website and app, disclosures that promise to at best annoy California consumers and more likely confuse, alarm, and mislead them.

The current proposal also exceeds the CCPA's grant of rulemaking authority. Though the CCPA was written to advance focused privacy and data-security objectives, the proposed regulations instead seek to redress complex social issues from civil rights to economic equity that are simply beyond the statutory mandate. Under the guise of regulating automated decisions, the rules propose to cover everyday decisions made by humans simply because those decisions rely in some part on software.

We thus urge the Agency to revisit these regulations to advance instead the privacy and security objectives that animated the CCPA, while allowing businesses to innovate free from exceptional restrictions that would not benefit any California consumer. We write to highlight our most pressing concerns.

I. The Proposed Regulations Exceed and Are Inconsistent with the Statutory Authorization

The proposed regulations must be consistent with the statute that authorized them.[2] And they may not vary from or enlarge the statute's terms.[3] The proposed regulations do not adhere to these principles in certain foundational respects.

The CCPA was originally enacted in 2018 with the stated goal of ensuring the privacy of Californians' personal information. As discussed in more detail below, the 2020 ballot initiative, Prop. 24, amended the CCPA to further strengthen the privacy and security of personal information – including by creating the CPPA to protect, as the Agency's name implies, Californians' privacy.

This 2020 amendment contains two relevant grants of authority. Section 1798.185(a)(14) authorizes the Agency to:

> [I]ssu[e] regulations requiring businesses whose processing of consumers' personal information **presents significant risk to consumers' privacy or security** . . . [to] [p]erform a cybersecurity audit on an annual basis . . . [and to] submit to the California Privacy Protection Agency on a regular basis a risk assessment.[4]

[2] Gov. Code, § 11342.2 ("No regulation adopted is valid or effective unless consistent and not in conflict with the statute").
[3] *Credit Ins. Gen. Agents Ass'n v. Payne* (1976) 16 Cal.3d 651, 656.
[4] Civ. Code, § 1798.185, subd. (a)(14)(B) (emphasis added).

And Section 1798.185(a)(15) authorizes the CPPA to:

> Issue regulations governing **access and opt-out rights** with respect to a business' use of **automated decisionmaking 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]

In several key ways, the proposed regulations stray from these narrow authorizations. They would cover a vast range of technologies, use cases, and perceived harms and would impose unprecedented requirements on virtually every business that uses technology. These requirements do not advance, but instead conflict with, the privacy and security aims of the animating law.

A. The proposed regulations would improperly regulate *human* decisionmaking under a grant of authority to regulate only *automated* decisionmaking

Subsection (a)(15) authorizes the Agency to issue targeted regulations governing "automated decisionmaking technology,"[6] a term which is not defined in the statute. The Agency has proposed defining "automated decisionmaking technology" as "any technology that processes personal information and uses computation to" do one of three things: "execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking."[7]

This definition conflicts with the statute. The statutory phrase "automated decisionmaking" is a term of art, first introduced in European privacy regulations, which refers to "a decision based solely on automated processing."[8] The same definition results from giving each word in "automated decisionmaking technology" its plain meaning: "Decisionmaking" is "the process or practice of making choices or judgments, esp. after a period of discussion or thought."[9] And "automated" means "self-acting or self regulating," "*without needing human control*."[10]

[5] Civ. Code, § 1798.185, subd. (a)(15) (emphasis added).
[6] Civ. Code, § 1798.185, subd. (a)(15).
[7] Proposed Text of Regulations (Cal. Priv. Prot. Agency, Nov. 2024) (hereafter Draft Regulations), § 7001, subd. (f) (emphasis added).
[8] EU General Data Protection Regulation (GDPR), art. 22.
[9] *Decision-making*, Black's Law Dict. (12th ed. 2024).
[10] *Automated*, Merriam-Webster Dict. ("operated automatically"); *Automatically*, Merriam-Webster Dict. ("done or produced as if by machine . . . having a self-acting or self-regulating mechanism"); *Automated*, Cambridge Dict. ("carried out by machines or computers without needing human control"); *Automated*, Oxford English Dict. ("Converted so as to operate automatically . . . automatic"); *Automatic*, Oxford English Dict. ("self-generated, spontaneous; . . . self-acting; having the power of motion within itself").

The proposed definition *partially* maps to this plain meaning. One of its three components is "any technology that . . . uses computation to . . . replace human decisionmaking," which tracks the statutory term. This is an appropriately narrow definition. It may cover, for example, a machine-learning algorithm used by a college to predict the future performance of high school students based on data in their application and then decide, without human input, which students to admit.

But the other two components of the definition do not track the statutory grant of authority. First, the proposed regulations would cover "*executing*" a decision already made by a human. By definition, then, technology in this bucket would not be "making" a decision and so fall outside the authorization. For example, if a law firm decides that associates who work above a certain number of hours will receive a bonus, a program that automatically identifies and notifies associates who are above or below that pre-determined threshold is merely executing the decision already made by the firm. It is not, in any meaningful sense, "making" a decision about who will receive a bonus. But the regulations would apparently cover this use case. The statute does not plausibly regulate this use of technology.

Second, the regulations improperly propose to regulate "human decisionmaking" that is "*substantially facilitat[ed]*" by technology. For instance, the regulations stipulate that "generat[ing] a score about a consumer that [a] *human reviewer* uses as a primary factor to make a significant decision" would be regulated.[11] By its own admission, then, this third proposed definition does not regulate "automated" decisionmaking.[12] Nothing in the CCPA authorizes regulating *human* decisions simply because they are aided or informed by technology.[13] In fact, in recent decades, a significant amount of human decisionmaking has been "substantially facilitated" by "the output of . . . technology." Take an entity that consults a medical diagnostic to help determine whether someone is eligible for a clinical trial; or a business that consults a review website's algorithm when choosing what plumber to hire, but ultimately has a human make the final call. Nobody would naturally say that these examples involve "*automated* decisionmaking," even if an automated process informs a decision that is ultimately made.[14]

[11] Draft Regulations, § 7001, subd. (f)(2).

[12] See *Southwest Airlines Co. v. Saxon* (2022) 596 U.S. 450, 457–58 (describing "meaning-variation canon" as "where [a] document has used one term in one place, and a materially different term in another, the presumption is that the different term denotes a different idea").

[13] "Facilitating" just means "mak[ing] easier" or "help[ing] bring (something) about." (See *facilitate*, Merriam-Webster Dict.). Like "executing," "facilitating" does not involve the making of any decisions.

[14] The Agency's proposed regulations governing the opt-out rights, and specifically the exemptions, underscore this problem. As an initial matter, this "human appeal" exception and the other exemptions in the proposed regulations are unmoored from the statutory purpose of advancing privacy and security, focusing instead on issues like accuracy, fairness, and discrimination. And the human appeal exception in particular demonstrates the overbreadth of the Agency's definition of ADMT: If a decision is subject to human review, then it is, by definition, not automated; it is ultimately being made by a human. Yet the exception applies only to certain types of decisions, when a human appeal should remove a decision from

Although the draft regulations propose to exempt technologies akin to a "calculator," this limitation does not do anything. In the same breath, the regulations provide that calculators and the like *are* covered if used to "execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking."[15] Since that is just the definition of ADMT reprinted, the "calculator" exception does not change the scope of the regulations' coverage. And indeed the regulations are replete with supposed examples of "automated decisionmaking technology" that work exactly like calculators. For example, the regulations offer as an example of ADMT "a business's use of a spreadsheet to run regression analyses" on employees' performance records.[16] But many calculators have a regression function.[17] It is even possible to calculate a regression on a four-function calculator (or even by hand), using just addition, subtraction, multiplication, and division.[18] If regressions count as ADMT, the purported exclusion of "calculators" cannot mean very much. Likewise, Section 7150(c)(1) contends that the regulations would apply when a rideshare platform assigns rides to drivers, even though rideshare platforms typically allocate work based on human-specified geospatial formulas that calculate which driver is closest to the customer, rather than any sort of automated decision.[19] The lack of real difference between the technologies explicitly included and purportedly excluded under the regulations suggests that in practice, virtually all forms of computation will be covered. Because the CCPA authorizes regulations only of automated decisionmaking, however, these regulations go well past their authorized scope.

Another tell that the regulations exceed the statutory mandate is that their definition of "automated decisionmaking" is out of step with how that term is used internationally. As noted, Europe recognizes that "automated decisionmaking" does not cover decisions that involve humans. Article 22 of the General Data Protection Regulation ("GDPR"), on "Automated Individual Decision-Making, Including Profiling" covers "decisions based *solely* on automated processing."[20]

the scope of the regulations entirely. This further demonstrates that the definition of ADMT is overbroad and strays beyond the statutory mandate.

[15] Draft Regulations, § 7001, subd. (f)(4).

[16] Draft Regulations, § 7001, subd. (f)(4).

[17] *Solution 11918: Calculating and Graphing a Linear Regressions on the TI-83 Plus*, Texas Instruments Knowledge Base (accessed January 31, 2025), https://education.ti.com/en/customer-support/knowledge-base/ti-83-84-plus-family/product-usage/11918.

[18] Bobbitt, *How to Perform Linear Regression by Hand*, Statology (May 8, 2020).

