CENTER FOR DEMOCRACY & TECHNOLOGY

February 19, 2025

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

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

I. Introduction

The Center for Democracy & Technology (CDT) respectfully submits these comments to the California Privacy Protection Agency (Agency) in response to the Agency's Notice of Proposed Rulemaking (NPRM) under the California Consumer Privacy Act (CCPA). CDT is a nonprofit 501(c)(3) organization that works to advance civil rights and civil liberties in the digital age. CDT's work includes advocating for strong, effective requirements for the responsible, rights-respecting use of automated systems.

We commend the Agency's work to strengthen regulatory oversight of automated decision-making technologies (ADMTs). The CCPA explicitly authorizes the Agency to issue regulations on ADMTs, which contribute to the privacy harms that the CCPA addresses. Consumers need meaningful transparency regarding the role ADMTs play in critical aspects of their lives, and protections implemented against risks of these systems. Industry should be held accountable for biased ADMTs and should already be engaging in much of the risk assessment processes required by this rule. It is therefore reasonable for California to enact a rule affirmatively requiring businesses to put robust transparency measures in place for ADMTs.

II. Definitions

A. Expand the definition of "automated decision-making technology."

The Agency has improved the meaning of "profiling" within the definition of ADMT by expanding it to include analyzing or predicting aspects concerning a person's intelligence, ability, aptitude, and predispositions. In addition, the definition of AI under the proposed regulation is similar to the Organisation for Economic Cooperation and Development's (OECD) definition,

which informs the Agency's current proposed definition.[1] Overall, OECD's definition is appropriate because the proposed regulations specify which requirements apply to AI systems used as part of ADMTs and which requirements apply to AI systems used for purposes enumerated under Sec. 7150(b)(4).

We urge the Agency to make additional improvements to the overall definition of ADMT. The proposed definition of "ADMT" only applies to technologies that process personal data to execute a decision, replace human decision-making, or substantially facilitate human decision-making. The phrase "substantially facilitate human decision-making" is further defined to mean the use of the ADMT's output as a key factor in a human's decision-making, and the illustrative example uses the term "primary factor."

Businesses are likely to interpret "key factor" and "primary factor" narrowly and conclude that their uses of ADMTs are not subject to any of the proposed requirements in most, if not all, cases. Importantly, whether a company uses an ADMT output as a "key" or "primary" factor in a decision, and thus whether these rules apply at all, would be an internal decision made by that company – the strong incentive will be not to have to comply. For instance, an employer could rely substantially on an automated personality assessment's output when making critical decisions about which employees to promote to a position that does not require the evaluated traits. However, the company could still determine the system is not an ADMT within the scope of the CCPA because the employer gives (variable) weight to other factors such as written human reviews of those employees, or might have an internal policy advising that humans should (though in practice may never actually) make the final decision.[2] In this situation, the employer could avoid the ADMT requirements, including disclosing that it is using an ADMT in the first instance. As a result, neither the workers subject to decisions made based on the system, nor the Agency, would have transparency into ADMT systems.[3]

New York City's experience is illustrative. The city has been struggling with implementing NYC LL 144, which requires transparency and bias audits only for automated systems that "substantially assist or replace discretionary decision-making" in employment decisions. According to a 2024 study, this language has limited the ability to verify whether other employers are in compliance

[1] Initial Statement of Reasons, p. 13.
[2] Testimony of Matt Scherer before California Privacy Protection Agency, Nov. 8, 2024.
[3] Comment of UC Berkeley et al to California Privacy Protection Agency, Feb. 19, 2025.

or are violating the law.[4] Out of 391 employers, researchers only found transparency notices for three percent and bias audits for five percent of employers.[5] The study observed that employers can "claim[] (correctly or incorrectly) that their decision-making process does not 'substantially' rely upon the outputs, or [use] techniques that evade the technical definition."[6] Much like the ADMT proposal here, employers in New York City have discretion over whether the definition applies to their automated systems, and disclosures are only available from the limited number of employers that admit they use systems to substantially assist or replace their decision-making.[7]

As the Agency states in the Initial Statement of Reasons, the definition of ADMTs includes systems that substantially facilitate human decision-making because it is necessary to "address harms to consumers' privacy that can result when human decision-makers significantly rely upon automated decision-making technologies in their decision-making."[8] There are better definitions already in use in California. Specifically, the California State Administrative Manual's definition of "automated decision system" is better aligned with the Agency's goal: "a computational process derived from machine learning, statistical modeling, data analytics, or artificial intelligence that issues simplified output, including a score, classification, or recommendation, that is used to assist or replace human discretionary decision-making and materially impacts natural persons."

