32] Annie Waldman, *How UnitedHealth's Playbook for Limiting Mental Health Coverage Puts Countless Americans' Treatment at Risk*, ProPublica (Nov. 19, 2024), https://www.propublica.org/article/unitedhealth-mental-health-care-denied-illegal-algorithm.
[33] Darshali A. Vyas et al., *Challenging the Use of Race in the Vaginal Birth After Cesarean Section Calculator*, Women's Health Issues 2019 May-June; 29(3):201-204 (May 6, 2019), https://pubmed.ncbi.nlm.nih.gov/31072754/.
[34] Laleh Seyyed-Kalantari, et al., *Underdiagnosis Bias of Artificial Intelligence Algorithms Applied to Chest Radiographs in Under-Served Patient Populations*, 27 Nat Med 2176–2182 (2021), https://www.nature.com/articles/s41591-021-01595-0; Haoran Zhang, Thomas Hartvigsen & Marzyeh Ghassemi, *Algorithmic Fairness in Chest X-Ray Diagnosis: A Case Study*, MIT Case Studies in Social and Ethical Responsibilities of Computing, no. Winter 2023 (February) (Feb. 27, 2023), https://mit-serc.pubpub.org/pub/algorithmic-chest/release/2.
[35] Ziad Obermeyer, Brian Powers, Christine Vogeli & Sendhil Mullainathan, *Dissecting Racial Bias in Algorithm Used to Manage the Health of Populations*, Science (Oct. 25, 2019), https://www.science.org/doi/10.1126/science.aax2342.
[36] Eleni Manis et al., Surveillance Technology Oversight Project, *Seeing Is Misbelieving* (2024), https://www.stopspying.org/seeing-is-misbelieving; Aaron Sankin et al., *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.

exacerbates over-policing by increasing unnecessary police confrontations.[37] Reliance on facial recognition systems in policing, long criticized for lower accuracy on non-white faces,[38] has led to wrongful arrests of numerous Black individuals.[39]

These racial disparities in facial recognition technologies make their use by businesses particularly concerning. For example, many stadiums that host sporting events use video surveillance systems with facial recognition.[40] Major League Baseball teams have installed facial recognition entry systems.[41] Concert venues and music festival venues are integrating facial recognition systems, purportedly to detect ticket fraud and reduce unauthorized attendees from gaining entry.[42] Radio City Music Hall in New York recently denied a lawyer entry to a concert for which she had a ticket because the law firm she worked for was involved in a lawsuit against

[37] Letter to Attorney General Merrick Garland, EPIC (Sept. 27, 2023), https://epic.org/wp-content/uploads/2023/09/EPIC-DOJ-23-09-27-Title-VI-Petition-ShotSpotter.pdf; David Gwidt, *Shotspotter Leak Shows that Surveillance Tech is Used to Overpolice Black and Brown Communities*, ACLU Wisconsin (Mar. 6, 2024), https://www.aclu-wi.org/en/news/shotspotter-leak-shows-surveillance-tech-used-overpolice-black-and-brown-communities; Dell Cameron & Dhruv Mehrotra, *US Justice Department Urged to Investigate Gunshot Detector Purchases*, Wired (Sept. 28, 2023), https://www.wired.com/story/shotspotter-doj-letter-epic/.

[38] Christina Swarns, *When Artificial Intelligence Gets It Wrong*, Innocence Project (Sept. 19, 2023), https://innocenceproject.org/when-artificial-intelligence-gets-it-wrong/.

[39] 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/.

[40] 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/.

[41] 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.

[42] 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.

the venue's parent company.[43] RiteAid, the pharmacy chain, used facial recognition technology in its stores that disproportionately and falsely identified people of color as likely shoplifters, spurring an FTC settlement banning the company from using facial recognition technology.[44] Wide adoption of facial recognition to automatically detect people to prevent entry into a business can create a private network of watchlists that individuals don't know that they might be on and have no ability to appeal, while disproportionately impacting people of color.

In housing, ADMTs impact tenant screening, mortgages, and applications for public housing. For example, EPIC filed a consumer protection complaint against a tenant screening company, RentGrow, for automatically generating tenant screening reports with serious errors and racial biases that impeded applicants' ability to apply for apartments.[45] Errors in tenant screening reports have serious ramifications for individuals, hindering their ability to secure housing they can afford in a timely manner, disproportionately impacting low-income people and

[43] 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.
[44] 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; Press Release, Fed. Trade Comm'n, *Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology Without Reasonable Safeguards* (Dec. 19, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without.
[45] Complaint of EPIC, *NACA v. RentGrow* (Oct. 1, 2024), https://epic.org/documents/naca-v-rentgrow/.

people of color.[46] Algorithms used in making mortgage lending decisions have shown racial disparities, rejecting mortgage applications by people of color at higher rates.[47]

Throughout education, students are scrutinized by various ADMT systems. Colleges and universities are increasingly using ADMTs to help make enrollment and scholarship decisions.[48] In one survey, a majority of schools using AI say they already employ it to make final decisions at some point in the process.[49] However, studies show that algorithms used to predict future student success produce more inaccurate results for Hispanic and Black students compared to white students.[50]

Schools are also increasingly turning to technology that use apps, cameras, noise detectors, and invasive mental health prediction tools with poor results.[51] For example, schools

---

[46] 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 [hereinafter "EPIC Screened & Scored Report"]; 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/.

[47] Emmanuel Martinez & Lauren Kirchner, *The Secret Bias Hidden in Mortgage-Approval Algorithms*, The Markup (Aug. 25, 2021), https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms; Taylor Giorno, *Fed Watchdog Warns AI, Machine Learning May Perpetuate Bias in Lending*, The Hill (July 18, 2023), https://thehill.com/business/housing/4103358-fed-watchdog-warns-ai-machine-learning-may-perpetuate-bias-in-lending/.

[48] Lilah Burke, *Why Colleges Are Using Algorithms to Determine Financial Aid Levels*, Higher Ed Dive (Sept. 5, 2023), https://www.highereddive.com/news/colleges-enrollment-algorithms-aid-students/692601/.

[49] Jonathan Chang & Meghna Chakrabarti, *Colleges Are Using AI in Admissions. How Can They Do it Right?*, WBUR (Sept. 4, 2024), https://www.wbur.org/onpoint/2024/09/04/colleges-ai-admissions-application-university-students#.

[50] Denisa Gándara, Hadis Anahideh, Matthew Ison & Lorenzo Picchiarini, *Inside the Black Box: Detecting and Mitigating Algorithmic Bias Across Racialized Groups in College Student-Success Prediction*, AERA Open (July 11, 2024), https://www.aera.net/Newsroom/Inside-the-Black-Box-Detecting-and-Mitigating-Algorithmic-Bias-Across-Racialized-Groups-in-College-Student-Success-Prediction; Erik Ofgang, *Colleges Are Using AI To Predict Student Success. These Predictions Are Often Wrong*, Yahoo News (Aug. 29, 2024), https://www.yahoo.com/news/colleges-using-ai-predict-student-090000670.html?guccounter=2.

[51] Sarah Roth et al., *Orwell's Classroom: Psychological Surveillance in K-12 Schools*, Surveillance Technology Oversight Project (2023),

monitor students on school-provided devices, using internet searches, social media posts, and private messages with friends to flag students that are considered at-risk of mental health emergencies.[52] While there are examples of successful interventions, the surveillance persists through all hours of the day, and overall efficacy of the systems is unproven.[53] The Center for Democracy and Technology reports that while many technologies are marketed to improve student safety, they are more often used for student discipline, with disproportionately harmful impact to students of color and LGBTQ+ students.[54] Monitoring technology has put students at higher risk of interactions with law enforcement, outed LGBTQ+ students to administrators, and led to a chilling effect on students' ability to express themselves.[55] Schools are also deploying "aggression detectors" that purport to detect aggressive behavior so that security officers can "engage antagonistic individuals immediately."[56] However, these detectors have high rates of false alarms, creating unnecessary confrontations between students and law enforcement.[57]

---

https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/6577641fcf3354170a1df2b1/1702323231386/2023-12-11+Mental+Health+School+Surveillance.pdf.