[19] Patent No. US12086897, *Dynamic Optimized Reassignment of Providers at Geohash Level*, Applicant: Lyft, Inc., February 3, 2020, https://patentimages.storage.googleapis.com/ee/e5/49/b80dd99269e026/US12086897.pdf; Patent No. US20200072622A1, *Determining Matches Using Dynamic Provider Eligibility Model*, Applicant: Lyft, Inc., February 3, 2020, https://patentimages.storage.googleapis.com/4a/3d/da/1a310f2e188a4a/US20200072622A1.pdf.

[20] GDPR, art. 22 (emphasis added); see also GDPR, recital 71.

Similarly, the U.K. government, in its guidance on the U.K. version of the GDPR, explains that "automated decision-making is the process of making a decision by automated means *without any human involvement*."[21] Brazil's equivalent law similarly equates "automated decision[s]" with "decisions made solely based on automated processing."[22] To interpret California's law to extend to human decisionmaking using technology would be incongruous and wrong.

The proposal to regulate human decisionmaking – as opposed to an "automated decision" based "solely on automated processing" – thus exceeds the grant of authority that supports the regulations. The references to "executing" and "substantially facilitating" human decisions should be removed from the proposed regulations, and the regulations should be modified to exclude examples, like in Sections 7001(f)(4) and 7150(c)(1)–(2), that do not involve the making of decisions solely by automated technology.

B. There is no basis in the statute for keying the regulatory requirements off the overly broad category of "significant decisions"

The proposed rules extensively regulate businesses that use automation to make any "significant decision," which the Agency defines to include decisions without any connection to the privacy concerns that establish its authority to regulate here. The category of "significant decisions" is instead defined to cover much of the economy with no privacy tether at all: any decision "that results in access to, or the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice (e.g., posting of bail bonds), employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services (e.g., groceries, medicine, hygiene products, or fuel)."[23] When a business uses automation to make a significant decision as the proposed regulations define that term, it must conduct a risk assessment, issue a pre-use notice, and (unless it meets certain exceptions) offer consumers the right to opt out of ADMT and a right of access.

The throughline across these supposedly "significant" decisions is plainly not privacy (and the regulation barely purports to have that theme); it is that these decisions arguably involve a socially important industry. For example, the regulations would govern remote software used to proctor a college-admissions test that processes a consumer's IP address. Examples like this are covered

[21] Information Comm'r's Off., What is Automated Individual Decision-Making and Profiling? (accessed Jan. 31, 2025), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/.

[22] Lei Geral de Proteção de Dados (LGPD), Art. 20, Official Journal of the Brazilian Government (August 14, 2018).

[23] Draft Regulations, § 7220, subd. (a)(1).

because the Agency considers educational admissions to be important, not because they implicate privacy concerns in any real sense.

But there is no basis in the statute to have these sweeping requirements turn merely on whether a decision is "significant," without any tether to the statute's focus on data privacy and security. The CCPA is a *privacy* law, not an all-purpose regulator of automation applications perceived to be socially important. Prop. 24 was titled the "California *Privacy* Rights Act."[24] And the resulting law is about data privacy from top to bottom. The law mentions "privacy," "security," and "personal information" more than 500 times, but "automated decisionmaking" only once, in a single sentence.[25] That sentence is one subsection of one subsection out of Prop. 24's 31-section, over-20,000-word ballot initiative.[26] It is implausible that in this single sentence, California voters intended to authorize a new legal framework for regulating automated decisionmaking entirely disconnected from privacy concerns.[27] There is nothing in the CCPA to support the idea that the agency is now empowered to enforce it as a general consumer-protection or anti-discrimination statute.[28]

The CPRA's enactment history further confirms what was (and was not) on California voters' minds when they approved Prop. 24. As the public debated the law, the *only* concerns presented to them involved privacy and security.[29] The ballot guide explained that Prop. 24 sought to "amend[] consumer privacy laws."[30] The Attorney General's official summary promised that the

[24] Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020).
[25] Draft Regulations.
[26] Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020).
[27] Indeed, these other concerns are already being addressed by other agencies. The California Civil Rights Department has issued its own proposed regulations concerning the use of "automated-decision systems" in potentially discriminatory ways. (Second Modifications to Initial Text of Proposed Modifications to Employment Regulations Regarding Automated-Decision Systems (Civil Rights Council, Jan. 27, 2025), https://calcivilrights.ca.gov/wp-content/uploads/sites/32/2025/02/Second-Modifications-to-Proposed-Modifications-to-Employment-Regulations-Regarding-Automated-Decision-Systems.pdf.)
Such regulations are best left to an agency which has the authority and competence to address discrimination and fairness. The regulations should be narrowed to focus the opt-out right on factors that relate to privacy and security.
[28] It is also no answer that subsection (a)(15) authorizes the Agency to regulate automated decisionmaking. That subsection is prefaced and cabined by section 1798.185, subd. (a), which requires all regulations to "further the purposes of this title." As we have explained, those purposes all relate to privacy. By contrast, Prop. 24's "purpose and intent" section does not mention automation or AI even once. Thus, subsection (a)(15) authorizes the agency to regulate automated decisionmaking as necessary to promote data privacy and security. It does not grant a freestanding power to regulate ADMT unmoored from those concerns.
[29] California Secretary of State, Official Voter Information Guide, November 3, 2020, pp. 66–71, https://vig.cdn.sos.ca.gov/2020/general/pdf/complete-vig.pdf.
[30] *Id*. at p. 66.

law would let consumers "prevent businesses from sharing personal information," "correct inaccurate personal information," and "limit businesses' use of sensitive personal information."[31] It also explained that the Agency would "enforce and implement consumer privacy laws."[32] The Legislative Analyst added that Prop. 24 would "change[] existing consumer data privacy laws" and "provide new consumer privacy rights" concerning the "*sharing* of personal data" and "use of 'sensitive' personal data."[33] He also noted that the CPPA's authority to "develop[] . . . new regulations" encompassed the power to pass "rules for correcting consumer personal data."[34] And the arguments for and against Prop. 24 focused exclusively on whether the law would "protect . . . personal information" and how it would impact "privacy rights."[35]

By contrast, automated decisionmaking and artificial intelligence were not on anyone's radar. The terms "automated decisionmaking" and "artificial intelligence" do not appear even once in any of the ballot-initiative materials that accompanied Prop. 24.[36] Nor did the Legislative Analyst discuss regulating ADMT, much less for decisions involving non-sensitive information. The complete absence "of such a goal . . . [from the] ballot materials" is a strong tell that the law did not enact it.[37] Indeed, "[i]f this quite significant consequence were consistent with the most reasonable understanding of Proposition [24]'s purpose . . . one would assume there would be some mention of such a goal elsewhere in Proposition [24]."[38] "[E]nactors do not 'hide elephants in mouseholes.'"[39] And here, that simply cannot be a sound principle of statutory interpretation; Prop. 24's drafters were forbidden from wedging a comprehensive AI bill into their privacy statute. Under California law, "[a]n initiative measure embracing more than one subject may not be submitted to the electors or have any effect."[40]

It comes as little surprise then that even the primary advocate for and drafter of Prop. 24, Alastair Mactaggart, has also commented on how the draft regulations have improperly strayed from the privacy mandate.[41] At the November 8, 2024 CPPA board meeting, for instance, Mactaggart

[31] *Ibid.*
[32] *Ibid.*
[33] *Id.* at pp. 67–68.
[34] *Id.* at p. 68.
[35] *Id.* at pp. 7071.
[36] Official Voter Information Guide.
[37] *Cal. Cannabis Coalition v. City of Upland* (2017) 3 Cal.5th 924, 940.
[38] *Ibid.*
[39] *Ibid.*
[40] Cal. Const. art. II, § 8(d); see, e.g., *Cal. Trial Lawyers Assn. v. Eu* (1988) 200 Cal.App.3d 351, 359–360 (provision regulating insurers' campaign contributions was not related to the initiative's subject of "spiralling insurance costs").
[41] Nov. 8 CPPA Bd. Hr'g Tr. pp. 99–103.

reminded the Agency that "we should focus on our privacy mandate" after explaining how the draft regulations exceed their authorized scope.[42]

A comparison to Europe's GDPR also shows why the statute does not authorize the regulation of decisions based solely on their "significance." As we noted in Part I.A, there is some overlap in the language between Prop. 24 and the GDPR. For example, both laws regulate automated decisionmaking – an indicator that the concept should have similar meaning in both jurisdictions. But the converse is also true: When Prop. 24 conspicuously failed to borrow a certain aspect of the GDPR, that is evidence the voters did *not* intend to import this facet of the European regulations. In this vein, it is telling that, whereas the GDPR regulates the use of automated decisionmaking to make "significant[]" decisions, Prop. 24 omitted that phrasing from its provision concerning automated decisionmaking, instead keeping the focus on the narrower domain of privacy.[43] Given that the California voters specifically declined to import the "significance" framework, it would be inappropriate for the implementing regulations to reverse course and do just that.

Because the regulations turn on the broad category a business decision falls into, not the degree to which (or even whether) the decision implicates privacy, they are inconsistent with the privacy rationale explicitly stated in Prop. 24 and approved by the voters. And when coupled with the overly broad definition of ADMT, these regulations cover an astoundingly large swath of the economy that Prop. 24 could not have plausibly meant to regulate. The proposed rules plainly exceed their authorization in the CCPA and must instead be revised to cover only decisions with a significant privacy impact.

