Comments of the Software & Information Industry Association

California Privacy Protection Agency
Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies

February 19th, 2025

The Software & Information Industry Association (SIIA) appreciates the opportunity to provide comments on the California Privacy Protection Agency's (CPPA's) draft regulations. SIIA is the principal trade association for those in the business of information, including its aggregation, dissemination, and productive use. Our members include roughly 380 companies reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used worldwide, and companies specializing in data analytics and information services.

SIIA supports privacy as a fundamental value, and one essential to individual autonomy and a functioning democracy. Data privacy standards that harmonize meaningful consumer safeguards with appropriate business compliance will ensure smooth implementation of data privacy practices. We have previously provided stakeholder input on the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), since these laws set an important milestone for companies engaging in interstate commerce both within and outside of California.

We appreciate the goals of the regulations and the Agency's attention to concerns we have previously articulated regarding the efficacy and potential unintended consequences of overly prescriptive requirements. In this submission, we focus on provisions in the draft regulations that are likely to have further unintended consequences, including undermining protections for consumers and burdening companies attempting to operate in good faith – without, on balance, providing meaningfully stronger guardrails around consumer data. When possible, we provide specific recommendations intended to better align the proposed regulations with the letter and spirit of the statute.

Definitions

1. **The definition of ADMT requires greater clarity.**

Further clarifying the definition of ADMT would greatly reduce chilling effects, consumer confusion, and compliance costs associated with using innovative technologies in California.

We recommend that California align this definition with existing privacy laws, scoping ADMT to solely automated processing that makes, rather than merely facilitates, human decisionmaking. The phrases "substantially facilitate" and "key factor" remain vague and differ from the approach taken by U.S. state privacy laws and even Europe's General Data Protection Regulation (GDPR).

We also suggest that the Agency provide clarity on the scope of ADMT by identifying situations in which the definition will *not* apply. Providing such clarity will help prevent uncertainty in scenarios California businesses and their compliance teams are likely to frequently encounter. Our specific proposed carveouts to § 7001(f) chiefly address the challenge of delineating between automated tools that render a decision – which fall within the definition of ADMT – and automated tools that perform a task, but do not render a "decision," and are thus outside the scope of ADMT.

Recommendation: § 7001(f). "Automated decisionmaking technology" means any solely automated technology that processes personal information and uses computation for the primary purpose of making a solely automated significant decision about a consumer.~~to execute a decision, replace human decisionmaking, or substantially facilitate human decision making. (1) For purposes of this definition, "technology" includes software or programs, including those derived from machine learning, statistics, other data-processing techniques, or artificial intelligence. (2) For purposes of this definition, to "substantially facilitate human decisionmaking" means using the output of the technology as a key factor in a human's decisionmaking. This includes, for example, using automated decisionmaking technology to generate a score about a consumer that the human reviewer uses as a primary factor to make a significant decision about them. (3) Automated decisionmaking technology includes profiling.~~

Recommendation: § 7001(f)(5). An ADMT does not "substantially facilitate human decisionmaking" when it:

(i) performs a narrow procedural task;

(ii) improves the result of a previously completed human activity;

(iii) detects decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment without proper human review; or
(iv) performs a preparatory task to an assessment relevant to a significant decision.

2. **The proposed AI definition exists outside the scope of the CCPA, conflicting with existing California law and leaving the Agency's final regulations open to legal challenges.**

Despite the Agency's authority under the CCPA to regulate ADMT, we believe whole cloth inclusion of *AI* is so overly broad as to encompass nearly all software, and thus operate well beyond the scope of what was intended and authorized by the CCPA. AI is significantly broader than ADMT. Notably, the CCPA does not mention AI, as it was not intended to govern AI development and use, nor to create consumer rights regarding AI.