[52] Ellen Barry, *Spying on Student Devices, Schools Aim to Intercept Self-Harm before it Happens*, N.Y. Times (Dec. 9, 2024), https://www.nytimes.com/2024/12/09/health/suicide-monitoring-software-schools.html.

[53] *Id.*

[54] Elizabeth Laird et al., *Report-Hidden Harms: The Misleading Promise of Monitoring Students Online*, Center for Democracy and Technology (Aug. 3, 2022), https://cdt.org/insights/report-hidden-harms-the-misleading-promise-of-monitoring-students-online/.

[55] *Id.*; Alejandra Caraballo, *Remote Learning Accidentally Introduced a New Danger for LGBTQ Students*, Slate (Feb. 24, 2022), https://slate.com/technology/2022/02/remote-learning-danger-lgbtq-students.html.

[56] Jack Gillum & Jeff Kao, *Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students*, ProPublica (June 25, 2019), https://features.propublica.org/aggression-detector/the-unproven- invasive-surveillance-technology-schools-are-using-to-monitor-students/.

[57] *Id.*; Drew Harwell, *Parkland School Turns to Experimental Surveillance Software that Can Flag Students as Threats*, Wash. Post (Feb. 13, 2019), https://www.washingtonpost.com/technology/2019/02/13/parkland-school-turns-experimental-surveillance-software-that-can-flag-students-threats/.

Remote provision of exams during the pandemic also incentivized the adoption of technology that purports to detect cheating.[58] Numerous companies in the U.S. claim their software can accurately detect and prevent cheating in online tests.[59] However, these technologies invade student privacy and discriminate against students of color and students with disabilities. For example, proctoring software consistently prompted one black female university student "to shine more light on her face," and denied her exam access because the system could not validate her identity.[60] Emotion recognition systems also tend to label disabled or neurodivergent students as suspicious.[61] Because different disabilities may affect how an individual looks, moves, communicates, expresses themself, processes information, or copes with anxiety, students with disabilities are at a higher risk of being flagged as suspicious when their demeanor simply differs from the majority.[62]

Behavioral advertising invades consumer privacy. Much of the sweeping collection of data is in service of behavioral advertising, which relies on the use of ADMTs to function.[63] Behavioral advertising allows advertisers to determine who should be targeted with economic

[58] Clive Thompson, *What AI College Exam Proctors Are Really Teaching Our Kids*, Wired (Oct. 20, 2020), https://www.wired.com/story/ai-college-exam-proctors-surveillance/.
[59] Shea Swauger, *Software that Monitors Students During Tests Perpetuates Inequality and Violates Their Privacy*, MIT Tech. Rev. (Aug. 7, 2020), https://www.technologyreview.com/2020/08/07/1006132/software-algorithms-proctoring- online-tests-ai-ethics/.
[60] *Id.*; *see also* Mitchell Clark, *Students of Color Are Getting Flagged to Their Teachers Because Testing Software Can't See Them*, The Verge (Apr. 8, 2021), https://www.theverge.com/2021/4/8/22374386/proctorio-racial-bias- issues-opencv-facial-detection-schools-tests-remote-learning.
[61] Lydia X. Z. Brown, *How Automated Test Proctoring Software Discriminates Against Disabled Students*, Center for Democracy and Technology (Nov. 16, 2020), https://cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students/.
[62] *Id.*
[63] EPIC FTC Comments on Commercial Surveillance, *supra* note 8, at 48–49; Sauvik Das & Yuxi Wu, *How Online Behavioral Advertising Harms People*, Center for Democracy and Technology (Dec. 13, 2023), https://cdt.org/insights/how-online-behavioral-advertising-harms-people/.

opportunities based on detailed profiles of individuals.[64] This can cause harm to marginalized communities by reinforcing inequities in opportunities for housing, healthcare, financial services, employment, and educational opportunities.[65] For example, advertisers can use characteristics like race, gender, income, or proxies like zip codes for income or race, to filter their audience and target certain audience segments.[66]

In 2017, ProPublica reported that employment ads on Facebook were targeted to certain age groups, excluding older workers.[67] In 2019, Facebook was reported to allow employment advertising targeting only one gender, often in line with gender stereotypes about the role advertised.[68] Also in 2019, the Department of Housing and Urban Development charged Facebook with engaging in housing discrimination by allowing advertisers to determine which users saw housing ads based on protected characteristics such as race, religion, and national origin.[69] In 2023, Facebook's parent company, Meta, settled a case with the Department of

---

[64] Jeremy B. Merrill, *Does Facebook Still Sell Discriminatory Ads?*, The Markup (Aug. 25, 2020), https://themarkup.org/the-breakdown/2020/08/25/does-facebook-still-sell-discriminatory-ads; Bennett Cyphers & Adam Schwartz, *Ban Online Behavioral Advertising*, Electronic Frontier Foundation (Mar. 21, 2022), https://www.eff.org/deeplinks/2022/03/ban-online-behavioral-advertising.

[65] Anita Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform*, 131 Yale L.J.F. 907, 913–28 (Feb. 20, 2022), https://www.yalelawjournal.org/forum/dismantling-the-black-opticon; Till Speicher, *Potential for Discrimination in Online Targeted Advertising*, Proc. of the 1st Conference on Fairness, Accountability and Transparency, 81 Proc. Mach. Learning Rsch. 5 (2018), https://proceedings.mlr.press/v81/speicher18a.html ("The potential for discrimination in targeted advertising arises from the ability of an advertiser to use the extensive personal (demographic, behavioral, and interests) data that ad platforms gather about their users to target their ads. An intentionally malicious—or unintentionally ignorant—advertiser could leverage such data to preferentially target (i.e., include or exclude from targeting) users belonging to certain sensitive social groups (e.g., minority race, religion, or sexual orientation).").

[66] *Surveillance Advertising: What About Discrimination?*, Consumer Federation of America (Aug. 26, 2021), https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-discrimination/.

[67] 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.

[68] 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.

[69] 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.

Justice that alleged the platform's ad targeting systems caused algorithmic discrimination on the basis of race and sex; the settlement required Meta to develop a new ad system that addresses this algorithmic discrimination and to work with an independent, third-party auditor to ensure compliance with the settlement.[70] Just this month, the nonprofit Equal Rights Center sued Meta, alleging that its advertising system causes algorithmic discrimination by disproportionately targeting Black users with advertisements for for-profit colleges and universities while targeting white users with ads for public nonprofit colleges and universities.[71]

Advertisers can infer and target specific sensitivities and vulnerabilities to increase clicks and sales.[72] These conditions include mental and physical health conditions,[73] medical conditions (including pregnancy and addiction),[74] financial instability,[75] bereavement,[76] and unhealthy body stigma.[77] In fact, credit agencies label individuals with categories like "Struggling Elders,"

---

[70] Press Release, *Justice Department and Meta Platforms Inc. Reach Key Agreement as They Implement Groundbreaking Resolution to Address Discriminatory Delivery of Housing Advertisements*, Department of Justice (Jan. 9, 2023), https://www.justice.gov/archives/opa/pr/justice-department-and-meta-platforms-inc-reach-key-agreement-they-implement-groundbreaking.

[71] 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/.