C. The provisions limiting how a business can advertise to its own customers based on existing data are not authorized by and are inconsistent with the statute

The draft regulations impose far-reaching and unauthorized obligations on first-party "behavioral advertising." The regulations put a raft of requirements – extensive disclosures, burdensome evaluations, and mandatory opt-out rights – on businesses that engage in so-called "extensive profiling," which, contrary to the plain meaning of those words, is defined to encompass *all* personalized advertising, including advertising based on data a business *already has* through its own transactions with its customers.[44] All these requirements may apply to, for example, a retailer that recommends cleaning supplies to a customer who previously bought them, at a point when

[42] *Id*. at p. 106.
[43] See Prop. 24.
[44] Draft Regulations, § 7001, subd. (g) ("'Behavioral advertising' means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity . . . *within the business's own distinctly-branded websites, applications, or services.*") (emphasis added).

those supplies may be running low. But the CCPA does not authorize the extensive regulation of this benign conduct; indeed the voters consciously drew a line between such first-party advertising, which they allowed, and cross-context behavioral advertising, which they explicitly gave consumers the right to opt out of.[45]

Indeed, when voters amended the CCPA, they directly addressed the question of how to regulate advertising, leaving no room for the proposed rules. The CCPA, as enacted by the legislature, permitted businesses to use consumers' personal information for advertising and marketing, and gave consumers the right to opt out only from their data being sold to third parties.[46] Prop. 24 expanded that opt-out right to cover both the "selling" and "sharing" of personal information. It specifically identified "cross-context behavioral advertising" – that is, advertising "based on the consumer's personal information obtained from the consumer's activity *across businesses, distinctly-branded websites, applications, or services*" – as a type of "sharing."[47] So while Prop. 24 provided a right to opt out of cross-context behavioral advertising, it did not impose any comparable restrictions on first-party advertising.

Prop. 24's preamble and legislative history further underscore the voters' intent to regulate third-party advertising only. The preamble indicates that voters were focused on the selling or sharing of their personal information with other businesses.[48] The Legislative Analyst confirmed that one of the key rights created by Prop. 24 was to limit the "*sharing* of personal data."[49] Similarly, in describing why Prop. 24 added the concept of "sharing" data and created opt-out rights for "cross-context behavioral advertising," Mactaggart explained that Prop. 24 made it "crystal-clear, when it comes to sharing consumer information for cross context behavioral advertising, that the law gives consumers the right to opt out."[50] On the other hand, he noted that "*first-party data the business has can be used in any way that the business wants with that consumer*."[51] That was the fundamental balance struck by Prop. 24: consumers were given a right to opt out of *third-party* targeted advertising, but businesses maintained the ability to engage in *first-party* advertising – that is, to advertise to consumers based on information gathered as part of a business's own

[45] Draft Regulations, § 7001, subd. (g).

[46] Cal. Assem. Bill No. 375 (2017–2018 Reg. Sess.); Civ. Code, § 1798.140, subd. (d)(4).

[47] Civ. Code, § 1798.140, subds. (k), (ah)(1).

[48] Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 2.I ("Consumers should have the information and tools necessary to limit the use of their information to non-invasive, pro-privacy advertising, where their personal information is not sold to or shared with hundreds of businesses they've never heard of, if they choose to do so.").

[49] California Secretary of State, Official Voter Information Guide, November 3, 2020, pp. 66–71.

[50] Davis + Gilbert LLP, *Alastair Mactaggart's Privacy Perspective: Past, Present and Where We're Headed* (2022), https://www.mondaq.com/unitedstates/data-protection/1183432/alastair-mactaggarts-privacy-perspective-past-present-and-where-were-headed.

[51] *Ibid.*

relationship with a consumer. In adding opt outs and burdensome requirements for first-party advertising, the proposed regulations are fundamentally at odds with the voters' intent in approving Prop. 24.

Nor does the mere use of the word "profiling" in the statute justify the scope of the proposed regulations. In explaining its expansive definition of that word, the Agency points to various other state statutes that also regulate "profiling." But each of these laws – like the CCPA and Prop. 24 – treats profiling and advertising as distinct concepts. Each law creates a right to opt out of profiling in some circumstances.[52] And then each law handles advertising with *separate* statutory language, reflecting the universal understanding that "advertising" and "profiling" are distinct practices.[53] (And in turn, the "advertising" proscriptions in these statutes unflaggingly cover only "*targeted* advertising" – a term, much like "cross-context behavioral advertising" in Prop. 24, defined to exclude first-party advertising.)[54] It is precisely because Prop. 24 was enacted against a legal background in which "profiling" did not cover "advertising" that Prop. 24 needed to separately address advertising. And when it did, it explicitly carved out first-party advertising from opt-out rights.[55]

The Agency has no authority to include first-party advertising in the draft regulations and should remove all references to first-party behavioral advertising.

[52] See, e.g., Va. Code Ann., § 59.1-577, subd. (5)(iii) (providing the ability to opt out of "profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer"); Colo. Rev. Stat. Ann., § 6-1-1306, subd. (1)(a)(I)(C) (similar); Conn. Gen. Stat. Ann., § 42-518, subd. (a)(5)(c) (similar); Del. Code Ann. tit. 6, § 12D-104(a)(6)(c) (similar); Fla. Stat., § 501.705, subd. (2)(e)(3) (similar); Ind. Code, § 24-15-3-1, subd. (b)(5)(C) (similar).

[53] See, e.g., Va. Code Ann., § 59.1-577, subd. (5)(i) (providing the ability to opt out of "targeted advertising"); Colo. Rev. Stat. Ann., § 6-1-1306, subd. (1)(a)(I)(A) (similar); Conn. Gen. Stat. Ann., § 42-518, subd. (a)(5)(A) (similar); Del. Code Ann. tit. 6, § 12D-104, subd. (a)(6)(a) (similar); Fla. Stat., § 501.705, subd. (2)(e)(1) (similar); Ind. Code § 24-15-3-1(b)(5)(A) (similar).

[54] See, e.g., Va. Code Ann., § 59.1-575 ("'[t]argeted advertising' does not include . . . [a]dvertisements based on activities within a controller's own websites or online applications"); Colo. Rev. Stat. Ann., § 6-1-1303, subd. (25) (similar); Conn. Gen. Stat. Ann., § 42-515, subd. (39) (similar); Del. Code Ann. tit. 6, § 12D-102, subd. (33) (similar); Fla. Stat., § 501.702, subd. (33) (similar); Ind. Code, § 24-15-2-30 (similar).

[55] The Federal Trade Commission distinguishes between first-party data use and third-party data sharing as well, singling out the latter for enforcement. See, e.g., *In re Gateway Learning Corp.* (July 7, 2004), FTC No. 042-3047,
https://www.ftc.gov/sites/default/files/documents/cases/2004/07/040707agree0423047.pdf;
In re Chitika, Inc. (Mar. 14, 2011), FTC No. 1023087,
https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110314chitikaagree.pdf.

D. The regulations related to "physical or biological identification or profiling" are unauthorized

The draft regulations seek to impose multiple unwarranted requirements on "physical or biological identification or profiling." The regulations define "physical or biological identification or profiling" to mean "identifying or profiling a consumer using information that depicts or describes their physical or biological characteristics, or measurements of or relating to their body."[56] A business who uses "physical or biological identification or profiling" for a "significant decision" or "extensive profiling" must "conduct an evaluation" of its "identifying or profiling to ensure that it works as intended" and "does not discriminate"; and "must implement policies, procedures, and training to ensure" that the "identifying or profiling works as intended."[57] The regulations would grant consumers a complete right to opt out of the use of their personal information for any training of ADMT that is capable of being used "for physical or biological identification or profiling."[58] These regulations are incompatible with the statute.

To start, although the Agency has apparently proposed these regulations under its Subsection (a)(15) power to regulate "access and opt-out rights with respect to a business' use of automated decisionmaking technology, including profiling," the regulations fly past this grant of authority in two ways. For one thing, they regulate far more than access and opt-out rights. They set substantive criteria that "identification or profiling" must satisfy and compel testing and quality-assurance procedures. There is no basis for this substantive aspect of the regulations. The regulations also exceed the statutory requirement that they concern "automated decisionmaking technology, including profiling." The regulations cover, in addition to profiling, the mere "identifying" of a consumer using biometrics.[59] "Identifying" is not "profiling."[60] The draft

[56] Draft Regulations, § 7001, subd. (gg).

[57] Draft Regulations, § 7201.

[58] Draft Regulations, §§ 7200, subd. (a), 7221, subd. (a)–(b).

[59] No other comprehensive state law includes "identification" in the definition of "profiling." See, e.g., Va. Code Ann., § 59.1-575 ("'Profiling' means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements." Identification does not fall under this definition because identification does not require businesses to "evaluate, analyze, or predict . . . personal aspects" like "health" or "personal preferences," but rather to verify or confirm one's identity.); Ind. Code, tit. 24, § 24-15-2-23 (defining profiling as "solely" automated processing but similarly excluding "identification" because it is not an "evaluat[ion], analy[sis], or predict[ion] relating to "personal aspects" like "health records," "interests," or "movements").