One way in which the proposed regulations go beyond the scope of what can be reasonably implied by the CCPA itself is the conflation of different roles in the AI value chain. The proposed definition of AI does not distinguish between the unique roles of AI developers and AI deployers. This creates a blunt category that lumps together technologies as disparate as generative AI and frontier models. Further, the definition actually conflicts with other California AI frameworks, such as those recently enacted to govern generative AI transparency.[1] The CCPA was simply never intended for this purpose.

Without removing this definition of AI, the Agency will therefore, as a practical matter, likely encounter legal challenges pertaining to its scope. In addition to operating outside the intended scope of the CCPA, this would only serve to unnecessarily complicate the implementation of the proposed regulations of ADMT that do fall within its remit.

Recommendation: § 7001(c). ~~"Artificial intelligence" means a machine-based system that infers, from the input it receives, how to generate outputs that can influence physical or virtual environments. The artificial intelligence may do this to achieve explicit or implicit objectives. Outputs can include predictions, content, recommendations, or decisions. Different artificial intelligence varies in its levels of autonomy and adaptiveness after deployment. For example, artificial intelligence includes generative models, such as large language models, that can learn from inputs and create new outputs, such as text, images, audio, or video; and facial- or speech-recognition or -detection technology.~~

[1] *See* SB-942 California AI Transparency Act.

3. **Publicly accessible places should be scoped appropriately to physical places, and public profiling should cover data that is inherently sensitive or potentially harmful to consumers.**

The proposed regulations' definition of "publicly accessible place," "public profiling" and "systematic observation" are overbroad and poorly scoped to the CCPA's approach to publicly available information (PAI).

First, we recommend that the Agency clarify that the definition of "publicly accessible place" applies only to physical spaces and not to online spaces. Absent this clarification, the definition conflicts with the exemption for PAI under the CCPA. Much of the data collected online "through systemic observation of a publicly accessible place" constitutes garden variety PAI. The proposed regulation would then collide with the text and intent of the CCPA by including the collection of PAI under the CCPA within the definition of "extensive profiling."

The CCPA explicitly exempts "publicly available information," defined as information made available from the consumer to the general public or from widely distributed media, or if the consumer has not restricted the information to a specific audience.[2] This decision was made very deliberately during drafting to avoid clear-cut constitutional infirmities that would otherwise run afoul of the First Amendment.[3]

In addition, we recommend that the regulations focus the concept of "public profiling" to avoid restricting the collection and dissemination of PAI that is neither sensitive in nature nor presents a significant risk of harm to consumers. The draft regulations create a concept of "public profiling" even when it does not result in legal or similarly significant effects concerning consumers. It then combines this with a definition of "publicly accessible place" that eschews locations most likely to yield sensitive data and references instead stores, restaurants, and amusement parks, among others. The draft lastly includes a broad definition of "systematic observation" that would wrap in even services consumers use to monitor their own movements, such as location trackers.

We strongly urge the Agency to revise these definitions to remain within its remit and avoid wrapping in publicly available information, better scope information collected in publicly accessible places to genuinely sensitive data, and prevent burdensome intrusions on consumer experiences for services where these consumers have already opted in.

---

[2] *See* Cal. Civ. Code § 1798.100 et seq.

[3] *See Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011).

Recommendation: § 7001(ll). "Publicly accessible place" means a physical place that is open to or serves the public. Examples of publicly accessible places include hospitals, medical clinics or offices, airports, public wi-fi hotspots, workplaces, and government buildings.~~shopping malls, stores, restaurants, cafes, movie theaters, amusement parks, convention centers, stadiums, gymnasiums, hospitals, medical clinics or offices, transportation depots, transit, streets, or parks.~~

Recommendation: § 7150(B)(ii). Profiling a consumer through systematic observation of a publicly accessible place that results in legal or similarly significant effects concerning that consumer ("public profiling"); or

Recommendation: § 7001(eee). "Systematic observation" means methodical and regular or continuous observation. This includes, for example, methodical and regular or continuous observation using Wi-Fi or Bluetooth tracking, radio frequency identification, drones, video or audio recording or live-streaming, technologies that enable physical or biological identification or profiling; and geofencing, location trackers, or license-plate recognition. "Systematic observation" does not include services consumers choose to use to monitor their own movements, such as location trackers.