B. Preserve the current definition of behavioral advertising.

The definition of "behavioral advertising" is scoped appropriately. It includes cross-contextual advertising, and it excludes "nonpersonalized advertising" as described in the CCPA. This definition ensures that the proposed regulations apply to all behavioral advertising that uses personal data to profile consumers in ways that violate their privacy and are not aligned with how they reasonably expect to interact with the business. Businesses would still be able to earn revenue from and promote their products and services through advertising – the definition simply prevents them from exploiting consumers' data to do so. The proposed definition would

[4] Lucas Wright et al, *Null Compliance: NYC Local Law 144 and the Challenges of Algorithm Accountability*, Proceedings of the 2024 Conference on Fairness, Accountability, and Transparency 1701 (2024), https://dl.acm.org/doi/pdf/10.1145/3630106.3658998.
[5] *Id.* at 1708.
[6] *Id.* at 1709.
[7] *Id.* at 1707.
[8] Initial Statement of Reasons, p. 14.

allow businesses to engage in contextual advertising,[9] paid search advertising, advertising to a business's own email and social media subscribers, and other forms of advertising that do not rely on collecting and analyzing a consumer's personal data.

III. Risk assessment requirements for automated decision-making

Sec. 7154 prohibits processing of personal data when risks to consumers' privacy outweighs benefits to consumers, the business, other stakeholders, and the public. The final regulations should state: "The business must not process personal information for any processing activity identified in Section 7150, subsection (b), if the risks to consumers' privacy outweigh the benefits to the consumer. Benefits to the business, other stakeholders, and the public can be included in certain circumstances, but they must significantly outweigh the risks to consumer privacy. Strong risk assessment requirements are necessary to detect when the use of an ADMT is prohibited on this basis, and to help businesses recognize when corrective measures are needed and put them in place.

A. Clarify business's obligations when they obtain ADMTs from or provide ADMTs to other parties.

Per 7152(a)(6)(B)(iii), if a business obtains an ADMT from another person, the business must identify whether it reviewed that person's evaluation of the ADMT and whether that person's assessment included requirements or limitations relevant to the business's proposed use, and it must identify any accuracy and nondiscrimination safeguards it has implemented or plans to implement. The final regulations should clarify that the business must comply with 7152(a)(6)(B)(i)-(ii) even if it obtained the ADMT from another person, and that requirements under (iii) are additional factors the business must address.

Sec. 7153 requires businesses that make ADMTs available to other parties to provide "all facts necessary" for these recipient parties to perform risk assessments, and an explanation of relevant requirements or limitations for these parties' permitted use. To ensure that businesses do indeed provide all facts necessary for recipient parties' risk assessments without misrepresentations, Sec. 7153 should advise businesses that "all facts necessary" includes, at minimum, making their own risk assessments available to the recipient parties that use their

[9] *See* Nathalie Maréchal and Nick Doty, Center for Democracy & Technology, *Defining Contextual Advertising* (2024), https://cdt.org/insights/brief-defining-contextual-advertising/.

ADMTs. Access to risk assessments of businesses that make ADMTs available would better inform the risk assessments of parties deploying the ADMTs.

B. Require further explanation of businesses' safeguards against harmful ADMTs.

Sec. 7151(b) states that stakeholder engagement may involve experts in detecting and mitigating bias in ADMT, a subset of consumers whose personal information the business seeks to process, or representatives of consumers' interests. The final regulations should advise businesses that consult with these stakeholders to explain in their risk assessments how they conducted these consultations and the feedback they received. If a business did not, or claims to have been unable to, consult with stakeholders, its risk assessment should explain why.

Sec. 7152(a)(6)(A) lists safeguards that businesses may consider to address negative impacts identified in Sec. 7152(a)(5), including an evaluation of the need for human involvement for use of ADMT and implementation of policies, procedures, and training to provide for human involvement. The final regulations should affirmatively require businesses to evaluate the need for human involvement when using ADMTs and what such human involvement would entail. For instance, businesses should evaluate whether human personnel would review the ADMT's output, have the necessary training to understand how the ADMT produced its output and when decisions should not rely on the output, to have access to all the same information as the ADMT (in addition to the output itself), and exercise authority to override the output in the decision-making process.