[60] It does not appear that the Agency has tried to justify this regulation under the authority to regulate "automated decisionmaking." And for good reason: identification does not entail making a decision. When an online grocery store uses a scanner to check the ID of someone buying medicine, or a college's anti-cheating software automatically verifies the student ID of a remote exam taker, to say that anyone

regulations define "profiling" as processing personal information to "analyze or predict aspects concerning that natural person's intelligence, ability, aptitude, performance at work, economic situation; health, including mental health; personal preferences, interests, reliability, predispositions, behavior, location, or movements"[61] – in short, predicting someone's behavior or personal characteristics. Someone's identity, however, is not a behavior or characteristic. Other parts of the CCPA bolster this distinction between "identifying" and "profiling." For example, the CCPA grants consumers the right to opt out of certain uses of their biometric information, but not if a business has collected this information "without the purpose of inferring characteristics about a consumer."[62] And even the portion of the regulations ostensibly directed at "profiling" exceeds the statutory limit. The statute authorizes at most a right for consumers to opt out of having their data used to profile them – not the right created by the regulations, a right to opt out of having their data used merely to train a technology that theoretically could be used to profile other people.[63]

The regulations also conflict with the statute by erecting a confusing scheme for regulating biometric information that competes with a different one already created by the statute. The statute already defines a category called "sensitive personal information," which includes "the processing of biometric information for the purpose of uniquely identifying a consumer."[64] The statute then guarantees consumers the right to limit the use of their sensitive personal information.[65] But this right is highly qualified. Consumers cannot opt out of businesses' using their data to "improve, upgrade, or enhance the service[s]" they offer.[66] The statute also authorizes additional rules qualifying this right of consumers in order to protect the "legitimate operational interests of businesses."[67]

The draft regulations conflict with this carefully balanced scheme. For example, under the draft regulations, a user may opt out of the use of her biometric data to "improve [a business's] algorithm."[68] This is irreconcilable with the statute's express safe harbor allowing businesses to use sensitive personal information to improve the services they offer. And putting this specific glaring conflict aside, given that the statute already lays out an approach to biometric regulation and does so using a specific statutory term, the statute cannot be plausibly read to authorize the

has made a "decision" would be strained. There has been no judgment or weighing of options; the identifications are no more a "decision" than when a calculator determines whether two values are equal.

[61] Draft Regulations, §7001, subd. (kk).

[62] Civ. Code, § 1798.121, subd. (d).

[63] Civ. Code, § 1798.185, subd. (a)(15).

[64] Civ. Code, § 1798.140, subd. (ae)(2).

[65] Civ. Code, § 1798.121.

[66] Civ. Code, §§ 1798.121, subd. (a), 1798.140, subd. (e)(8).

[67] Civ. Code, § 1798.185, subd. (a)(18)(C).

[68] Draft Regulations, §§ 7200, subd. (a), 7221, subd. (a)–(b).

Agency to define a new similar, overlapping term and design a separate scheme of rights associated with that term.[69]

The proposed regulations of "physical or biological identification or profiling" should therefore be removed. At the very minimum, "identification" and "identifying" should be deleted from the definition.

E. The "Pre-Use Notice" requirements are not authorized by the statute

Even though the enabling provision authorizes "regulations governing *access* and *opt-out* rights" for automated decisionmaking, the proposed regulations invent an entirely new category of requirements.[70] Specifically, businesses engaged in ADMT must provide a "prominent and conspicuous" pre-use notice with extensive information, including: a "plain language explanation of the specific purpose for which the business proposes to use the automated decisionmaking technology"; an explanation of any exceptions to the right to opt out that the business relied on; "information about how the automated decisionmaking technology works," such as the "logic," "key parameters," and "intended output" of the ADMT; and information about the role of humans in the decision.[71]

These mandated disclosures conflict with the CCPA. Not only does the statute nowhere mention them, it explicitly handles consumer notice differently. When discussing consumers' right to "information about [an algorithm's] logic," the law specifically couches that right in terms of an "access" request rather than any sort of pre-use notification. Meanwhile, other parts of the law require businesses to give notice, in some form, of what personal information they collect and how it is used "at or before the point of collection"[72] – but as other parts of the regulations make clear, this flexible requirement can be satisfied by providing consumers with a link to a section of its

[69] Further illustrating that implausibility is that in addition to conflicting with the statute, the draft regulations conflict sharply with the existing regulations fleshing out limitations on the use of "sensitive information." Under the existing regulations, businesses have the right to use sensitive information like biometrics to "verify or maintain" the quality of the business's products and "improve, upgrade, or enhance" their service or device (§ 7027, subd. (m)). By contrast, under the draft regulations, a business may not use biometrics to "improve [its] algorithm" if a user opts out (Draft Regulations, §§ 7200, subd. (a), 7221 subd. (a)–(b)). It is inevitable that having two separate regulations of essentially the same activity will lead to conflicts like this – not to mention unsettle the expectations of businesses that have already invested money complying with the first set of regulations – which is further evidence the statute did not authorize that.

[70] Civ. Code, § 1798.185, subd. (a)(15).

[71] Draft Regulations, § 7220. While Civ. Code, § 1798.185, subd. (a)(15) authorizes the Agency to issue regulations requiring "meaningful information about the logic involved in those decisionmaking processes," that is only in connection with "response[s] to access requests," not a "pre-use notice."

[72] Civ. Code, § 1798.100, subd. (a).

privacy policy.[73] Elsewhere, the CCPA does expressly require businesses to issue certain "prominent" disclosures, but notably not here.[74] The legislature and voters thus know how to create a "pre-collection" notice regime, and even created an intricate one. They chose not to authorize the Agency to create yet another. [75]

And for good reason. Especially given the scope of the regulations, users would be bombarded with the proposed pre-use notifications constantly. As detailed in Part II below, copious social-science research confirms that consumers are likely to suffer from this information overload. The California law, correctly interpreted, does not allow this anti-consumer result. The Agency has no authority to include a pre-use notice requirement in the draft regulations and should remove the requirement.

II. The Regulations Are Not Supported by Substantial Evidence

Regulations must be reasonably necessary to implement the statute authorizing them,[76] and the proposed regulations are not. Although the draft regulations would impose unprecedented burdens on California businesses and consumers, there is not substantial evidence that they are necessary to effectuate the goals of the CCPA. Those goals, as we have noted, were explicit. Prop. 24 states that "the rights of consumers and the responsibilities of businesses should be implemented with the goal of strengthening consumer privacy, while giving attention to the impact on business and innovation."[77] The proposed regulations advance many concerns unrelated to privacy and security while impeding innovative product development.

This is why Mactaggart, now a member of the CPPA's board, has expressed concern about the "overreach" of the draft regulations," that they "undermine[] privacy rather than protecting it," and that they mandate obligations inconsistent with the "privacy and security" focus of the statute.[78] As explained more below, the overly burdensome demands of the regulations are likely to lead

[73] Cal. Code Regs., tit. 11, § 7012, subd. (f).

[74] Specifically, "prominent and robust" notice is required when a business transfers personal information to a third party as part of a "merger, acquisition, bankruptcy, or other transaction" and the third party "materially alters how it uses or shares the personal information." (Civ. Code, § 1798.140, subds. (ad)(2)(C), (ah)(2)(C).) Third parties are permitted, but not required, to satisfy their notice obligations by "prominently and conspicuously" "providing the required information . . . on the homepage of its internet website." (Civ. Code, § 1798.100, subd. (b)); Civ. Code, § 1798.130, subd. (a)(5)(C)).

[75] *Hamdan v. Rumsfeld*, (2006) 548 U.S. 557, 578 ("A familiar principle of statutory construction . . . is that a negative inference may be drawn from the exclusion of language from one statutory provision that is included in other provisions of the same statute.").

[76] Gov. Code, § 11342.2 ("No regulation adopted is valid or effective unless . . . reasonably necessary to effectuate the purpose of the statute.").

[77] Prop. 24, § 3, subd. (C)(1).

[78] Nov. 8 CPPA Bd. Hr'g Tr., pp. 99–103.

businesses to divert limited resources from effective privacy protections, resulting in a net reduction in actual privacy and security protections for consumers. As Mactaggart put it, "this just creates a regulatory burden that I think has a negative impact on privacy."[79]

A. There is no basis for regulating human decisionmaking merely because it is assisted by technology

The Agency has not put forward substantial evidence to support its definition of ADMT, which imposes onerous requirements on uses of technologies that only "execute" or "substantially facilitate" decisions made by humans. California businesses have used algorithms, artificial intelligence, "regression analyses," "computation," and other technology to assist with human decisions for decades. As Mactaggart noted, the proposed "definition of ADM[T] includes the use of almost any computerized technology in a way that describes how humans have used computers for 30 or 40 years."[80] Businesses have deployed these techniques to execute or inform countless "significant decisions" and instances of "extensive profiling" (as the regulations define those terms), and the use of this technology is essential to California's economy.[81] Yet the Statement of Reasons does not cite any evidence that decisions executed by technology or substantially facilitated by technology put consumers at a heightened privacy or security risk and must be regulated.

Instead, the Statement merely notes that its definition of ADMT "is informed by other frameworks addressing the use of ADMTs," including the Biden Administration's now-rescinded Blueprint for an AI Bill of Rights, an EEOC guidance document, and an academic article that discusses government uses of ADMT.[82] These policy documents do not support the proposed definition, however, since none defines ADMT to include the mere "execution" or "substantial facilitation" of a human decision or contends that those activities present privacy concerns.[83] To the contrary, such a broad scope would put California out of step with other states, including Connecticut,[84]

[79] Nov. 8 CPPA Bd. Hr'g Tr., p. 106.

[80] Nov. 8 CPPA Bd. Hr'g Tr., p. 100.