Substantive Provisions

4. **Restricting first-party behavioral advertising conflicts with the text and intent of the CCPA.**

We recommend that the Agency avoid requiring both risk assessments and a consumer opt-out whenever a California business advertises to its own customers using first-party behavioral advertising. This proposal conflicts directly with the CCPA and would have severe unintended consequences.

Behavioral advertising is based on data collected by a business from its own customers, and is used to enhance their experiences in the future. For example, a California resident may purchase dishwasher detergent at regular intervals in an online marketplace. Today, the marketplace could suggest, such as via email or SMS text, that the customer may need to order again. This type of feature is designed to provide value to consumers and does not result in the sharing of consumer data with any third parties beyond the business that already possesses it. This practice therefore does not further proliferate a consumer's information in a privacy-invasive manner, nor produce legal or similarly significant effects.

Furthermore, requiring risk assessments and opt-outs for first-party behavioral advertising is directly in conflict with the CCPA, which does not impose these burdens on first party ads. The CCPA, along with other privacy laws like the Colorado Privacy Act, imposes requirements on targeted, *cross-contextual* behavioral advertising – but, critically, not first-party behavioral ads.[4] When the CCPA was drafted, California legislators specifically decided to permit California businesses to productively use data from their own customers to improve their products and to advertise to them, without the threat of a lawsuit. An opt-out requirement for first-party advertising effectively undercuts that decision. In fact, no other state privacy regime compels an opt-out for basic first-party advertising, nor do they compel risk assessments for this type of advertising.

The consumer right to opt out of ADMT used for behavioral advertising would also create serious unintended consequences. These types of ads are integral to a business's ability to advertise to its own customers. Forcing California businesses to opt out their own customers would force a whole cloth redesign of online marketplaces to provide opted-out customers with their "own version" of popular online platforms.

Finally, applying these requirements to first party behavioral advertising raises serious First Amendment issues. The requirements compel subjective and editorial speech about an entity's own advertising activities, and place a burden on their protected commercial speech. Established First Amendment jurisprudence is hostile to requiring businesses to comply with requirements for an activity that amounts to no more than selecting an audience for a specific advertisement. These ads are inherently expressive and associational – not "decisions" within the definition of ADMT.

In fact, the inclusion of "behavioral advertising" in the draft regulations likely exceeds the Agency's authority whole cloth, because it is not reasonably necessary to effectuate the purpose of the statute, and in fact conflicts with its clear intent. The CCPA lists many areas in which the Agency should promulgate regulations, but the scope of "advertising" to be regulated is not among them.[5] In fact, the statute expressly excludes from regulation personal information provided in connection with "services with which the consumer intentionally interacts."[6]

---

[4] *See* C.R.S. § 6-1-1303(6).

[5] See Cal. Civ. Code § 1798.185 (listing the areas in which the CPPA is directed to promulgate regulations and not including "advertising").

[6] *Id.* at § 1798.140(k) (defining cross-context behavioral advertising).

We recommend that the Agency remove the reference to "behavioral advertising," which would cause confusion alongside the CCPA's reference to cross-contextual behavioral advertising. The CPPA should also strike the behavioral advertising obligations present in the proposed regulations. At the very least, they should be replaced with a targeted advertising opt-out requirement that is aligned with the existing approach in the CCPA and other U.S. state omnibus privacy laws.

Recommendation: § 7001(g). ~~"Behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity—both across businesses, distinctly-branded websites, applications, or services, and within the business's own distinctly-branded websites, applications, or services.~~

Recommendation: § 7150(b)(3)(B). For purposes of this Article, "extensive profiling" means:

(i) Profiling a consumer through systematic observation when they are acting in their capacity as an applicant to an educational program, job applicant, student, employee, or independent contractor ("work or educational profiling"); or

(ii) Profiling a consumer through systematic observation of a publicly accessible place ("public profiling")~~; or~~

~~(iii) Profiling a consumer for behavioral advertising~~.

