Statement on behalf of the Center for Democracy & Technology
Before the California Privacy Protection Agency
Pre-rulemaking Stakeholder Session on Automated Decision-making

May 4th, 2022

By Ridhi Shetty
Policy Counsel, Privacy & Data Project

Thank you for the opportunity to speak before the California Privacy Protection Agency today. My name is Ridhi Shetty and I am a Policy Counsel at the Center for Democracy & Technology (CDT). CDT is a nonprofit, nonpartisan 501(c)(3) organization based in D.C. that advocates for civil rights and civil liberties in the digital world. CDT works on many areas involving impacts of data practices in the public and private sector, including privacy risks and inequities resulting from data-driven or algorithmic decision-making.

The California Privacy Rights Act (CPRA) requires the Agency to issue regulations "governing access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling," and requiring businesses to respond to a consumer's access requests by providing "meaningful information" about the logic involved in these systems and the likely outcomes these systems will have for that consumer.[1] To this end, we call on the Agency to ensure that the CPRA regulations address four points.

First, the CPRA regulations should explicitly articulate what *automated decision-making* encompasses, in terms of both the system itself and the context in which it is used. The CPRA defines "profiling," a related term, as the automated processing of a person's personal information "to analyze or predict aspects concerning [their] performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements."[2] The regulations should build on this definition by clarifying that there are two key aspects of the "automated decision-making technology" that are subject to regulation. One aspect is the design, training data, logic, inputs, and outputs of the methodologies involved in the automated decision-making system, with a particular eye toward biases in those methodologies.[3] For

[1] Cal. Civ. Code §1798.185(16).
[2] Cal. Civ. Code §1798.140(z).
[3] *See* Hannah Quay-De La Vallee and Natasha Duarte, Ctr. for Democracy & Tech., Algorithmic Systems in Education: Incorporating Equity and Fairness When Using Student Data 6-8 (2019), https://cdt.org/wp-content/uploads/2019/08/2019-08-08-Digital-Decision-making-Brief-FINAL.pdf [Hereinafter "Algorithmic Systems in Education"].

1401 K Street NW, Suite 200 Washington, DC 20005

example, when racial, gender-based, and/or ableist biases are embedded in an automated decision-making system's training data, the system can reproduce long-standing inequities *at scale* and cause extensive harm to underrepresented and marginalized populations.

The other aspect is the overall context in which the automated decision-making system is deployed, including the system's purpose and the ramifications of using a flawed system for that purpose, explainability of the system's design and function, and the manner and extent to which humans rely on the system's output to render any particular final outcome related to a person.[4] Despite arguments that automated decision-making systems are less biased than human decision-making, automated systems are far more limited in their ability to examine context and make nuanced decisions based on individual circumstances. Therefore, how and why the systems are deployed are just as important as the systems' design, logic, and inputs and outputs.

Second, the CPRA regulations should elaborate on substantive notice requirements so that consumers are empowered to hold automated decision-making systems and the businesses that deploy them accountable. Under the CPRA, notice to consumers must be easy for average consumers to understand, and must be available in accessible formats for disabled consumers and in languages primarily used to interact with consumers.[5] The CPRA regulations should further address the substance of these notices and elaborate on the explanation that consumers must receive about how their personal data is processed to produce a decision. Specifically, *before* subjecting consumers to an automated decision-making process, businesses should provide consumers with meaningful information about the logic involved in the process and its potential outcomes, and their right to opt out of automated decision-making. *After* using such systems, businesses also should provide consumers with the principal reasons for any adverse decisions, data or factors used to render such decisions, and how the systems generated their outputs.[6]

Third, the Agency's rulemaking should pay particular attention to the impacts of discriminatory systems affecting critical areas of opportunity. Automated decision-making systems are playing a growing role influencing hiring, compensation, promotion, and

[4] *Id.*
[5] Cal. Civ. Code §1798.185(6).
[6] Ctr. for Democracy & Tech., Comments on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning 5-6 (Jul. 1, 2021), https://cdt.org/wp-content/uploads/2021/07/2021-07-01-CDT-Request-for-Information-and-Comment-on-Financial-Institutions-Use-of-Artificial-Intelligence-including-Machine-Learning.pdf.

termination decisions in the workplace and labor market;[7] limiting housing and credit eligibility;[8] designating academic tracks, school intervention programs, and disciplinary actions;[9] and determining eligibility, budget allocations, and potential fraud in public benefits.[10] Across these sectors, these systems are often trained to recreate ongoing decision-making patterns by evaluating a person against data from groups and subgroups that have benefited from historical discrimination. Even when those systems attempt to control for that bias, seemingly neutral data can function as proxies that lead to discriminatory impacts.[11] All of this makes it considerably more difficult for historically marginalized groups to access critical life opportunities.