[81] Additional longstanding practices now covered by these regulations include: use of software or programs derived from statistics or other data-processing techniques (§ 7001, subd. (f)(1)); a business's use of a regression analysis to evaluate employee performances (§ 7001, subd. (f)(4)); a dating app's provision of geolocation, ethnicity, and medical information from a consumer's profile to its analytics service provider (§ 7150, subd. (c)(3)); a grocery store's use of wifi tracking within its stores to observe consumer shopping behavior (§ 7150, subd. (c)(5)); an educational provider's use of software that automatically screens a student's work for plagiarism (§ 7220, subd. (d)(3)).

[82] California Privacy Protection Agency, Initial Statement of Reasons (hereafter ISOR), (July 2024) p. 14.

[83] ISOR at p. 14 n.64.

[84] Conn. Gen. Stat. Ann., § 42-518.

Delaware,[85] Indiana,[86] Montana,[87] Rhode Island,[88] Mayland,[89] Texas,[90] Florida,[91] Nebraska,[92] Tennessee,[93] and New Hampshire,[94] which all provide a right to opt out of profiling in furtherance of "solely" automated decisions. By producing no evidence of privacy harms stemming from the broader range of activities it seeks to cover, the Agency fails to justify the scope of its regulation.[95]

B. There is no basis to define "significant decisions" and "extensive profiling" to cover everyday uses of technology that pose no privacy concerns

The Statement of Reasons does not contain substantial evidence to support the regulations' broad definitions of "significant decisions" or "extensive profiling." In fact, the Statement contains no evidence that the far-reaching scenarios covered by these definitions present any risk to the privacy or security of personal information – much less "substantial evidence" that regulating ADMT in these contexts is necessary.

The Statement offers only high-level explanations for its sweep, without linking the categories the regulations would cover to real privacy concerns. For example, while the Statement cites a generalized concern about the "lack of consumer control over their personal information,"[96] it does not link this concern to examples of a "significant decision" or "extensive profiling," and especially not to examples of first-party behavioral advertising. Nor does the Statement attempt to tie this putative privacy harm to any specific ADMT use (let alone the uses that the Agency characterizes as "significant") or explain why the alleged harms are not adequately addressed by the CCPA and numerous sector-specific laws.[97]

[85] Del. Code Ann., tit. 6, §12D-104, subd. (a)(6)(c).

[86] Ind. Code, § 24-15-23.

[87] Mont. Code Ann., § 30-14-2808.

[88] 6 R.I. Gen. Laws, § 48.1-5, subd. (e)(4).

[89] Md. Code Ann. Com. Law, § 14-4605, subd. (b)(7)(iii).

[90] Tex. Bus. & Com. Code, § 541.001, subd. (24).

[91] Fla. Stat., § 501.702, subd. (25).

[92] Neb. Rev. Stat., § 87-1102, subd. (25).

[93] Tenn. Code Ann., § 47-18-3201, subd. (21).

[94] N.H. Rev. Stat. Ann., § 507-H:4, subd. (I)(e).

[95] During the November 8, 2024 CPPA board meeting, Mactaggart stated, "If a human is materially involved in a decision, no opt-out should be required. And . . . again, I think we should focus on our privacy mandate." (Nov. 8 CPPA Bd. Hr'g Tr., p. 106–107.)

[96] ISOR at p. 60.

[97] See Civ. Code, §§ 1798.110, 1798.120. Consumer-privacy concerns are already addressed by existing sector-specific laws. See Health Insurance Portability and Accountability Act, 45 C.F.R., § 164.502; see also Fair Credit Reporting Act, 15 U.S.C., § 1681, subd. (b); see also Equal Employment Opportunity Commission, 29 C.F.R., § 1635.9.

Although a broader policy debate has recently emerged around the potential benefits and harms of fully automated decisionmaking and AI, this debate has not been principally focused on privacy concerns.[98] Rather, these technologies implicate fairness considerations and broader philosophical questions around the appropriate role of technology in everyday life. This discussion has tended toward the theoretical, emphasizing the potential harms to society if technology is left to its own devices – but with very few examples of real harms related to the Agency's privacy-and-security mandate.[99]

A comparison to Europe's GDPR helps underscore why the regulations here are inappropriately broad. The GDPR covers a broader range of applications (though even then, only with respect to *solely* automated decisions), but it does so in order to implement sweeping human-rights objectives. The GDPR frames its purposes in all-encompassing terms: to "serve mankind," and protect all manner of "freedoms" and "fundamental rights," ranging from "freedom of expression and information" to "diversity."[100] And the GDPR is itself grounded in the European Union's Charter of Fundamental Rights, which enshrines principles such as human dignity, nondiscrimination, and due process.[101] It is no surprise, then, that the GDPR covers all manner of decisions with a legal or similarly significant effect.[102] The CCPA, by contrast, was never meant to promote such a diverse array of human-rights or policy priorities, beyond privacy. It does not establish a comprehensive rights-based framework. As detailed above, it was enacted to enhance transparency, provide consumers with greater control over their personal information, and regulate how businesses collect, share, and sell that information.[103] And thus it cannot carry the weight that the draft regulations seek to put on it.

The references to "behavioral advertising" should be deleted, and as discussed in Part I.B, the regulations should be revised to cover only decisions with a significant privacy impact.

[98] Krupa and Brandstätter, *UK data reform nurtures innovation but ensures safeguards to ensure EU adequacy, officials say* (November 21, 2024), Mlex, https://www.mlex.com/mlex/articles/2264157/uk-data-reform-nurtures-innovation-but-ensures-safeguards-to-ensure-eu-adequacy-officials-say (on UK proposed reform); Kern, *Humans versus machines: Who is perceived to decide fairer? Experimental evidence on attitudes toward automated decision-making* (October 14, 2022), Patterns, Vol. 3, Iss. 10, https://www.sciencedirect.com/science/article/pii/S2666389922002094.

[99] Chakravorti, *AI's Trust Problem* (May 3, 2024) Harv.Bus.Rev, https://hbr.org/2024/05/ais-trust-problem.

[100] GDPR, recital 4.

[101] *Charter of Fundamental Rights of the European Union* (Dec. 7, 2000) O.J. (C 364).

[102] *Ibid.*

[103] See Prop. 24.

C. There is no basis to support the burdensome pre-use notice and request-to-access requirements

Similarly, the detailed and burdensome disclosure obligations contained in the proposed regulations are not necessary to protect consumers' privacy or security.[104] To the contrary, substantial evidence demonstrates that mandating extensive "conspicuous" notices in the course of routine consumer interactions would *undermine* privacy and security by overwhelming consumers and leading them to tune out important disclosures. At the same time, the enormous compliance burden on businesses will be a headwind on innovation.

The Agency has not put forward any evidence that the pre-use notices or access rights will help consumers. The Statement's discussion of pre-use notices is bereft of any evidence justifying the invention of this requirement.[105] And its justification of the "request to access" regulations is nearly as sparse. On that score, the Statement points only to consumers' right to access how credit scores are calculated.[106] But discrete information about credit score calculations is a far cry from the detailed disclosures required here.

Worse still, the regulations are likely to backfire for consumers, because the pre-use notice requirements will result in a highly disruptive online experience. Given the staggering proposed coverage of the "automated decisionmaking" regulations, consumers would be bombarded with pre-use notifications constantly. And given the dense list of required information, the notices will be long. Businesses will need to pepper users with numerous detailed categories of information, ranging from the fine details of how the automation works (its "logic" and "parameters") to a non-generic (that is, long) explanation of the purpose behind the automation, to a list of rights.[107] What is worse, users *must* be presented with most of these details before they even interact with the business or product; this is not like a warning label on a microwave that they may exercise autonomy over whether to read. So it is inevitable that many users will be force-fed excessive information they do not want.

Abundant social science confirms the intuition that overloading consumers with this information will be bad for them. Studies show that forcing consumers to view "excessive information" will overwhelm them and "degrade the quality" of their choices.[108] One reason is that "mandated

[104] ISOR at pp. 85, 91–92.
[105] ISOR at pp. 83–86.
[106] ISOR at pp. 91–97 & nn. 141–143.
[107] Draft Regulations, § 7220, subd. (c).
[108] See Latin, *Good Warnings, Bad Products, and Cognitive Limitations* (1994) 41 UCLA L.Rev. 1193, 1214–15, https://heinonline.org/HOL/LandingPage?handle=hein.journals/uclalr41&div=41&id=&page=; see also Zheng et al., *How Causal Information Affects Decisions* (2020) 13 Cogn. Res. Princ. Implic.,

disclosure can crowd out useful information" and focus users on irrelevant considerations.[109] For example, an FTC study showed that a "proposed disclosure of brokerage fees" caused consumers to focus overly on those fees, and thus "overestimate the total cost of loans."[110] Mandatory disclosures are also often too complicated for consumers to understand.[111] And the situation becomes even worse when disclosures accumulate across products: each decreases the effectiveness of every other one, as they "compete[] for . . . time and attention with [each other]."[112] "Even if [consumers] wanted to read all the disclosures relevant to their decisions, they could not do so proficiently," and they will "soon learn their lesson and give up any inclination they may have had to devote their lives to disclosures."[113] The upshot is that both the "use of encyclopedic warnings" and the "overuse of warnings" "may, in fact, decrease the effectiveness of all warnings."[114] Excessive disclosures may also lead consumers to simply shut down and avoid interacting with covered businesses at all.[115]

Here, consumers will at best tune out the annoying barrage of similarly sounding pre-use notices they see every day, and at worst be distracted from the details they actually need to know, like the features and price of a product, the admissions criteria of a university, or an employer's personnel policies. In no way will they benefit. Consider perhaps the closest analogy to the proposed disclosures, the now-ubiquitous cookie banner that websites display to comply with European regulations. The cookie banner has been a consensus failure for consumer privacy and empowerment, because Internet users have been so inundated with the disclosures that they simply disregard them.[116]

https://pubmed.ncbi.nlm.nih.gov/32056060/ (documenting a psychological experiment showing that giving consumers certain "information can actually lead to worse decisions"); Dalley, *The Use and Misuse of Disclosure as a Regulatory System* (2007) 34 Fla. St. U. L.Rev. 1090, 1115, https://ir.law.fsu.edu/lr/vol34/iss4/2/ (describing "information overload" and how an excess of information can lead decisionmakers to make ill-informed decisions).