Recommendation: § 7200(A)(2). For extensive profiling of a consumer. For purposes of this Article, "extensive profiling" means:

(A) Profiling a consumer through systematic observation when they are acting in their capacity as an applicant to an educational program, job applicant, student, employee, or independent contractor ("work or educational profiling"); or

(B) Profiling a consumer through systematic observation of a publicly accessible place ("public profiling")~~; or~~

~~(C) Profiling a consumer for behavioral advertising~~.

5. **Imposing a pre-use notice requirement, access right, and opt-out right for such a broad category of ADMT and training data will have unintended consequences that hurt consumers.**

The pre-use notice requirement, access right, and opt-out right for ADMT training data is well intentioned, but overbroad and in places ill conceived. We are concerned that these would paradoxically harm smaller developers and consumers alike by hamstringing their ability to maintain representative data sets and prevent discriminatory outcomes.

First, the Agency does not propose to limit ADMT-related obligations to those tools that produce legal or similarly significant effects. Decisions that have no such effects should not be subject to expansive regulations. Wrapping in even technology "capable" of being used for certain purposes would affect basic AI tools like chatbots, analytics technology, and even automated spreadsheets, which are almost always "capable" of affecting consumers in significant ways even if this is not their intended use.

Furthermore, ADMT "training" encompasses a broad swath of activities. This could be adjusting the parameters of an algorithm used for ADMT or artificial intelligence, improving the algorithm that determines how a machine-learning model learns, or iterating the datasets fed into ADMT or artificial intelligence. The ability of ADMT to deliver faster, fairer and more inclusive outcomes to consumers depends on developers' ability to alter algorithms to incorporate both new information and wider datasets representative of all consumers. Restricting developers from tweaking algorithms at scale would be incredibly burdensome. It would have a disproportionate impact on smaller California firms, and also, inevitably, harm consumers' use of and experience with AI tools.

The text of the draft regulations compounds this overbreadth problem by compelling a pre-use notice, an access right and an opt-out right in multiple ways that are at odds with best practices in consumer protection. For example, U.S. state privacy regimes have repeatedly rejected in-your-face notices even for far more privacy-invasive practices – such as selling sensitive information – out of concern over consumer notice fatigue. It is also virtually impossible to provide access rights to ADMT training data on an individual level, particularly in "plain language" as mandated by the draft regulations. Lastly, imposing a backward-facing opt-out is not workable in cases where data is previously integrated into a technology in a manner that does not permit reidentification, such as where data is integrated into a model. This is because it would be prohibitively costly to delete and rebuild a model each time deletion is requested. Like the provisions around actual *sales* of data, we believe this provision should be solely forward-looking.

The opt-out right would also restrict California businesses when developing their own productive ADMT applications internally by working off larger models from tech companies. In addition to reducing innovation in the state, it would complicate and perhaps render impossible efforts on the part of ADMT developers to combat discriminatory outcomes resulting from automated tools. The opt-outs would inevitably result in unrepresentative data sets, and this skew would adversely impact those who are subject to automated decisions simply due to representative bias. Unfortunately, biased outcomes under such a regime are all-but inevitable.

This is even the case where the consumers who are themselves subject to automated decisions do *not* opt out.

Further, the draft regulations fail to acknowledge that in practice, much of AI training involves "publicly available information" that would be PAI under the statute. However, this PAI does not constitute personal data under the CCPA. Even from a purely privacy-protective standpoint, training data sets in practice typically include nothing more than a *de minimis* amount of personal data. Yet requiring implementation of an opt-out process conversely runs counter to best practices in data minimization. In fact, it may even require individual identification – a practice wholly counterproductive to privacy and the intent behind the proposed ADMT regulations.