[72]Yuxi Wu, W. Keith Edwards, Sydney Bice & Sauvik Das, *The Slow Violence of Surveillance Capitalism*, 2023 ACM Conference on Fairness, Accountability, and Transparency (June 12-15, 2023), https://dl.acm.org/doi/pdf/10.1145/3593013.3594119.

[73] Stevie Chancellor et al., *A Taxonomy of Ethical Tensions in Inferring Mental Health States from Social Media*, In Proceedings of the conference on fairness, accountability, and transparency, 79–88 (2019), https://dl.acm.org/doi/10.1145/3287560.3287587.

[74] Jon Keegan & Joel Eastwood, *From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You*, The Markup (June 8, 2023), https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you.

[75] *Id.*

[76] *Id.*; Rae Nudson, *When Targeted Ads Feel a Little Too Targeted*, Vox (Apr. 9, 2020), https://www.vox.com/the-goods/2020/4/9/21204425/targeted-ads-fertility-eating-disorder-coronavirus.

[77] Liza Gak, Seyi Olojo, & Niloufar Salehi, *The Distressing Ads that Persist: Uncovering the Harms of Targeted Weight-Loss Ads Among Users with Histories of Disordered Eating*, Proc. ACM Hum.-Comput. Interact. 6, CSCW2, Article 377 (Nov. 2022), https://arxiv.org/abs/2204.03200.

"Tough Times," and "retiring on empty."[78] Armed with profiles of consumers, advertisers can target products that exploit such knowledge to push them to purchase products or services, which may not be in the consumer's best interest. For example, payday loan companies target young people in need of cash, who may not understand the consequences of such high-interest loans.[79] Anti-abortion groups advertised to people potentially seeking abortion through device locations at or near clinics such as Planned Parenthood to send misleading ads for anti-abortion "crisis pregnancy centers."[80] This pervasive and manipulative online landscape that behavioral advertising creates causes harms such as psychological distress, loss of autonomy, change of behavior online, and marginalization or manipulation of vulnerabilities.[81]

Americans are dissatisfied with this reality. In a 2024 survey report by Consumer Reports, nearly half of U.S. adults said that they would be "very uncomfortable" if AI programs had a role in the job interview process, and about 4 in 10 adults said they would be "very uncomfortable" if banks used an AI program to determine if applicants qualified for a loan.[82] Most Americans (83%) said if an AI or algorithm had been used to determine whether or not they would be interviewed for a job they applied for, they would want to know specifically what information the program used to make the decision.[83] AI provides a cloak of unwarranted rationality to decisions based on ADMT outputs that makes holding such decisions accountable

[78] Keegan & Eastwood, *supra* note 74.
[79] Sergio Flores & Nicholas Kjeldgaard, *Payday Loan Ads on Social Media Targeting New, Young Audience*, NBC San Diego (June 16, 2022), https://www.nbcsandiego.com/news/investigations/nbc-7-responds/payday-loan-ads-on-social-media-targeting-new-young-audience/2972920/.
[80] Justin Sherman, *The Data Broker Caught Running Anti-Abortion Ads—To People Sitting in Clinics*, Lawfare (Sept. 19, 2022), https://www.lawfaremedia.org/article/data-broker-caught-running-anti-abortion-ads—-people-sitting-clinics.
[81] Wu, Edwards, Bice & Das, *supra* note 72.
[82] Consumer Reports, *AI/Algorithmic Decision Making: Consumer Reports Nationally Representative Phone and Internet Survey* (2024), https://advocacy.consumerreports.org/wp-content/uploads/2024/07/Public-Facing-Report-2024-AES-AI-Algorithms-7.25.24.pdf.
[83] *Id.*

difficult.[84] Consumers are often left unable to determine what data is collected, for what reason, how it is used, how automated decisions are made about them, and how to appeal such decisions.[85] Because ADMTs can centralize biased data and assumptions and automate the decision-making process, they expand the scale of erroneous and unfair outcomes, including discrimination, to masses of people.[86] For these reasons, it is past time for regulatory frameworks to move beyond notice and consent regimes to allow consumers to have actionable transparency and meaningful choices around ADMTs, including those used in behavioral advertising. EPIC commends the CPPA for tackling this important issue.

c. Strong ADMT provisions will ensure adequate coverage, establish strong opt-out and correction rights, and limit exceptions.

The proposed ADMT provisions offer important steps to ensure that covered entities using ADMTs are accountable to impacted individuals, but there are ways to further ensure that consequential ADMT uses will be covered and that Californians will have meaningful ways to opt out of or challenge ADMT decisions. To strengthen the protections that the ADMT provisions will provide, EPIC and CFA make six recommendations. First, the definition of ADMT should be strengthened by adopting the State Administrative Manual's definition to ensure the definitions cover the most frequently used contexts of ADMTs for significant decisions. Second, it is important that the ADMT provisions retain the right of consumers to opt out of profiling for behavioral advertising. Third, the consumers' right to opt out should be extended to use of personal data to train generative AI. Fourth, the human appeal exception to the right to opt out of ADMT use should be removed. Fifth, the access right should be strengthened to ensure Californians have actionable information about ADMT decisions and

[84] TechTonic Justice Report, *supra* note 23, at 6.
[85] *Id.*
[86] *Id.* at 15.

clarify how the right to correct works in practice. And lastly, the exceptions for security, fraud detection, and safety should be construed narrowly. Without these changes, the privacy protections in the ADMT regulations may be more easily sidestepped or denied to consumers.

First, the definition of automated decisionmaking technology should be strengthened. We urge the Agency to adopt the State Administrative Manual (SAM)'s definition of Automated Decision System, in place of the current proposed regulation's definition ADMT definition. The SAM definition is broader and more appropriate for regulating the commercial use of ADMTs:

> Automated Decision System: A computational process derived from machine learning, statistical modeling, data analytics, or artificial intelligence that issues simplified output, including a score, classification, or recommendation, that is used to assist or replace human discretionary decisionmaking and materially impacts natural persons. An "automated decision system" does not include a spam email filter, firewall, antivirus software, identity and access management tools, calculator, database, dataset, or other compilation of data.[87]

This definition is more effective than the definition in the proposed regulations because it is both sufficiently broad to cover the contexts in which ADMTs are most often used as part of significant decisions (specifically, to *assist* humans in making significant decisions) and sufficiently specific to ensure that the ways ADMTs are most often used (to generate a score or recommendation about an individual) are covered.

First, the SAM definition covers situations in which ADMTs "replace" human decisionmaking but also situations in which the ADMT "assists" a human decisionmaker. In contrast, the current proposed definition only covers ADMTs that "execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking."[88] The current

[87] California Department of General Services, State Administrative Manual, Definitions - 4819.2 (last revised March 2024). Accessed at https://www.dgs.ca.gov/Resources/SAM/TOC/4800/4819-2.
[88] Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies, § 7001 (Nov. 22, 2024) [hereinafter Proposed Regulations].

definition is quite narrow. By adding the "substantially" modifier to "facilitates" in the latest draft,[89] the Agency risks creating a loophole for controllers to argue that they do not need to comply with these regulations because they do not consider their use of ADMTs to be "substantial" in facilitating a significant decision. The regulations state that an automated decision system "substantially facilitates" human decision if the system's output is a "key factor" in the human's decision.[90] This narrowing of the definition of ADMT incentivizes controllers to classify as many uses of ADMTs as possible as unlikely to "substantially facilitate" human decisionmaking, even when those decisions may be about topics as significant as an individual's health care, employment, or housing. In fact, research shows that humans are likely to place too much trust in the outputs of an automated decision system, so these systems will likely play a key role in human's decisions, whether a controller classifies the system as "substantially facilitating" human decisionmaking or not.[91]

Second, the SAM definition explicitly includes uses of AI to produce a "score, classification, or recommendation," which, in practice, is the type of ADMTs controllers are most likely to be using in the process of making significant decisions about an individual. The SAM definition also clearly delineates everyday uses of AI that are not considered automated decision systems, such as spam filters and firewalls. The Agency should replace the current definition of automated decisionmaking technology in the proposed regulations with the SAM definition of automated decision system to provide additional clarity for businesses about which uses of ADMTs are covered by these regulations and which are not and to ensure risky uses of ADMTs are covered.