C. Strengthen the Agency's power to take necessary actions based on risk assessments.

To strengthen the Agency's ability to determine when a business is not complying with the CCPA when using ADMTs, the final regulations should describe the steps the Agency can take to investigate further and take enforcement actions. An additional subsection should be added to the end of Sec. 7157 stating that if the Agency has reason to conclude based on a business's risk assessment that the risks of the business's use of an ADMT do not outweigh the benefits, or finds the risk assessment insufficient to conclude that the benefits outweigh the risks, the Agency may require the business to submit the documentation or evidence necessary to evaluate the ADMT's risks and benefits. The subsection should also state that if the Agency's conclusion has not changed after reviewing the additional documentation or evidence, the Agency may hold a hearing to determine if a violation has occurred, and if so, the Agency may

issue an order restricting or prohibiting the business's use of the ADMT to address the risks it poses.[10]

IV. Rights to notice, access, opt out, and appeal

A. Strengthen requirements for pre-use and post-use notice and for businesses to respond to requests to access or appeal ADMTs.

The proposed regulations make some notable positive changes. The existing requirements and specified timeframe for businesses to respond to requests to delete, correct, know, or limit are rightfully extended to the right to access or appeal ADMTs under the proposed regulations. The transparency measures are supported by the requirement for businesses to compile metrics for the number of requests to access or to opt out of the business's ADMTs that the business received, complied with in whole or in part, and denied. The proposed regulations' exemptions from the right to opt out also correctly do not apply to using ADMTs for behavioral advertising, or to training ADMTs that are capable of being used to make significant decisions, to establish identity, or for physical or biological identification or profiling.

There are additional areas in which the rights to notice and access should be strengthened to empower consumers to understand how an ADMT may impact them and take steps to protect their rights.

Sec. 7220 should require businesses' pre-use notice to consumers to identify the risks posed by their use of their ADMTs, based on the negative impacts enumerated under Sec. 7152(a)(5). The section should also require pre-use notices to identify any available alternatives to the use of ADMTs that consumers can request instead. These disclosures will help consumers make more informed decisions as to whether to opt out. They will especially help groups at heightened risk of negative impacts, such as workers whose ability to obtain or keep a job would be affected, to pursue recourse.

Sec. 7221(j) allows consumers to use an authorized agent to submit a request to opt out of ADMTs. Similar language should be added to Sec. 7222 to clarify that consumers, including workers, have the right to use an authorized agent to request access to information about the business's use of ADMTs with respect to the consumer. Access is necessary to help consumers

[10] Comment of UC Berkeley et al to California Privacy Protection Agency, Feb. 19, 2025.

determine the harms an ADMT may have caused them, and the inability to have an authorized agent facilitate requests can be a barrier to exercising the right to access.

Under Sec. 7222(k), adverse significant decisions trigger additional notice requirements regarding access rights. Sec. 7222(k)(1) should be expanded so that adverse significant decisions include decisions affecting the terms or conditions applied to the contexts described in this provision. For instance, Sec. 7222(k)(1)(A) should include disciplinary actions and changes to work schedules or assignments, and Sec. 7222(k)(1)(B) should include pricing and interest rates and the quality of services provided. In addition, a new provision under Sec. 7222(k)(2) should affirmatively require businesses to provide consumers with the logic and reasoning behind the specific adverse decision and a user-friendly mechanism to access the range of possible outputs and aggregate output statistics. This will also help groups who are at heightened risk of negative impacts from the use of an ADMT to understand how their outcomes resulting from an ADMT compare to other consumers' outcomes.

B. Provide more specific parameters for the security exception to the right to limit the use and disclosure of sensitive personal information.

Sec. 7027(m) provides examples of the exceptions to the consumer's right to limit, including to detect or prevent security incidents or malicious or illegal actions. The proposed regulations add Sec. 7027(m)(2)(B), which states that businesses may scan employees' outgoing emails to prevent leaking of sensitive personal information, but not for other purposes. Sec. 7027(m)(3)(B) states that businesses may collect and use employees' biometric information to authenticate access for authorized people to secure areas of the workplace, but may not retain this information indefinitely or use it for unrelated purposes. Only the latter example, Sec. 7027(m)(3)(B), specifies that the collected information cannot be reused for other purposes. To make sure that businesses understand the limits of Sec. 7027(m)(2)(B), the final regulations should clarify that in both examples, collected information cannot be reused for other purposes.

V. Conclusion

We commend the Agency for advancing this rulemaking proceeding, and for the Agency's efforts to improve businesses' transparency and risk mitigation when using ADMTs. We urge the Agency to make sure the final regulations are properly scoped to equip consumers to exercise their rights and to prevent businesses from circumventing the CCPA's protections.