Finally, these obligations are likely beyond the scope of the statute itself. Imposing heightened obligations on the processing of personal information to train ADMT is not reasonably necessary to effectuate the purpose of the underlying statute, creating potential legal challenges in the future. ADMT *training* does not involve decisions that concern a specific consumer. It therefore is not automated "decisionmaking," which is what the statute addresses. The scope of the CPPA's rulemaking authority is limited to "access and opt-out rights" with respect to "automated decision-making."[7] It is the right to access, correct, or delete consumer data that provides consumers with mechanisms to acquire information about, or avoid, the processing of their personal information to train ADMT models.

Moreover, the content requirements within the pre-use notice requirement around the "intended output" and "how the business plans to use the output" again attempt to regulate expressive content and compel protected speech on the part of California businesses to explain their intent and judgments about their processes. The California legislature likely recognized this infirmity, which is why it limited the rulemaking provision regarding "notice" to rules related to *how* notice is provided and not *what* notices should contain.[8]

Recommendation: § 7150(b). ~~4) Processing the personal information of consumers to train automated decisionmaking technology or artificial intelligence that is capable of being used for any of the following:~~

~~(A) For a significant decision concerning a consumer;~~

[7] Cal. Civ. Code § 1798.185(a)(16).

[8] § 1798.185(6) directs the CPPA to "[e]stablish[] rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumers, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer." (Emphasis added.)

~~(B) To establish individual identity;~~
~~(C) For physical or biological identification or profiling;~~
~~(D) For the generation of a deepfake; or~~
~~(E) For the operation of generative models, such as large language models.~~

6. **The Agency should provide a reasonable implementation period.**

Certain requirements, specifically those in Articles 1, 9, 10, and 11, require significant upfront implementation, but this is not provided for in the proposed regulations. Uniquely, the requirement for proactive submission of risk assessment materials in § 7157(a) is also a first in the nation requirement. In addition to its broad scope, these submissions by their nature are likely to invite further internal questioning and risk of disclosure. We do not believe that 10 days is sufficient to meaningfully respond to these requirements. Instead, it is in the best interest of covered entities as well as the Attorney General's office to provide more time to make these detailed assessments.

Recommendation: Civil and administrative enforcement of the provisions set forth in Articles 1-11 shall not commence until one year from the date the provisions are in effect.

Recommendation: § 7157(d). "Risk Assessments Must Be Provided to the Agency or to the Attorney General Upon Request. The Agency or the Attorney General may require a business to provide its unabridged risk assessments to the Agency or to the Attorney General at any time. A business must provide its unabridged risk assessments within ~~10~~30 business days of the Agency's or the Attorney General's request."

7. **The cybersecurity audit provisions could undermine security without further revisions.**

The proposed cybersecurity audit provisions do not align with the CCPA's requirements nor operate flexibly in the context of future security challenges, unnecessarily burdening California businesses while providing few corresponding security benefits.

As currently drafted, California businesses' ability to conduct an audit that retains the same requirements as a CCPA audit under § 7123(f) is not wholly useful – this is because there are no other audit regimes that impose equivalent requirements to CCPA audits. Therefore, businesses will simply be required to conduct separate audits under the CCPA regardless of existing best practices. We would encourage the Agency to adopt a series of common cybersecurity audit frameworks to be accepted as compliant with the regulations, rather than counterproductively requiring businesses to make a CCPA-centric determination in each case.

Otherwise, the unique and detailed requirements of the proposed rule will drive a significant amount of the cost of conducting the audits.

Similarly, the controls articulated in § 7123(b) are likely to become outdated in the near future. For this reason, existing cybersecurity audit standards assess how organizations achieve particular outcomes. For example, the NIST recommends as a security control that "the confidentiality, integrity, and availability of data-at-rest are protected." The Agency's proposal, however, requires *specific* security controls to achieve certain outcomes (e.g., requiring assessment of encryption of personal information at rest, assuming the use of multi-factor authentication and passwords when businesses are increasingly moving to passkeys). We believe this is out of step with the core purpose of audits – to identify and remediate risks – rather than mandate detailed papering exercises.