[89] Proposed Regulations, *supra* note 88, at § 7001.
[90] Proposed Regulations, *supra* note 88, at § 7001(2).
[91] Lauren Leffer, *Too Much Trust in AI Poses Unexpected Threats to the Scientific Process*, SCIENTIFIC AMERICAN (Mar. 18, 2024), https://www.scientificamerican.com/article/trust-ai-science-risks/.

Finally, because the SAM definition is already in use in California, adopting this definition will better align these regulations with other areas of state policy on artificial intelligence, such as public sector AI procurement and other agency regulations.[92]

Second, the Agency should retain the right of consumers to opt out of profiling for behavioral advertising. Due to the risks that profiling of consumers poses to their privacy, EPIC commends the CPPA for explicitly including profiling within the definition of ADMTs.[93] Short of banning behavioral advertising outright, allowing individuals to opt out of the use of ADMTs for behavioral advertising purposes, with no exemptions, is the best way to protect Californians. Requiring opt-outs gives consumers a real choice about whether they benefit from behavioral advertising or whether they want to opt out.

The advertising industry tends to claim that a mandated opt-out option will undermine the entire digital ecosystem. However, targeted ads based on profiling results in consumers seeing advertisements for lower quality products with higher prices that are largely irrelevant to them.[94] The opt-out will provide consumers with choice and encourage the advertising industry to innovate toward advertising methods that do not sacrifice consumer privacy. Thus, the Agency should retain this opt-out right for behavioral advertising.

This right builds in crucial ways on the CCPA behavioral advertising rules already in place. The existing rules allow people to opt out of behavioral advertising that is "cross-context," meaning that the advertising is based on the consumer's personal information "across businesses,

[92] California Department of Technology, *State of California GenAI Guidelines for Public Sector Procurement, Uses and Training* (March 2024). Accessed at https://www.govops.ca.gov/wp-content/uploads/sites/11/2024/03/3.a-GenAI-Guidelines.pdf.
[93] Proposed Regulations, *supra* note 88, at § 7001(f)(3).
[94] Sara Geoghegan, *Data Minimization: Regulating the Ineffective, Irrelevant, and Invasive Practice of Surveillance Advertising*, EPIC (Aug. 8, 2023), https://epic.org/data-minimization-regulating-the-ineffective-irrelevant-and-invasive-practice-of-surveillance-advertising/.

distinctly-branded websites, applications, or services."[95] The opt-out limitation to only cross-context behavioral advertising is significant because it allows large consumer-facing platforms—like Meta, Google, Microsoft, and Amazon—to continue serving behavioral advertising even when people don't want them. An opt-out rule, like the one in the proposed regulations, is warranted because, as the CPRA states, "[r]ather than diluting privacy rights, California should strengthen them over time."[96]

Third, the Agency should extend consumers' right to opt out of the use of personal data to train AI to include generative AI. Under the proposed regulations, consumers would be able to prevent the use of their data for training ADMT systems that are capable of being used (1) for a significant decision concerning a consumer; (2) to establish individual identity; (3) for a physical or biological identification or profiling; or (4) for the generation of a deepfake.[97] We commend the Agency for including this right. For years, consumers' privacy has been violated by companies that use personal data to train powerful and lucrative technologies. For example, FTC settled with a company called Everalbum for using consumers' photos uploaded to its services to train its facial recognition model without obtaining consent.[98] Facebook was sued in Illinois for harvesting facial data for its photo-labeling service without user permission.[99] It is never necessary for businesses to develop ADMT models using consumers' data without consent. With the proposed regulations, Californians can have a say in whether they consent to

[95] Cal. Civ. Code § 1798.140(k).
[96] California Privacy Rights Act, Section 2(E).
[97] Proposed Regulations, *supra* note 88, at § 7200 (a)(3).
[98] Press Release, Fed. Trade Comm'n, *California Company Settles FTC Allegations It Deceived Consumers About Use of Facial Recognition in Photo Storage App* (Jan. 11, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/01/california-company-settles-ftc-allegations-it-deceived-consumers-about-use-facial-recognition-photo.
[99] Natasha Singer & Mike Isaac, *Facebook to Pay $550 million to Settle Facial Recognition Suit*, N.Y. Times (Jan. 29, 2020), https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html.

their personal data being used to train ADMTs, separate from their choice to interact with the covered entity in the first place.

With that said, the proposed opt-out for training ADMTs should also extend to training generative AI models. Section 7221(b)(6)'s requirement to provide opt-out does not generally cover processing personal information of consumers to train ADMT or artificial intelligence that can be used for the operation of generative models, such as large language models. However, such use is included in the list of processing activities that present significant risk to consumers' privacy under § 7150(b), along with the other uses for which processing of personal information to train ADMTs requires providing ability to opt out under § 7221(b)(6).[100] Because the processing presents significant risk to consumers' privacy, the processing entity must conduct a risk assessment to initiate the processing.[101] If processing of data to train generative models presents a significant risk to consumers' privacy, it should be included among the types of models that trigger the requirement for covered entities to provide a training opt-out.

Many large tech firms began training their generative AI models before notifying users or allowing users to opt-out beforehand. The list includes Meta's Instagram,[102] LinkedIn,[103] Microsoft's Bing,[104] and X's Grok.[105] The training of AI models using vast, scraped data sets of

[100] Proposed Regulations, *supra* note 88, at § 7150(b)(4).
[101] Proposed Regulations, *supra* note 88, at § 7150(a).
[102] Geoffrey A. Fowler, *Your Instagrams Are Training AI. There's Little You Can Do About It*., Wash. Post (Sept. 27, 2023), https://www.washingtonpost.com/technology/2023/09/08/gmail-instagram-facebook-trains-ai/.
[103] Joseph Cox, *LinkedIn Is Training AI on User Data Before Updating its Terms of Service*, 404 Media (Sept. 18, 2024), https://www.404media.co/linkedin-is-training-ai-on-user-data-before-updating-its-terms-of-service/.
[104] Katyanna Quach, *Microsoft May Store Your Conversations with Bing if You're Not an Enterprise User*, The Register (Aug. 15, 2023), https://www.theregister.com/2023/08/15/microsoft_will_store_your_conversations/.
[105] Omar Gallaga, *X Is Using Your Tweets to Train its AI. Disabling that Is Still an Option, for Now*, CNET (Oct. 22, 2024), https://www.cnet.com/tech/services-and-software/x-is-using-your-tweets-to-train-its-ai-heres-how-to-disable-that/.

personal information violated—and continues to violate—consumers' privacy by putting their personal data to unnecessary, unexpected, and out-of-context uses. Further, training generative AI models using personal data can lead to the model leaking personal data unexpectedly when it is deployed to the market, threatening further privacy harms.[106] Sometimes, businesses allow consumers to opt out, but others either do not offer an opt-out or, worse, automatically opt consumers in to having their data used to train AI.[107] Even if companies do allow consumers to opt out, it's unclear what happens to the data ingested by the training model prior to opting out, and it is impossible for consumers to ensure their data is fully deleted from the training set. The proposed regulations should include processing of personal data for training generative models in the list of uses for which businesses must provide an opt-out to consumers.