[109] Ben-Shahar and Schneider, *The Failure of Mandated Disclosure* (2011) 159 U.Penn.L.Rev. 647, 737, https://www.jstor.org/stable/41149884.

[110] Craswell, *Taking Information Seriously: Misrepresentation and Nondisclosure in Contract Law and Elsewhere* (2006) 92 Va. L.Rev. 565, 584, https://virginialawreview.org/articles/taking-information-seriously-misrepresentation-and-nondisclosure-contract-law-and/.

[111] Ben-Shahar and Schneider at pp. 665–672.

[112] *Id.* at p. 689.

[113] *Id.* at p. 690.

[114] Schwartz and Driver, *Warnings in the Workplace: The Need for a Synthesis of Law and Communication Theory* (1983), 52 U.Cin.L.Rev. 38, 43.

[115] See Craswell at p. 584; Accenture, *The Empowered Consumer* (2024), https://www.accenture.com/us-en/insights/consulting/empowered-consumer (finding that in a three-month period, three quarters of consumers "walked away from purchases simply because they felt overwhelmed" by information).

[116] See, e.g., Utz et al., *(Un)informed Consent: Studying GDPR Consent Notices in the Field* (2019), https://arxiv.org/abs/1909.02638 (studying user behavior in reaction to cookie banners and noting the "[r]ecurring theme[]" "that the notices were 'annoying . . . , so [users] just ignore them out of

The regulations will also be a costly drag on business. Generating the required disclosures for the pre-use notifications and access rights will be an exceedingly complex task. The proposed regulations require an explanation of "the output of the automated decisionmaking technology with respect to the consumer," "the role the output played in the business's decision and the role of any human involvement," and "how the automated decisionmaking technology worked with respect to the consumer."[117] These disclosures will apparently have to be individualized to each consumer. This poses an immense data-governance and retention challenge. Businesses will have to store detailed information regarding every single "significant decision" made using ADMT, and will have to build systems that can, upon request, parse that data to construct a usable individualized response. This is orders of magnitude more challenging than responding to a request to know or a request to correct, under California law, given the inherent complexity of automated processing. Despite that, the regulations do *not* provide any exceptions when compliance would involve "disproportionate effort" – even though similar exceptions exist for requests to correct, delete, or know.[118] Maintaining and processing this data for the entire range of "significant decisions" would necessarily stifle the innovative engines that drive California's economy. But neither the Agency's statement of reasons nor its economic analysis addresses these concerns.

And there are yet more reasons why the disclosures will hurt the public that the Statement does not grapple with. To start, the regulations would compel businesses to make statements that are confusing and even misleading. Disclosing the "logic" and "key parameters" of an ADMT in "plain language" may often be an impossible task. The most advanced AI models today have *billions* or even *trillions* of parameters. Their internal logic is just "a long list of numbers."[119] Translating these numbers into human-understandable explanations is far from trivial.[120] The field

frustration'"); O. Kulyk et al., *Has The GDPR Hype Affected Users' Reaction to Cookie Disclaimers* (2020) 6 J. Cybersecurity, https://academic.oup.com/cybersecurity/article/6/1/tyaa022/6046452 (studying web users' behavior and concluding that "participants considered the cookie disclaimer as a nuisance" and so "tend[ed] to accept cookie disclaimers blindly to get rid of it"); M. Nouwens et al., *Dark Patterns after the GDPR: Scraping Consent pop-ups and Demonstrating their Influence* (2020), https://dl.acm.org/doi/10.1145/3313831.3376321 ("[T]he frequency of the pop-ups caused frustration and consent fatigue.").

[117] Draft Regulations, § 7222, subd. (b).

[118] Draft Regulations, §§ 7022, subd. (b)–(c), 7023, subd. (f), 7024, subd. (h).

[119] Anthropic, *Mapping the Mind of a Large Language Model* (May 21, 2024), https://www.anthropic.com/research/mapping-mind-language-model.

[120] See J. Woods, *Machine Learning Interpretability: New Challenges and Approaches* (Mar. 14, 2022) Vector Institute, https://vectorinstitute.ai/machine-learning-interpretability-new-challenges-and-approaches/; See generally R. Dwivedi, *Explainable Ai (XAI): Core Ideas, Techniques, and Solutions* (2023), 55 ACM Computing Surveys, https://dl.acm.org/doi/10.1145/3561048.

of research devoted to this task has made promising advances.[121] But even when sophisticated researchers get a handle on how an advanced AI model works, their explanations have been long and jargon-filled.[122] And researchers have struggled to convert these explanations into a form understandable by non-expert humans.[123] So in many circumstances, any "plain language" explanation of the model's logic will be overly simplistic and misleading. It is never proper for the government to direct a business to mislead its customers.[124]

There is also ample reason to be concerned that such a disclosure regime could be misused to gain access to confidential business or consumer information. For example, it would be plainly inappropriate to compel the admissions office of a private college to disclose the "logic" and underlying "assumptions" of its admissions policy. A university may reasonably want to keep this information private, to prevent prospective students from gaming the system. But if a school implements or informs its admissions decisions in part using an automated system (as colleges fielding hundreds of thousands of applications necessarily will), it now may have to reveal exactly that confidential information.

Worse still, the disclosure requirements can be misused by malicious actors to gain unauthorized access to personal information. An unfortunately common scenario is that malicious actors use social engineering to obtain consumers' login credentials for a service.[125] Under a compelled-

[121] See Anthropic, *supra*; K. Wang et al., *Interpretability in the Wild: A Circuit for Indirect Object Identification in GPT-2 Small* (Nov. 1, 2022), https://arxiv.org/abs/2211.00593.

[122] See, e.g., Wang, *supra* (twelve technical pages to explain how a large language model predicted a single word in a sentence).

[123] See H. Siu et al., *STL: Surprisingly Tricky Logic (for System Validation)*, (May 26, 2023), https://arxiv.org/abs/2305.17258.

[124] Cf. *Barton v. Neeley* (6th Cir. 2024) 114 F. 4th 581, 592 (explaining that the First Amendment protects the "right to decide what to say and what not to say, and accordingly, the right to reject governmental efforts to require [someone] to make statements he believes are false"), and *Massachusetts Ass'n of Priv. Career Sch. v. Healey*, 159 F. Supp. 3d 173, 199–200 (D. Mass. 2016) (holding that a regulation requiring a business to make misleading statements was subject to heightened scrutiny under the First Amendment).

[125] See, e.g., Pavur & Knerr, GDPArrrrr: *Using Privacy Laws to Steal Identities*, Blackhat USA (2019), https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf (noting that "social engineers can abuse right of access requests as a scalable attack vector for acquiring deeply sensitive information about individuals"); IBM, *IBM Security X-Force Threat Intelligence Index 2024* at p. 9, https://www.ibm.com/reports/threat-intelligence (noting that "the focus has shifted towards logging in rather than hacking in, highlighting the relative ease of acquiring credentials compared to exploiting vulnerabilities or executing phishing campaigns"); *Verizon 2023 Data Breach Investigations Report* (2023) at p. 8, https://www.verizon.com/about/news/media-resources/attachment?fid=65e1e3213d633293cd82b8cb (noting that "74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering"); Stahie, *Billions of Leaked Credentials Available on the Dark Web*, Bitdefender (2020) (noting 15 billion credentials available on the dark web), https://www.bitdefender.com/en-us/blog/hotforsecurity/billions-of-leaked-credentials-available-on-the-dark-web.

disclosure regime, an attacker with these stolen credentials may now be able to learn even more information about his victim by obtaining the inferences a business has made about her and use that ill-gotten information in furtherance of identity theft or targeted phishing attacks. In this way, the regulations may be more harmful to privacy than enhancing of it.

D. There is no basis to require the onerous risk assessments

The Statement does not contain substantial evidence demonstrating that the extremely detailed and burdensome risk assessments are necessary to further consumers' privacy. Per the statute, the purpose of the risk assessment is to evaluate which instances of data processing have elevated "risks to privacy."[126] But many of the activities that must be addressed by the risk assessment have no impact on privacy at all. For example, the draft regulations would require each business to discuss the "completeness, representativeness, timeliness, validity, accuracy, consistency, and reliability" of its information sources and the "logic" of certain algorithms. None of these requirements bears any relationship to privacy or security concerns. The Statement does not explain otherwise.

