February 19th, 2025

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

Re: Public Comment on CCPA regarding ADMT

The Center for Data Innovation (datainnovation.org) appreciates the opportunity to provide comments on the California Privacy Protection Agency's proposed regulations on automated decision-making technology.

The Center for Data Innovation studies the intersection of data, technology, and public policy, and formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as open data, artificial intelligence, and the Internet of Things. The Center is part of the Information Technology and Innovation Foundation (ITIF), a nonprofit, nonpartisan think tank.

INTRODUCTION

The California Consumer Privacy Act (CCPA), enacted in 2018 and effective since 2020, is the most sweeping state data privacy law in the United States. It grants California residents specific rights over their personal data, including the ability to access, delete, and opt out of certain uses of their information. To ensure these rights, the law imposes obligations on for-profit businesses that either have annual gross revenues exceeding $25 million; buy, sell, or share the personal data of more than 50,000 California residents, households, or devices; or derive at least 50 percent of their annual revenue from selling personal data.

In 2020, voters approved the California Privacy Rights Act (CPRA), which amended and expanded the CCPA. The CPRA established the California Privacy Protection Agency (CPPA) to oversee enforcement and introduced additional consumer rights, such as the ability to correct personal data and opt out of automated decision-making. It also gave the CPPA the authority to develop regulations on automated decision-making technology (ADMT), including rules on transparency and opt-out rights.

The CPPA has now proposed regulations that would impose new requirements on businesses using ADMT in ways that significantly impact consumers. The rules define ADMT broadly, covering any technology that processes personal data to execute, replace, or substantially facilitate human

decision-making. The proposed changes include three key provisions. First, businesses must provide consumers with pre-use notices detailing how ADMT is used, including its purpose and key parameters. Second, consumers must be given the right to opt-out of most uses of ADMT, including profiling and automated decisions affecting access to jobs, education, healthcare, and financial services. Third, businesses must respond to consumer requests for information on how ADMT was used in decisions that affect them, explaining the system's role and output. Additionally, the CPPA is developing risk assessment rules that would require businesses to evaluate ADMT systems for accuracy, bias, and potential harms before deployment.

The CPPA's proposal oversteps its authority, transforming an already overbearing data privacy law into excessive AI regulation. It requires businesses to conduct risk assessments, provide detailed disclosures, and offer broad opt-out rights, effectively regulating AI development and use. The overbroad definition of ADMT captures low-risk tools, creating costly compliance burdens with little consumer benefit. The requirement that businesses become immediately responsible for the new rules after CPPA publishes them gives businesses no time to adapt, forcing rushed compliance or abandonment of ADMT. Moreover, by acting unilaterally, California is adding to regulatory fragmentation at the state level and complicating efforts to establish a coherent national AI governance framework.

1. THE PROPOSAL DISTORTS CCPA INTO A DE FACTO AI LAW

The CPPA's proposed regulations exceed its mandate by imposing AI governance measures rather than focusing solely on data privacy protections. In addition to providing opt-out and access rights for consumer data, the proposal would require businesses to comply with AI-specific rules that extend far beyond what is necessary for privacy oversight.

- **Mandatory Risk Assessments:** Businesses would be forced to conduct in-depth AI risk assessments of their ADMT systems. Rather than simply informing consumers about automated decision-making, § 7152 would require companies to evaluate data accuracy, identify potential biases, and document risks beyond consumer privacy. This transforms a privacy law into an AI governance framework and goes far beyond the original legislative text.
- **Detailed Transparency Requirements:** § 7220, subsection (c)(5) would require that businesses disclose the internal logic of their ADMT systems, including key parameters and intended outputs. Instead of just notifying consumers that an automated system is in use, companies would have to provide technical details about how the system operates which could reveal proprietary business information that could give advantages to competitors and help bad actors to manipulate or exploit these systems.
- **Misapplied consumer protections:** Under § 7151(c), businesses would have to provide disclosures and offer opt-out rights not only when ADMT systems use consumer data in