Fourth, the Agency should remove the human appeal exception to the right to opt out of ADMT use. The proposed regulations allow businesses to avoid offering an opt-out when ADMTs are used to make a significant decision concerning a consumer if the business provides a "method to appeal the decision to a qualified human reviewer who has the authority to overturn the decision."[108] This exception significantly weakens the opt-out provision. A human appeal process should be required in addition to an opt-out provision.

The current exception provides a path for businesses to avoid providing opt-outs by having human reviewers rubber-stamp ADMT outputs. Even if reviewers "consider the relevant information provided by the consumer in their appeal,"[109] human reviewers are likely to be

[106] Gerrit De Vynch, Rachel Lerman & Mitasha Tiku, Microsoft's AI Chatbot is Going off the Rails, Wash. Post (Feb. 16, 2023), https://www.washingtonpost.com/technology/2023/02/16/microsoft-bing-ai-chatbot-sydney/; Vilius Petkauskas, *ChatGPT Tied to Samsung's Alleged Data Leak*, Cybernews (Apr. 6, 2023), https://cybernews.com/news/chatgpt-samsung-data-leak/.
[107] Fowler, *supra* note 102.
[108] Proposed Regulations, *supra* note 88, at § 7221(b)(2).
[109] Proposed Regulations, *supra* note 88, at § 7221(b)(2)(A).

biased toward affirming the decision of the ADMT system, since people tend to overestimate the accuracy of AI outputs and businesses are incentivized to create processes that make approving ADMT outputs much easier than overturning or questioning them. With the human appeal exception, the option for consumers to opt out of ADMTs for uses outside those where opt-outs are required could become illusory.

Fifth, the Agency should strengthen the right of access to ensure Californians have actionable information about ADMT decisions and clarify how the right of correction must work in practice. We commend the Agency for including a pre-use notice requirement for businesses that use ADMTs and the right for consumers to access ADMTs. ADMTs are currently opaque to consumers that interact with them, preventing access to inner workings of how decisions were made. This opacity also prevents broader understanding of how ADMTs impact consumers based on protected classes, undermining meritorious antidiscrimination and consumer protection claims.[110]

Although the regulations establish the important rights to correct information and request access to ADMTs,[111] there are two critical gaps that should be addressed to make these rights meaningful for Californians. First, the Agency should strengthen the requirements for the information that must be given to consumers in response to access requests. Second, the Agency should clarify how a business must respond after consumers exercise their right to correct inaccurate information.

First, the nature of the right of access allows Californians to access information about how an ADMT worked in their specific circumstances only after an adverse decision is made about them. This information asymmetry and power imbalance between companies and

[110] EPIC Screened & Scored Report, *supra* note 46, at 22-23.
[111] Proposed Regulations, *supra* note 88, at §§ 7023, 7222.

individuals intensifies the need for actionable and detailed post-use consumer notices so that disadvantaged individuals can hold the necessary parties accountable in court or during an appeals process.

However, the post-use notice is only valuable to consumers if it is actionable. Without understanding how they compare to other consumers, consumers faced with adverse ADMT decisions will not know whether they should pursue additional action. For example, if a person who knows they have a high credit score sees they were considered a “high risk” for missing payments, they may choose to follow up with the landlord to ensure the system had accurate information. Or if a Black applicant was in the 99th percentile for "rentability” but was still denied, they may choose to pursue legal action against the company under anti-discrimination laws. Thus, to empower consumers, the regulations should be changed so that a business must provide contextual information. This requires only a small change to the existing regulations:

> **§ 7222. Requests to Access Information About the Business’s Use of Automated Decisionmaking Technology.**
>
> (b)(4)(C) A business also ~~**may**~~ **shall** provide the range of possible outputs ~~**or**~~ **and** aggregate output statistics to help a consumer understand how they compare to other consumers. For example, a business may provide the five most common outputs of the automated decisionmaking technology, and the percentage of consumers that received each of those outputs during the preceding calendar year.

Second, while California consumers and workers have the right to correct inaccurate information about themselves, there is no clear mechanism in these proposed regulations for remedying decisions made about them based on inaccurate information fed to an ADMT. The Agency should clarify either (1) that the right to correct information fed to an ADMT inherently includes a right to have the decision based on that inaccurate information reconsidered or (2) that individuals have a separate right to reconsideration when decisions made using an ADMT were based on inaccurate information. This clarification is clearly within the intent of the CCPA and

these proposed regulations, but without spelling out this right explicitly, California consumers and workers could be left unprotected. Companies using ADMTs in decisions may not willingly reconsider decisions, even if the personal information they input into the system is later found to be inaccurate and corrected, so the Agency should require companies to reconsider their decisions in this situation. The rights for individuals to both correct inaccurate information and to appeal adverse decisions is already in the Colorado AI Act,[112] which the agency could look to as a model for adding this type of provision into these proposed regulations.

Finally, exceptions for security, fraud detection, and safety should be construed narrowly. We commend the CPPA for including a substantive data minimization requirement under § 7050, which allows service providers and contractors to retain, use, or disclose personal information for enumerated purposes including prevention, detection, or investigation of fraudulent or illegal activity, provided that the "retention, use, or disclosure is reasonably necessary and proportionate" for such purposes.[113]

Historically, businesses have often used fraud prevention and detection as a cover to collect broad swaths of data. Indeed, data brokers like RELX have exploited fraud prevention to justify bulk collection of personal information,[114] which they then sell to advertisers, law enforcement agencies, and other third parties.[115] EPIC's report on DC government's use of ADMTs found that the system used to detect fraud in SNAP benefits collect data from a wide variety of sources, including data brokers, social networking sites, credit reporting agencies, web

[112] S.B. 24-205, 2024 Gen. Assemb., Reg. Sess. (Colo. 2024).
[113] Proposed Regulations, *supra* note 88, at § 7050(a).
[114] Alfred Ng, *Data Brokers Raise Privacy Concerns – but Get Millions from the Federal Government*, Politico (Dec. 21, 2022), https://www.politico.com/news/2022/12/21/data-brokers-privacy-federal-government-00072600.
[115] Emile Ayoub & Elizabeth Goitein, *Closing the Data Broker Loophole*, Brennan Center for Justice (Feb. 13, 2024), https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole.

scrapers, government databases, agency records, and location data.[116] This broad collection exposes consumers to privacy harms and unnecessary risks of data breaches.[117] Thus, it is important that retention, use, or disclosure of personal information for fraud detection, prevention, and investigation purposes have substantive limitations.

Other provisions related to data collection, use, and disclosure for fraud detection also raise concerns. There are many examples of fraud detection systems in the public benefits context falsely flagging individuals, causing these applicants to have essential healthcare benefits, unemployment benefits, or disability benefits cut off.[118] Oftentimes, the fraud detection systems produce discriminatory outputs based on factors that are proxies for protected characteristics.[119] Research on commercial fraud detection systems indicates that these systems also exhibit race, gender, and disability biases.[120]

Two provisions in the proposed regulations may prevent the CPPA and consumers' ability to understand how fraud detection ADMTs are used by covered entities when processing consumers' data. Under the risk assessment section, the proposed regulation provides that "[a] business is not required to provide information that would compromise its ability to prevent,