Yet, the CPRA and the Agency's invitation last fall for preliminary comments on proposed rulemaking under the CPRA did not mention discriminatory harms of data practices. The regulations should address discriminatory outcomes explicitly because, despite antidiscrimination protections, these systems have been used in ways that run afoul of civil rights and consumer protection laws with relative impunity. This is in large part due to the black box nature of automated decision-making.[12] One way to open the black box is through audit requirements. The CPRA regulations should specify covered entities' audit obligations, particularly frequency and substance of audits, and make clear the Agency intends to gather information and investigate equity impacts of automated decision-making systems.

---

[7] Matt O'Brien, *NYC Aims to Be First to Rein in AI Hiring Tools*, AP News (Nov. 19, 2021), https://apnews.com/article/technology-business-race-and-ethnicity-racial-injustice-artificial-intelligence-2fe8d3ef7008d299d9d810f0c0f7905d; Matthew Scherer and Aiha Nguyen, *Employment Law Still Has Roots in the Middle Ages. That's Terrible for Workers.*, Wash. Post (Mar. 17, 2022, 1:10 PM), https://www.washingtonpost.com/outlook/2022/03/17/labor-law-middle-ages-wisconsin/.

[8] Emmanuel Martinez and Lauren Kirchner, *The Secret Bias Hidden in Mortgage-Approval Algorithms*, The Markup (Aug. 25, 2021, 6:50 AM), https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.

[9] Algorithmic Systems in Education, *supra* note 3, at 9-14.

[10] Erin McCormick, *What Happened When a 'Wildly Irrational' Algorithm Made Crucial Healthcare Decisions*, The Guardian (Jul. 2, 2021, 12:30 PM), https://www.theguardian.com/us-news/2021/jul/02/algorithm-crucial-healthcare-decisions; Hannah Quay-de la Vallee, *Combatting Identify Fraud in Government Benefits Programs: Government Agencies Tackling Identity Fraud Should Look to Cybersecurity Methods, Avoid AI-Driven Approaches that Can Penalize Real Applicants*, Ctr. for Democracy & Tech. (Jan. 7, 2022), https://cdt.org/insights/combatting-identify-fraud-in-government-benefits-programs-government-agencies-tackling-identity-fraud-should-look-to-cybersecurity-methods-avoid-ai-driven-approaches-that-can-penalize-real-applicant/.

[11] *See e.g.,* Relman Colfax Pllc, Fair Lending Monitorship of Upstart Network's Lending Model 8, 22-23 (2021), https://www.relmanlaw.com/media/cases/1088_Upstart%20Initial%20Report%20-%20Final.pdf.

[12] *See generally* Solon Barocas et al., Designing Disaggregated Evaluations of AI Systems: Choices, Considerations, and Tradeoffs, Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society (2021), https://arxiv.org/pdf/2103.06076.pdf.

Fourth, the CPRA regulations should preserve the existing exceptions under the California Consumer Privacy Act (CCPA) for governmental service providers. The definition of "business" under the CPRA is insufficiently specific to address the issue of businesses that provide services for public entities. Those businesses may be subject to the CPRA's rights regarding access, disclosure, correction, and deletion, but requiring them to meet the CPRA's requirements may conflict with existing state and federal requirements for public entities regarding privacy, security, and public records.[13] Section 999.314(a) of the CCPA regulations rightfully classifies businesses that provide services to public entities as "service providers" and requires them to collect, use, and delete data only as directed by the government entity for whom they provide services.[14] This delineation of the duties of service providers is especially crucial for public schools, because compliance with the CPRA's requirements for access, correction, or deletion could cause unintended disruption to school services and student learning.[15] In a similar vein, improperly scoped compliance requirements for businesses that provide services for agencies to administer government benefits may also delay or bar access to public benefits for those in greatest need. The exception for these businesses under the CCPA regulations helps avoid conflict with federal and state laws that could result from obligating service providers to disclose or compromise public data that the public entity is responsible for keeping secure.

I appreciate the Agency's attention to these concerns and the Agency's efforts to strengthen California's regulatory framework with respect to automated decision-making. I look forward to working with the agency and I am happy to provide further resources expanding on these concerns. Thank you.

[13] Cal. Attorney Gen., Final Statement of Reasons 30 (2020), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor.pdf.
[14] Cal. Code Regs. tit. 11, § 999.314(a).
[15] Cal. Attorney Gen., Final Statement of Reasons, *supra* note 13, at 30.