decision-making, such as loan approvals or hiring where there is a clear risk of direct informational injury, but also when businesses use consumer data for broader internal purposes, such as training AI models, refining decision-making processes, or generating insights about potential customers. While personal data used in decision-making processes may create a clear risk to individuals, using personal data for internal processes does not automatically translate into direct harm. By forcing businesses to apply strict opt-out and disclosure requirements to all uses of consumer data, even when there is no direct impact on individuals, the proposal goes beyond what privacy regulations were originally meant to do—which is to prevent consumer harm. Instead, it turns into an AI governance measure, regulating how businesses develop and improve their systems.

The CPPA's authority under the CCPA and CPRA was meant to protect consumer privacy by giving individuals control over their data. But the proposed regulations go beyond privacy, effectively dictating how businesses design and operate AI systems. This is a major expansion of regulatory power that should be decided by the legislature (or voters), not imposed through agency rulemaking. AI regulation impacts more than privacy, it affects innovation, economic competitiveness, and governance. These trade-offs require legislative debate and public accountability. If Californian policymakers want to regulate AI, they should do so through a transparent legislative process, not privacy rulemaking repurposed for a broader agenda.

2. THE PROPOSAL UNDERMINES EFFORTS FOR A COHERENT NATIONAL AI GOVERNANCE APPROACH

Beyond the legal overreach, the CPPA's proposal risks creating a fragmented and inconsistent AI regulatory landscape. Indeed, this move directly undermines sensible efforts emerging at the national level, such as the bipartisan effort in Congress to establish a unified national AI governance strategy. In December 2024, the House AI Task Force presented a framework urging clear identification of AI risks, reliance on domain-specific regulators, and federal preemption to avoid a patchwork of state laws.[1] Rather than coordinating with this push for coherent national governance, the CPPA's proposal introduces another layer of regulation, making it more difficult for Congress and the administration to forge a single, innovation-friendly framework.

For businesses, CCPA's proposal creates compliance uncertainty and higher operational costs. Companies operating across multiple jurisdictions will be forced to navigate overlapping and potentially contradictory obligations, creating regulatory inefficiencies and discouraging innovation.

[1] House Bipartisan AI Task Force, *Bipartisan House Task Force on Artificial Intelligence*, December 2024, https://www.speaker.gov/wp-content/uploads/2024/12/AI-Task-Force-Report-FINAL.pdf.

Moreover, industry best practices, including those established by leading AI developers, prioritize adaptive, iterative risk management rather than rigid preemptive assessments. By mandating detailed disclosures of AI model logic and extensive pre-use risk assessments, the CPPA's proposal risks exposing proprietary AI systems to unnecessary scrutiny while failing to account for the evolving nature of AI risks and mitigations.

3. THE PROPOSAL'S OVERBROAD ADMT DEFINITION FORCES COSTLY COMPLIANCE WITH NO CONSUMER BENEFIT FOR LOW-RISK TOOLS

Even for purely privacy-related aspects of automated tools, the CPPA's draft regulations define ADMT so broadly that they sweep in routine or low-risk tools that pose minimal threats to personal data. The proposal defines ADMT as "any technology that processes personal information and uses computation to execute a decision, replace human decision-making, or substantially facilitate human decision-making." Although the regulations exclude certain routine technologies such as spreadsheets, the broad wording still risks ensnaring many low-risk tools like basic analytics dashboards or simple scoring algorithms.

For instance, consider a manager using a spreadsheet to rank employees based on peer evaluations. If the manager manually enters scores and sorts them, this is not ADMT. But if the spreadsheet automatically calculates an average score, the CPPA could argue that it "substantially facilitates" decision-making and impose compliance obligations. Businesses would then be required to conduct risk assessments, provide technical disclosures, and implement opt-out mechanisms for a tool that simply performs basic arithmetic. This overreach burdens businesses with unnecessary compliance costs without delivering meaningful privacy benefits.