---

[116] EPIC Screened & Scored Report, *supra* note 446, at 24-25.
[117] *Id.* at 29-30.
[118] TechTonic Justice Report, *supra* note 23, at 48-49; Parker L. Gilkesson, *SNAP 'Program Integrity': How Racialized Fraud Provisions Criminalize Hunger,* The Center for Law and Social Policy (2022), https://www.clasp.org/wp-content/uploads/2022/04/2022_SNAP20Program20Integrity20-20How20Racialized20Fraud20Provisions20Criminalize20Hunger.pdf.
[119] TechTonic Justice Report, *supra* note 23, at 6; EPIC Screened & Scored Report, *supra* note 46, at 23; *see also* Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* 1 (2018).
[120] Danny Butvinik, *Bias and Fairness of AI-Based Systems Within Financial Crime*, NICE Actimize (July 25, 2022), https://www.niceactimize.com/blog/fraud-bias-and-fairness-of-ai-based-systems-within-financial-crime/; José Pombal et al., *Understanding Unfairness in Fraud Detection Through Model and Data Bias Interactions*, KDD'22 Workshop on Machine Learning in Finance (July 13 2022), https://arxiv.org/abs/2207.06273; Parameswaran Kamalaruban et al., *Evaluating Fairness in Transaction Fraud Models: Fairness Metrics, Bias Audits, and Challenges*, Proc. Of the 5th ACM International Conference on AI in Finance 555-563 (Nov. 14, 2024), https://dl.acm.org/doi/10.1145/3677052.3698666.

detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information; resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions; or ensure the physical safety of natural persons."[121] Under the "Requests to Access ADMT" section, covered entities can rely upon the "security, fraud prevention, and safety exception" to avoid providing consumers with ability to opt out.[122] This exemption also allows covered entities to avoid providing consumers with an explanation of how the ADMT worked in relation to their individual circumstances if it would compromise the business's use of ADMT.[123] This overly broad exemption creates the risk that entities will be able to avoid providing consumers with information that they are entitled to under the proposed regulations.

Together, the proposed regulations may shield businesses' collection, use, and processing of data for fraud prevention, security, or safety from the view of the CPPA and the public—even though fraud alerts may lead to adverse significant decisions for consumers and other privacy harms. These exemptions may also shield from CPPA's eyes whether covered entities' retention, use, or disclosure of personal information for fraud detection purposes is indeed "reasonably necessary and proportionate" for such purposes.

The security, fraud prevention, and safety exception for providing risk assessments of ADMT systems and explaining how an ADMT worked with regard to the consumer should be construed narrowly. Specifically, businesses should not be able to use the blanket excuse that a system is used for fraud detection to avoid any disclosure about how the ADMT worked with regard to the consumer if disclosure of such information would not compromise the functioning

[121] Proposed Regulations, *supra* note 88, at § 7157 (b)(2)(D).
[122] *Id.* at § 7222(b)(4)(D).
[123] *Id.*

of the system. The proposed regulations should include a provision similar to § 7220(c)(1), where covered entities must provide a pre-use notice with "plain language explanation of specific purpose" for which the business will use the ADMT and the business may not use generic terms such as "to improve our services." Similarly, if a covered entity is using fraud prevention, security or safety exemptions from providing access to ADMT or providing risk assessments, they should be required to provide a sufficiently detailed reason as to why disclosure will compromise the functioning of the system, rather than just using generic explanation such as that the ADMT is used for a security, fraud detection or safety purpose.

II. Risk assessment regulations

EPIC and CFA commend the Agency for the addition of Article 10, which creates requirements for a business to conduct risk assessments when the business' processing of consumers' personal information poses a significant risk to consumers' privacy. Risk assessments are crucial for businesses to assess how privacy invasive their practices are and for consumers to understand the risks associated with the processing of their personal information. This section addresses several points. First, the Agency is within its authority to require risk assessment transparency and risk assessment transparency aligns with existing California laws. Second, the abridged risk assessments should include more information, such as a plain language explanation of why the negative impacts of the processing—as mitigated by safeguards—do or do not outweigh the benefits of the processing. Third, we recommend that the Agency make the abridged risk assessment information accessible in a machine readable, searchable database available on the Agency's website. Finally, we urge the Agency to explicitly affirm that it has the authority to reject the conclusions in the assessments. The proposed risk assessment provisions are a strong start, but without public access and transparency, the Agency will fall short of its

mandate to inform consumers about the risks associated with businesses processing their personal information.

a. Risk assessment requirements are consistent with existing laws and the Agency's mission.

Risk assessment transparency aligns with the California Constitution and the California Public Records Act. Public transparency is a core principle of the California Constitution.[124] Not only does it enshrine the people's "right of access to information concerning the conduct of the people's business,"[125] but it also dictates that a "statute, court rule, or other authority . . . shall be broadly construed if it furthers the people's right of access, and narrowly construed if it limits the right of access."[126]

CCPA risk assessments submitted to the Agency fall squarely within California's constitutional right of access, as well as the right of access under the California Public Records Act. The constitutional provision was enacted to enshrine public access rights under the Act[127] and thus reflects the Act's broad definition of "public records" to include "any writing containing information relating to the conduct of the public's business prepared, owned, *used, or retained* by any state or local agency regardless of physical form or characteristics" (emphasis added).[128] For example, in *Regents of University of California v. Superior Court* (Cal. Ct. App. 2013), the Court found that private equity documents concerning investments made by a state university *did* relate to the public's business and only fell outside the purview of the Public Records Act

[124] *See* Cal. Const. art. I, § 3(b).
[125] Cal. Const. art. I, § 3(b)(1).
[126] Cal. Const. art. I, § 3(b)(2).
[127] *See Sierra Club v. Superior Court*, 302 P.3d 1026, 1032 (Cal. 2013) ("In 2004, California voters approved Proposition 59, which amended the state Constitution to provide a right of access to public records.").
[128] Cal. Gov't Code § 6252(e).

because the documents were not prepared, owned, used, or retained by the state university.[129] Similarly, CCPA risk assessments relate to the public's business because they directly impact both the public's individual rights under the CCPA and the CPPA's obligations thereunder, and any risk assessment information disclosed to the CPPA—whether through abridged risk assessments, unabridged risk assessments, or upon request—is "used[] or retained" under the meaning of the Public Records Act.

Risk assessment transparency aligns with the California Uniform Trade Secrets Act. CCPA risk assessments categorically fall outside the ambit of the California Uniform Trade Secrets Act (CUTSA).[130] Under CUTSA, a "trade secret" is any information that (1) "derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use" and (2) "is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[131] However, not all trade secrets are protected under CUTSA; only trade secrets that are disclosed or used through "improper means"—"theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage"—qualify for protection.[132] CCPA risk assessments are neither "trade secrets" nor are they acquired or disclosed through "improper means" under CUTSA.

First, CCPA risk assessments are completed for the purpose of regulatory compliance and disclosure, not for economic value. Under the draft risk assessment regulations, businesses are obligated to complete risk assessments to "determine whether the risks to consumers' privacy from the processing of personal information outweigh the benefits to the consumer, the business,

[129] 166 Cal. Rptr. 3d 166, 178–79 (Cal. Ct. App. 2013).
[130] Cal. Civ. Code § 3426 *et seq.*
[131] Cal. Civ. Code § 3426.1(d).
[132] Cal. Civ. Code § 3426.1(a)–(b).

other stakeholders, and the public from that same processing."[133] Far from providing "independent economic value" under the CUTSA, CCPA risk assessments require businesses to internalize economic externalities; they must expend resources to identify and present information about the ways their economically valuable activities may produce costs to consumers, other stakeholders, and the public. Information about businesses' completion of CCPA risk assessments is also designed for disclosure to the CPPA; whether through regular disclosures or responses to CPPA requests for information, businesses know that risk assessments will be disclosed to government agencies rather than kept confidential. In sum, CCPA risk assessments cannot be trade secrets because they are completed for the purpose of disclosure, without attaching any independent economic value.