Not only is there no evidence that risk assessments are necessary to advancing privacy and security, but the overbroad compliance regime proposed here would undermine privacy and security.[127] The risk assessments must address dozens of discrete issues. Undertaking such an extensive assessment anytime ADMT is used for a broad category of "significant decisions" would be enormously resource-intensive. Companies throughout the economy would need to divert resources, including engineering talent, away from substantive risk mitigation and toward producing burdensome risk assessments with little relation to privacy or security. The Statement denies any tradeoff with the blanket statement that "risk assessments are cost effective."[128] But its only source discusses not the regulations here, but the burdens of complying with Europe's GDPR, an entirely different set of requirements. And even with respect to those requirements, the source does not support the point: it acknowledged that the cost of the GDPR's data-protection assessments may already be "prohibitive," particularly for smaller companies that otherwise could

[126] Cal. Civ. Code, § 1987.1785(a)(14)(b).

[127] Nov. 8 CPPA Bd. Hr'g Tr. 99 ("With respect to the risk assessments, I think these proposed regulations will make the inclusion criteria for risk assessments so broad that we will end up hurting the cause of privacy, not helping it. The scope of these regulations effectively mandates risk assessments for almost any business using software. This spread will hurt businesses and overwhelm our agency with, I think, largely form paperwork, diminishing our focus – our ability to focus on enforcement. There's no chance we'll be able to review tens and tens of thousands of multi-page risk assessments at this stage with our current resources.").

[128] ISOR, p. 71–72.

substantially benefit from automation.[129] The Agency must promulgate regulations that balance the enhancement of privacy with the promotion of innovation, and since the risk-assessment requirements would do little to improve privacy and stifle innovation, the significant cost imposed by risk assessments is unsupported and unnecessary.[130]

E. There is no basis for the rigid cybersecurity audit requirements

The cybersecurity audit requirements are overly simplistic, in both when they apply and what they entail. The Statement of Reasons fails to show that the draft regulations' blunt requirements are necessary or appropriate.

The thresholds for when an audit is required are unjustified. The thresholds are based on blunt indicators, a business's revenue and number of consumers whose data is processed.[131] These simplistic conditions fail to account for how cybersecurity practices and the need for an audit vary across different industries. For example, strict compliance checklists may be appropriate for a mature institution with a predictable workflow, but counterproductive for a software company with a rapidly evolving product and headcount.[132] The draft regulations could lead to disproportionate compliance costs for businesses without lowering true risks to consumer security. The Statement does not address this concern.

[129] Iwaya et al., *Privacy Impact Assessments in the Wild: A Scoping Review* (2024), https://www.sciencedirect.com/science/article/pii/S2590005624000225.

[130] The risk assessments, as envisioned by the proposed regulations, also run afoul of the First Amendment. Courts have repeatedly rejected recent attempts to require disclosures about a company's use of technology and its opinions on whether and how this use maps to ambiguous and often pejorative characterizations. The Ninth Circuit made this point twice in just the last year while striking down remarkably similar California laws. In one case, the law demanded, akin to the present regulations, that certain website operators report on whether "the design of the[ir] online product . . . could harm children" in various specific ways. (*NetChoice v. Bonta* (9th Cir. 2024) 113 F. 4th 1101, 1109.) The requirement was invalid because it compelled "covered businesses to opine on potential harm" of their product outside the context of any specific transaction. In the other case, the State compelled businesses to "implicitly opin[e] on whether and how certain controversial categories of content should be moderated." (*X Corp. v. Bonta* (9th Cir. 2024) 116 F. 4th 888, 901.) Yet this request too was invalid, because the government had no authority to make a company offer "opinions about and reasons for" its policies. The only difference here is that there is nothing "implicit" about what the new regulation asks for. It flat-out tells companies to express an opinion on whether or not their technology fits within the vague and value-laden categories in the regulations and, if so, the merits and drawbacks of their own policies. But this is well past the range of speech that a government can legitimately compel.

[131] Draft Regulations, § 7120.

[132] Wallace, *The Importance of Cybersecurity by Industry*, https://www.uscybersecurity.net/the-importance-of-cybersecurity-by-industry; Cristiano and Prenio, *Regulatory approaches to enhance banks' cyber-security frameworks* (2017), https://www.bis.org/fsi/publ/insights2.pdf.

And when audits are required, the mandated components are problematically rigid. The particular approaches that work in one industry or for one particular size of business may backfire elsewhere.[133] Moreover, the detailed cybersecurity audit requirements set forth in the regulations – including dozens of discrete requirements – would, at best, introduce a box-checking exercise and, at worst, distract businesses from focusing on actually optimizing security and keeping sensitive information safe.[134]

III. The Proposed Regulations Lack Clarity

Regulations must be easy to understand and follow,[135] and "due process also requires that regulations be written with sufficient clarity so that those subject to the law can understand what is required or prohibited."[136] But complying with the proposed regulations will require herculean guesswork. The regulations leave California businesses to puzzle over whether and when the regulations apply and, if they do, how to comply.

First, the **definition of ADMT** is troublingly vague. The flexible terms "execute," "substantially facilitate," and "key factor" provide little guidance to businesses about what qualifies as ADMT. It may be difficult to assess whether a particular output of a technology plays a "substantial" or "key" role in a decision, particularly when the technology merely informs human decisionmaking; there may be no agreed-upon way to quantify the weight that a factor plays in a human decision. The examples only compound this indeterminacy. Section 7001(f)(2) states that ADMT "substantially facilit[es] human decisionmaking" when it is used "to generate a score about a consumer that a human reviewer uses as a primary factor to make a significant decision." But in Section 7001(f)(4), the regulations indicate that using technology to "calculate" a "score that [a] manager will use to determine which [employee] will be promoted" is not even a use of ADMT. The regulation appears to discern between "generating a score" for the purpose of guiding a human

[133] Etoom, *Strategising cybersecurity: Why a risk-based approach is key* (2023), https://www.weforum.org/stories/2023/04/strategizing-cybersecurity-why-a-risk-based-approach-is-key/; Boehm et al., *The risk-based approach to cybersecurity* (2019), https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity.

[134] Marotta and Madnick, *Convergence and divergence of regulatory compliance and cybersecurity* (2021), https://doi.org/10.48009/1_iis_2021_10-50 ("regulatory compliance can negatively affect cybersecurity"); Sjouwerman, *5 Reasons Why Compliance Alone Is Not Efficient at Reducing Cyber Risks* (2022), https://www.corporatecomplianceinsights.com/compliance-not-enough-cybersecurity-risk/; Internet Security Alliance, *Cyber Regulations Are Counter-Productive to True Security* (2021), https://isalliance.org/cyber-regulations-are-counter-productive-to-true-security/.

[135] Gov. Code, § 11349, subd. (c); *FCC v. Fox Television Stations, Inc.* (2012) 567 U.S. 239, 253 (same under Due Process clause).

[136] See *FCC v. Fox Television Stations, Inc.* (2012) 567 U.S. 239, 253.

decision and "calculating a score" for that same purpose, but without any meaningful explanation of how the two are different.

Section 7001(f)(4) likewise creates confusion as to what "technology" is in scope. It alternately says that "calculators," "spreadsheets," and "similar technologies" are *not* ADMT, then asserts that the "use of a spreadsheet to run regression analyses" *is* ADMT if used by humans evaluating job performance, but then says that it is *not* ADMT if it "merely . . . organize[s] human . . . evaluations." As we noted above, the distinction between "regressions" and "calculators" is wholly unclear, and a business has little hope at guessing which side of the line its software falls on. The Agency's attempt to explain the regulation only adds confusion because "the language of the regulation conflicts with the agency's description of the effect of the regulation."[137] These artificial distinctions underscore the unworkability and ambiguity of the proposed definition of ADMT.

Second, **the term "significant decision**" also lacks clarity. The specific categories that count as "significant" are problematically vague. For example, what does it even mean for a decision to "result[] in access to, or the provision or denial of . . . criminal justice"? The regulations do not say, beyond offering the single example of the "posting of bail bonds." Suppose a security firm guarding a semiconductor factory uses an AI tool to decide which visitors must go through extra screening. Since the security screening could theoretically discover evidence of a crime and lead to a prosecution, does the company's use of AI fit the definition? It is likewise unclear what decisions count as affecting "housing." If a college assigns roommates using software that considers students' personal preferences, does it have to conduct a risk assessment and offer an opt-out? Or does housing extend only to the purchase or lease of real property? And what counts as an "essential good or service"? The regulations provide a handful of examples (groceries, medicine, hygiene products, or fuel) but what else should be considered "essential" and how is that decided? Is Internet access essential? Cultural opportunities? Firearms? And even if a good is unequivocally "essential," which decisions affect "access" to it? Do the regulations cover every single transaction related to that good (for example, a grocery store's denying a consumer access to one particular foodstuff on one occasion)? Or does a decision count only when it wholesale excludes a consumer from the good (like if the only utility company that services a consumer's home disconnects the power)? The proposed definition of "significant decision" creates more questions than it answers.

[137] Office of Administrative Law, OAL Review for Compliance with the Six Substantive Standards of the Administrative Procedure Act, § 3.03 (Apr. 2023), https://oal.ca.gov/wp-content/uploads/sites/166/2023/04/OAL-Review-for-6-APA-Standards.pdf.

Third, the proposed **pre-use notice** and **right to access** regulations likewise fail to explain how those disclosures would function. The pre-use notice and any response to a request to access may not "describe the purpose in generic terms" and must include information about the logic, key parameters, and output of the ADMT, which must be in "plain language." But, as discussed above, automated decisionmaking technology, including artificial intelligence, often involves dynamic and constantly evolving, highly technical systems that can consider hundreds of inputs of variable weights that lead to a range of different outputs. And businesses may be constantly tweaking and testing their technology to optimize for different circumstances or to account for changes in the marketplace. And as discussed above, translating any given iteration of an ADMT system into plain English may be an impossible task. The regulations provide no guidance on how to provide accurate and digestible information given this highly complex backdrop.