Research from ITIF shows that such over-inclusive privacy regulations can impose substantial economic burdens. In its 2022 report, "The Looming Cost of a Patchwork of State Privacy Laws," ITIF estimated that state-level privacy laws with expansive definitions could saddle U.S. businesses with out-of-state compliance costs exceeding $1 trillion over 10 years.[2] This burden falls disproportionately on small and mid-sized companies, which lack the resources to navigate a complex regulatory environment originally designed for high-stakes data processing, not everyday office software.

The CPPA's own analysis reinforces these concerns. According to the agency's Standardized Regulatory Impact Assessment (SRIA), the full regulatory package—including but not limited to ADMT provisions—would impose $3.5 billion in direct compliance costs on California businesses in the first

[2] Daniel Castro, Luke Dascoli and Gillian Diebold, "The Looming Cost of a Patchwork of State Privacy Laws," (ITIF, January 2022), https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws.

year alone, with an additional $1.08 billion in direct costs over the first decade.[3] The economic consequences extend far beyond compliance expenses: the SRIA projects a staggering $31 billion decline in investment in the state and a loss of 98,000 jobs.[4]

By treating all automated processes as equally risky, the CPPA's proposal would force organizations to deploy the same detailed privacy assessments and disclosures for trivial data operations as they would for genuinely consequential AI systems (e.g., mortgage approvals). That one-size-fits-all approach inflates compliance costs, yields little net gain for consumers, and ultimately undermines the law's effectiveness by diverting attention from truly high-risk scenarios.

4. UNREASONABLE COMPLIANCE TIMELINES WILL FORCE BUSINESSES TO EITHER RUSH IMPLEMENTATION OR ABANDON ADM SYSTEMS

The CPPA's draft regulations are set to take effect immediately upon finalization, which could be as early as mid-2025, giving businesses no reasonable adjustment period. Unlike other regulatory frameworks that phase-in compliance over months or years, these rules would require businesses to implement sweeping changes right away, including risk assessments, opt-out mechanisms, and detailed disclosures. The risks of non-compliance are significant. The CPPA has broad enforcement authority, allowing it to issue civil penalties of up to $7,500 per violation. Each individual instance of non-compliance could be counted as a separate violation, meaning that a single misstep, such as failing to provide a required explanation for an automated decision, could lead to massive financial penalties, particularly for businesses with high-volume consumer interactions.

These regulations would put many businesses in an impossible position. With little time to properly develop compliant systems, companies will be forced to either rush implementation, increasing the risk of errors and unintended consequences, or abandon certain ADMT tools entirely, even when these tools provide real benefits. This would be a loss for both businesses and consumers. While much of the public discourse around ADMT has focused on risks, these tools offer significant benefits, particularly for individuals who have historically faced limited opportunities. Algorithms can improve equity in decisions about allocating scarce resources in healthcare settings and expanding access to educational opportunities. They can also replace biased human decision-making in tasks like home appraisals, ensuring more objective and fair outcomes.[5]

---

[3] Berkeley Economic Advising and Research, "Standardized Regulatory Impact Assessment: California Privacy Protection Agency," prepared for the California State Privacy Protection Agency, August 2024, https://cppa.ca.gov/meetings/materials/20241004_item6_standardized_regulatory_impact_assessment.
[4] Ibid.
[5] 8 Debra Kamin, "Home Appraised With a Black Owner: $472,000. With a White Owner: $750,000," The New York Times, August 25, 2022, https://www.nytimes.com/2022/08/18/realestate/housing-discrimination-maryland.html

By imposing an immediate and punitive compliance regime, the CPPA's approach risks discouraging the responsible adoption of ADMT, ultimately harming consumers and undermining the very protections the law was meant to provide.

Yours sincerely,

Hodan Omaar
Senior Policy Manager
ITIF's Center for Data Innovation
homaar@datainnovation.org