Second, the substantive information that CCPA risk assessments must contain is not subject to the CUTSA. Under the draft regulations, businesses must include the following in risk assessments:[134]

1. The purpose for processing consumers' personal information;
2. The categories of personal information to be processed, including any sensitive personal information;
3. Operational elements of the business's processing, including the method of data collection, the business's retention plan, the technology to be used for processing, and more;
4. The benefits to the business, the consumer, other stakeholders, and the public from the processing of personal information;
5. The negative impacts to consumers' privacy associated with the processing;
6. The business's intended safeguards for addressing negative consumer impacts;
7. The business's decision to initiate the processing subject to the risk assessment;
8. Any contributors to the risk assessment; and
9. The date the risk assessment was reviewed and approved—and by whom.

Crucially, much of this information is *already* intended or required to be made public under the CCPA. Under the CCPA's notice-at-collection requirement, for example, businesses must

[133] Proposed Regulations, *supra* note 88, at § 7152.
[134] *Id.*

directly inform consumers of (1) the purpose(s) for a data collection; (2) the categories of personal information the businesses plan to collect; and (3) the business's data retention plan[135]—all of which maps onto the first three categories of information required under the CCPA's risk assessment requirement, as well as the entirety of what is required for abridged risk assessments.[136] The only categories of information in CCPA risk assessments that are unique under the CCPA are (1) the method and technology used for data collection and (2) the benefit-impact analysis, and neither raise CUTSA concerns.

Neither the method and technology for data collection nor the benefit-impact analysis—the two categories of information not already disclosed to consumers under the CCPA—are trade secrets under the CUTSA. First, the method and technology used for data collection is routinely and directly disclosed to consumers through business' privacy policies. Meta's Privacy Policy and Cookies Policy goes into great detail about how and why the business uses cookies and similar tracking technologies to collect personal data,[137] as do X's Privacy Policy,[138] OpenAI's Cookie Policy,[139] and countless other policies from businesses subject to the CCPA. And second, the benefit-impact analysis is conducted for the sole purpose of complying with the CCPA and disclosing information to the CPPA; the analysis is not conducted or maintained for economic value and not withheld from government agencies, but rather completed for the *purpose* of disclosing the information to government agencies that may use it to impose additional and sometimes costly obligations on the business.

[135] Cal. Civ. Code § 1798.100(a).
[136] Cal. Civ. Code § 7152, 7157(b)(2).
[137] *See Privacy Policy*, Meta (Nov. 14, 2024), https://www.facebook.com/privacy/policy/; *Cookies Policy*, Meta (Dec. 12, 2023), https://www.facebook.com/privacy/policies/cookies/.
[138] *See X Privacy Policy*, X (Nov. 15, 2024), https://x.com/en/privacy.
[139] *See Cookie Policy*, OpenAI (Nov. 8, 2024), https://openai.com/policies/cookie-policy/.

Third, CCPA risk assessments are not used or disclosed through improper means. Because risk assessments are intentionally disclosed to the CPPA via regular unabridged risk assessment reporting and upon-request disclosures of full risk assessments, the only form of improper means under the CUTSA that may apply is a breach of a duty to maintain secrecy. And in fact, the CCPA expressly requires the CPPA to maintain the confidentiality of information it receives under the Act *except* "to the extent that disclosure is required by the Public Records Act." As discussed in Subsection A, *supra*, CCPA risk assessments are both related to the public's business and used or retained by the CPPA, so disclosure would be required under the Public Records Act.

Risk assessment transparency is in the CPPA's best interests. Public transparency of risk assessments is not only inherently valuable as a principle of California law and policy; it is also an important tool for ensuring the effective, timely, and low-cost enactment of the CCPA's various provisions and related regulations. It does so in at least three important ways.

First, public transparency can improve enforcement and better protect the public. Given the broad scope of the CCPA and the level of detail provided within both abridged and unabridged risk assessments, the CPPA will find itself tasked with reviewing an ever-growing mountain of risk assessments for potential CCPA violations or consumer harms. The public—complete with community groups and civil society organizations like EPIC and CFA, both of which have expertise and interest in reviewing risk assessments—can serve an important supporting role for the CPPA, reviewing public risk assessment information and submitting tips to the agency for businesses or trends to investigate.

Second, making risk assessment information public by default can effectively reduce the costs of fielding Public Records Act requests or lawsuits seeking access to the information.

These processes require valuable employee time and resources that could be repurposed for affirmative investigations and enforcement processes—or a laundry list of other agency budget priorities—and thus *default* transparency is valuable on a purely budgetary basis.

Third, making risk assessment information public can help businesses to improve their own risk assessment and data collection practices. For example, increasing the adoption of effective negative impact safeguards across industries can meaningfully improve consumer protection against privacy and algorithm harms. These safeguards are not implemented for financial gain but rather for consumer protection, meaning the benefits of publicly disclosing information on benefits, negative impacts, and safeguards—particularly benefits to the public—will typically outweigh and business costs derived from information advantages.

b. Abridged risk assessments should include a plain language explanation of the business's benefit-risk analysis.

The final regulations should add a requirement that the abridged risk assessment include a plain language explanation of the benefit-risk analysis that the business is already required to perform under the proposed regulations. § 7157(b)(2) should add subsection (E) to include this explanation. This piece of the risk assessment is essential for the Agency, consumers, and the public to assess whether the business has complied with the law. The compliance burden for businesses will be minimal as businesses will have already conducted the analysis. The only further requirement is a simple, plain language summary of the already-completed analysis. The previous draft regulation language from December 2023 rightfully contained this minimal—yet crucial—requirement, and the Agency should restore that language.

c. The information contained in the abridged risk assessments should be made available in a machine readable, searchable database available on the agency website.

The Agency should provide a user-friendly way to access meaningful, company-specific information about the content and results of risk assessments required by the CCPA, consistent with the CCPA's trade secrets protections. This public database will help to protect consumers in a few ways. Civil society organizations and community groups have been strong allies in privacy and technology enforcement, providing valuable external pressure. These groups will be able to analyze the assessments and push for more privacy-protective business practices based on their contents. The Agency and Attorney General face resource constraints, making timely identification of issues difficult and public disclosure could help to alleviate this problem. Public Access to Risk Assessments mirrors public stakeholder engagement expectations in leading AI risk management frameworks (including the NIST AI RMF and OECD AI Principles). And importantly, businesses will not be incentivized simply to do the bare minimum and obscure issues within abridged risk assessments. With public disclosure and transparency, businesses will be incentivized to implement more rights-protecting business practices, explain publicly what negative impacts their practices cause, and identify what safeguards they will adopt to mitigate those impacts.

Accordingly, we suggest the following addition to the text:

7158 – Agency Publication of Risk Assessments

(a) The Agency shall create and maintain a public central repository of risk assessment content. The abridged assessment must be submitted in a format that is directly responsive to each required element in (2)(A) to facilitate the process of creating the database.

d. The regulations should grant the Agency authority to disagree with the risk assessment submissions.

The Agency should have explicit authority to review and deny a business' certification that the benefits of its processing activities outweigh the negative impacts of that processing. The purpose of the risk assessments is to restrict or prohibit processing when the risks to consumers' privacy outweigh the benefits from the processing to the consumer, business, other stakeholders, and the public. As proposed, the regulations would allow businesses to self-certify that their processing outweighs the associated negative impacts. This alone is not effective to protect consumers from harmful processing. There must be an effective oversight mechanism to ensure that the benefits and risks are appropriately and accurately assessed. The Agency is the best suited entity to oversee this and should update the regulations accordingly.