Lastly, given the new and potentially burdensome nature of the audits, it is critical that there are limitations on California businesses' obligations under the requirements for proactive cybersecurity audit submissions, in line with norms found in similar state privacy laws and even Europe's GDPR. This is because the requirement to compile all this information before processing commences, as the draft regulations suggest is required, makes the requirements potentially problematic. Further, information may not be fully knowable, and its evolving nature could cause companies to engage in fruitless guesswork rather than focus on harm mitigation. As such, these limitations should include 1) reasonable limitations on when businesses must submit full audits, 2) an exemption for the redaction of sensitive information or trade secrets, and 3) a requirement that the Agency keep the reports secure and confidential.

Recommendation: § 7125.

(a). A business may satisfy the obligations set forth in Sections § 7120 - § 7124 by completion of a comparable industry standard cybersecurity audit such as ISO 27001, ISO 27018, SOC 2 Type 2.

(b) A single cybersecurity audit that meets the requirements of section (a) may address a comparable set of processing operations that include similar activities.

Process

8. The cost estimate dramatically underestimates implementation costs.

The CPPA's Standardized Regulatory Impact Assessment (SRIA) of the remaining regulations estimates the cost at $3.4 billion for California businesses to implement, but this is likely well below the true cost that will be incurred. This is because the analysis mistakenly leaves out two key elements that dramatically increase the likely cost: 1) it underestimates the number of businesses affected, and 2) it does not consider the regulations' continuing effects on California businesses' operating costs and productivity.

First, the estimate only includes businesses with employees in California, eschewing the many out-of-state companies that sell into California and its markets. The SRIA actually acknowledges the proposed regulations' effects on out-of-state companies, yet opts to leave out these costs because they do not impact California businesses themselves. However, the SRIA also requires recognition of effects on jobs and investment in the state. Because the proposed requirements would compel out-of-state businesses to face the same audits, ADMT opt-out provisions, and risk assessment requirements, small entities especially will be incentivized to withdraw from California markets to avoid these costs. The cost of the reduction in choices, reduced competition, and higher prices is likely to raise first-year costs by potentially several billion dollars above the estimate.[9]

Second, the SRIA addresses only the costs of programming, cybersecurity audits and risk assessments, and ignores the effects of the proposed regulations on ongoing business operations, including negatives to cost and productivity. This underestimates the expense, especially of the proposed regulations around ADMT, whose broad scope and first in the nation impact will dramatically increase California business's ongoing costs.

These include costs associated with:

1) intake and response to ADMT opt-out requests from consumers,

2) administering a non-automated process for each ADMT-covered decision,

3) responding to consumer inquiries about the purpose for which the business is using ADMT and outputs regarding that consumer, and

4) the inevitably negative impact of consumer and employee opt-outs on the reliability of ADMT or the reliability of behavioral advertising (as previously discussed).

[9] Comments on August 2024 CPPA SRIA for California Chamber of Commerce.

Policies that stifle a significant fraction of the total value of AI adoption and use would likely have impacts in excess of tens of billions per year – a cost that far exceeds any savings accrued from the proposed regulations.[10]

* * *

Thank you for considering our feedback regarding the draft regulations. We are happy to discuss any of these comments in further detail. SIIA's points of contacts for this submission are Paul Lekas, SVP and Head of Global Public Policy and Government Affairs (plekas@siia.net) and Anton van Seventer, Counsel for Privacy and Data Policy (avanseventer@siia.net).

[10] Goldman Sachs, "Generative AI Could Raise Global GDP by 7%." April 5, 2023. https://www.goldmansachs.com/insights/articles/generative-ai-could-raise-global-gdp-by-7-percent.