We echo the ACLU of Northern California's comments calling attention to this issue. We also endorse the language set out in those comments, which—drawing on the statutory damages provisions in Section 1798.155(a)—creates an explicit mechanism for the Agency to question and take action against deficient risk assessments:

> Upon review of a business's Risk Assessment, if the Agency has any cause to conclude that the benefits of the processing do not outweigh the costs as required by statute, the Agency may require additional documentation or evidence from the business. If the Agency determines, after reviewing any further materials as necessary, that there is probable cause for believing that the benefits of the processing do not outweigh the costs in violation of the statute, the Agency may hold a hearing pursuant to Section 1798.199.55(a) to determine if a violation has occurred. If the Agency so determines that a violation has occurred, it may issue an order requiring the violator to restrict the processing to address such costs or prohibiting the business from such processing.

III. Cybersecurity regulations

EPIC and CFA support the proposed regulations' cybersecurity audit requirements, and we offer one suggestion to strengthen the final regulations. Specifically, we support the proposed related definitions, scope of cybersecurity audits, and requirements for both auditors and third

parties. We suggest that the cybersecurity audit include information about the business' data minimization program.

Cybersecurity audits provide redress to security incidents and promote good security practices. Article 9 § 7120-24 in the proposed regulations reflect the Agency's work to protect consumers' data privacy by promoting strong cybersecurity. Cybersecurity audits are an important part of addressing data security issues, and their benefits are twofold. Retroactively, audits help to identify and redress security incidents and to inform consumers when their information has been accessed without authorization. Proactively, audits help to promote good data security practices, identify risks before they materialize against consumers, and encourage businesses to invest in strong data security protections. This is important because, as the Agency has recognized, the harms from unauthorized activity are myriad.[140] EPIC and CFA support the framing of Article 9, which centers risk to consumers instead of merely risk to businesses. Often, cybersecurity regulations focus on reducing risk to businesses of having to report breaches to their users. The Agency's approach appropriately focuses on protecting consumers against the risk of cybersecurity harms.

The cybersecurity audit definitions provide clarity to covered businesses. Section 7001[141] in the proposed regulations added definitions for terms related to cybersecurity audits

[140] The Agency's Initial Statement of Reasons said, "The harms that result from unauthorized actions related to personal information are myriad, and they can be long-lasting and severe. The harms include monetary losses, lost time and opportunities, and psychological and reputational harm." It listed identify theft, fraud losses, being denied from a financial product or service, suffering fear and anxiety from identity theft, stalking, cyberstalking, harassment, physical violence, psychological harms (including anxiety, depression, and emotional distress), incurred medical costs for treatment of such harms, social harm, death, and PTSD as possible consequences that consumers may experience as a result of unauthorized access to their personal information. Initial Statement of Reasons (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations), Cal. Privacy Protection Agency (Nov. 22, 2024), at pp.4-6 https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_isor.pdf.
[141] Proposed Regulations, *supra* note 88, at § 7001(l)-(m).

that help provide clarity for businesses and customers. Subsection (l) defines "cybersecurity audit" and provides a clear threshold for businesses to determine whether they must conduct a cybersecurity audit. It further defines "cybersecurity program" in subsection (m) which harmonizes different related descriptions and definitions to make the regulations more readable and understandable.

The scope of the cybersecurity audit requirements ensures complete auditing. Section 7123 of the proposed regulations provides the requirements for the scope of a cybersecurity audit. It requires that a business document and assess its cybersecurity program, and it must identify the components found in § 7123(b)(2), including: authentication; encryption; zero trust architecture; restricting privileged accounts' access functions to only those necessary to perform the account-holder's job; network monitoring and defenses; retention schedules; and oversight of service providers, contractors, and third parties to ensure compliance with other parts of the proposed regulations.[142] These are necessary components for an effective cybersecurity audit. § 7123 further requires that a "[i]f the cybersecurity audit, assessment, or evaluation completed for the purpose of compliance with another law or regulation or for another purpose does not meet all of the requirements of this Article, the business must supplement the cybersecurity audit with any additional information required to meet all of the requirements of this Article." This is an example of the Agency leading the way to better protect the data security of consumers. This will prevent businesses from submitting a weaker or less complete audit because they are required to do so under a different law or regulation. Often, businesses will write off compliance requirements by claiming they are regulated under a different law or regulation. With this

[142] *Id.* at § 7123(b)(2).

provision, businesses will likely perform the more robust cybersecurity audit, and this will set a new, higher floor with stronger cybersecurity audit requirements and ultimately, protections.

Requiring a qualified, objective, and independent auditor ensures robust cybersecurity audits. EPIC and CFA commend the requirements that an auditor be qualified, objective, and independent contained in § 7122. Businesses will not be able to rely on internal auditors that may not be impartial or who may rubberstamp an audit. Instead, § 7122 requires that "[n]o finding of any cybersecurity audit may rely primarily on assertions or attestations by the business' management." The auditor must rely primarily on specific evidence they deemed appropriate.[143] This requirement will ensure accurate audits that will ultimately better protect the safety of Californians' personal information. We also support the addition to § 7050(h) which requires that service providers or contractors provide all relevant information to the business' auditor as necessary to complete the cybersecurity audit. This is a privacy-protective provision to encourage businesses to thoroughly vet their third-party affiliates and their data security practices.

Cybersecurity audits should include information about the business' data minimization program. We suggest that the Agency include a data minimization component in § 7123 as part of the scope of a cybersecurity audit in the final regulations. A cybersecurity audit should identify, assess, and document how the business' data minimization program protects personal information from unauthorized access, destruction, use, modification, and disclosure. The business should maintain a data handling program to retain personal information for only as long as is reasonably necessary to fulfill the purpose for which it was collected. The Agency can look to the Federal Trade Commission's recent consent agreement with Marriot/Starwood as an

[143] *Id.* at § 7122(d).

exemplar, which requires the companies to "maintain a policy designed to retain Personal Information for only as long as is reasonably necessary to fulfill the purpose for which the Personal Information was collected, and shall disclose the purpose for which the Personal Information is collected and the specific business need for retaining Personal Information in its terms of use or privacy policy."[144] While retention schedules are a strong step forward, data minimization is a critical further step to promote data security.[145] The Agency should require that a cybersecurity audit document a business's data minimization program because minimization is the surest way to protect consumers' personal information. A business does not need to protect personal information it never collected or that it has already deleted.

IV. Conclusion

EPIC and CFA support the Agency's efforts to operationalize (1) consumers' rights to access and to opt out of businesses' use of ADMT; (2) the requirement to conduct a risk assessment; and (3) the requirement to complete an annual cybersecurity audit. We urge the Agency to make the changes suggested throughout these comments to limit harms to consumers from ADMT. The Agency should similarly make our suggested changes to the risk assessment provisions to ensure public transparency and limit risky data processing. And the Agency should add our suggested requirements to the cybersecurity audits businesses must conduct to protect consumers and encourage strong data security practices. We thank the CPPA for the opportunity to comment on its proposed regulations and look forward to working with the Agency in the future to protect the privacy of all Californians.

[144] Agreement Containing Consent Order, *In re Marriott International and Starwood Hotels*, Fed. Trade Comm'n (Oct. 9, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/1923022marriottacco.pdf.
[145] John Davisson, *Data Minimization: A Pillar of Data Security, But More Than That Too*, EPIC (June 22, 2023), https://epic.org/data-minimization-a-pillar-of-data-security-but-more-than-that-too/.

Respectfully submitted,

/s/ John Davisson
Director of Litigation and
EPIC Senior Counsel

/s/ Sara Geoghegan
EPIC Senior Counsel

/s/ Kara Williams
EPIC Law Fellow

/s/ Mayu Tobin-Miyaji
EPIC Law Fellow

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)

/s/ Ben Winters
Director of AI and Privacy

CONSUMER FEDERATION
OF AMERICA
1620 I Street NW
Suite 200
Washington, DC 20006
202-387-6121 (tel)