*   *   *

We appreciate this opportunity to share some of our concerns with the Agency and hope that the Agency will revise the proposed regulations to focus on the privacy and security concerns expressed by the People of California in approving Prop. 24.

Respectfully submitted,

[redacted]

Ashlie Beringer
Partner
Co-Chair of the Privacy, Cybersecurity and Data Innovation Practice Group

[redacted]

Jane Horvath
Partner
Co-Chair of the Privacy, Cybersecurity and Data Innovation Practice Group

[redacted]

Cassandra Gaedt-Sheckter
Partner
Co-Chair of the Artificial Intelligence Practice Group

Grenda, Rianna@CPPA

From:	Gig Workers Rising <info@gigworkersrising.org>
Sent:	Tuesday, February 18, 2025 11:42 AM
To:	Regulations@CPPA
Subject:	Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments:	2-18-25-GWR-Comment-Letter.pdf

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Attached is the written comment submitted on behalf of Gig Workers Rising.

GIG WORKERS RISING

February 18, 2025

Submitted by Email to: regulations@cppa.ca.gov

California Privacy Protection Agency
2101 Arena Boulevard
Sacramento, CA 95834

Re: Public Comment on Risk Assessments and ADMT

Dear Board Members, Executive Director, and Agency Staff,

Gig Workers Rising ("GWR") appreciates the opportunity to provide recommendations in response to the California Privacy Protection Agency's request for comments on proposed regulations for the California Consumer Privacy Act ("CCPA"). We commend the Executive Director, Agency staff, and members of the Board for their commitment and dedication to giving guidance to California businesses, consumers, and now workers on the most important and consequential data privacy policy in the U.S.

GWR is a campaign of Working Partnerships USA that supports app-based workers who are organizing for better wages, working conditions, and respect on the job. GWR has been empowering drivers and delivery workers across the San Francisco Bay Area since 2018, and has organized countless meetings, listening sessions, protests, and actions. GWR continues to support app-based workers as they organize for better wages, a seat at the table, and safer working conditions.

For union and non-union workers alike, the emergence of AI and other data-driven technologies represents one of the most important issues that will shape the future of work in California for decades to come, potentially affecting workers' privacy, race and gender equity, wages and working conditions, job security, health and safety, right to organize, and autonomy and dignity.

By covering worker data in the CCPA and in the promulgation of regulations, California has a historic opportunity to lead the U.S. in establishing workers as key stakeholders in decisions about how best to govern artificial intelligence and related technological innovation—and in particular, to ensure that workers have the ability to control the collection and use of their personal data.

GWR has signed onto a joint letter, submitted under separate cover, with detailed recommendations, which include: (1) expanding the definition of automated decision-making technology ("ADMT"), (2) strengthening notice and access rights for workers when an employer has used ADMT about them, (3) restoring a meaningful right for workers and consumers to opt out of consequential ADMT systems, (4) strengthening the required elements of risk assessments, and (5) clarifying the roles of workers and unions in risk assessments.

In this letter, we would like to share with you stories from our worker members about how data-driven technologies—particularly automated or "robo-firings"—are impacting their work lives, underscoring why fully protecting workers in these new regulations is so important. App-based companies call these robo-firings "deactivations," but it's essentially being fired by an automated message on your phone. Imagine going to work one day to find that you can't get in because your key no longer works. You never get any explanation and probably can't even talk to a person—that's what it's like to be deactivated.

David[1] has been driving for Uber and Lyft in California's Bay Area for over two years. David drives almost every day, sometimes as many as 12 or 13 hours. One day, David was picking up and dropping off passengers as usual, and took a break to eat his lunch. When David turned the app back on, he was shocked to discover that Uber had suddenly deactivated his account.

David had no idea what happened, so he went to Uber's office in Oakland. It turns out that someone had tried to open a fake account using David's information, so Uber decided to deactivate his account and cut him off from work. When David spoke to Uber's representatives, they told David that he needed to file an identity theft report with the police. In the meantime, Uber would start an investigation that could take up to 3 months to resolve.

David filed the police report and submitted all the relevant documents Uber had requested to complete its investigation. A week later, Uber asked for more information and David gave it to them. Then another month passed and Uber asked for the same information.

David decided to go to Uber's office again. Apparently, a piece of information in the documents David had submitted was not visible, so the investigation hadn't even started yet. At this point, David had already spent over a month cut off from his job, waiting for Uber to investigate and reactivate his account.

Deactivations like David's happen all too often to drivers who rarely have transparency or a clear appeal process to get our accounts back. In David's words, "We spend hours in our cars doing the hard work for these corporations, but we can lose our jobs in the blink of an eye."

Robert is an Uber and Lyft driver who has completed thousands of rides with satisfied passengers in California's Bay Area for over a decade. But all it took was a misunderstanding with one passenger for Lyft to permanently deactivate Robert.

Two years ago, Robert was asked to pick up a passenger on a packed street. The passenger asked Robert to drive right up to him to do the pick-up. Robert explained that he

[1] All the first names of drivers in this letter have been changed to protect the worker.

could not because it was so crowded. He asked the passenger to come to him. The passenger flipped Robert off. Fearful of letting the passenger into his vehicle, Robert drove away.

Robert stopped by the store. When he turned the app back on to provide his next ride, he was shocked to discover that Lyft had deactivated him. Robert would not be allowed to log-on again until the company had completed a full review.

Robert didn't know why he was deactivated. He drove over an hour to Lyft's office in Oakland to find out. At the office, Lyft told Robert that the passenger had accused Robert of discrimination. Lyft said they were going to have someone call him from the company.

Lyft called Robert. Robert tried to tell his side of the story, but felt like the company did not give him a fair chance to do so. Instead, the company said that it had made the decision to permanently deactivate him. Robert was at a loss to understand the basis of Lyft's findings.

The harmful impacts of sudden and arbitrary deactivations impact not only drivers who are deactivated, but also drivers who are discouraged and intimidated from reporting health and safety and other serious incidents with passengers, due to the ever-present fear of deactivation.

Sandra has been an Uber and Lyft driver in the San Francisco Bay Area for over seven years. She has experienced multiple incidents in which male passengers—often intoxicated—would sexually harass her while she was driving.

One time, after Sandra had finished giving a passenger his ride, the passenger re-entered the car, pulled the driver's seat back, got close to her face, and said he wanted her number so he could ask out for a date. Usually, Sandra tries to manage these situations by giving the passenger a fake number to write down. This time, however, the passenger refused. He insisted that Sandra input her number into his phone. He wanted to immediately call and double-check that it was truly her number.

Sandra tried to tell the passenger that she was going to be late picking up another ride, but the passenger wouldn't budge. He said he wouldn't get out of her car until he could call and see that her phone was ringing.

Fearful the situation would escalate further, Sandra gave him her number. Only after the passenger had called and seen that Sandra's phone was ringing, did he finally relent and leave the car.

Sandra felt like she couldn't afford to report the incident to the company. At the time, her customer satisfaction rating was lower than normal, and she was feeling vulnerable. She worried that if she reported the incident, the customer would turn the tables by making a false accusation against her. She had heard many stories of drivers who had been deactivated for less. Sandra felt she had no choice but to keep silent.

Unfortunately, stories like David's, Robert's and Sandra's, are all too common. Unjust deactivations and other forms of arbitrary ADMT cost workers not only their livelihoods—but their lives. A 2023 survey of over 810 current and former Uber and Lyft drivers in California found that **two-thirds** of all surveyed drivers had experienced deactivation.[2] A 2023 national survey of over 900 Uber and Lyft drivers found that **59%** of surveyed drivers said they had accepted a ride when they felt unsafe, fearing negative reviews leading to deactivation.[3] **Thirty-one** app-based drivers and delivery workers were murdered on the job in 2022 alone.[4]

The experiences of app-based drivers are a preview of the conditions that all workers will be facing unless strong guardrails and protections are put in place. It is estimated that over 80% of employers use some type of artificial intelligence or algorithms to assist with human resource functions.[5] The U.S. workplace is rapidly becoming a major site for the deployment of AI and other digital technologies, a trend that will only escalate going forward.

Full coverage and protection by the CCPA are critical first steps to ensure that California workers have the tools necessary to advocate for their rights in the 21st century data-driven workplace. Thank you for the opportunity to provide feedback during this important rulemaking process.

Sincerely,

[redacted]

Cesar Palancares
Lead Organizer
Gig Workers Rising/Working Partnerships USA

[2] Asian Americans Advancing Justice and Rideshare Drivers United, *Fired by an App: The Toll of Secret Algorithms and Unchecked Discrimination on California Drivers,* p. 4, https://www.asianlawcaucus.org/news-resources/ guides-reports/fired-by-an-app-report. Accessed 12 Feb. 2025.

[3] Strategic Organizing Center et al. *Driving Danger: How Uber and Lyft create a safety crisis for their drivers,* April 2023, p. 12–13, https://thesoc.org/wp-content/uploads/sites/342 /SOC_ RideshareDrivers_ rpt-042023.pdf. Accessed 12 Feb. 2025.

[4] Gig Workers Rising and Action Center on Race and the Economy, *Murdered Behind the Wheel,* May 2023, p. 5, http://www.datocms-assets.com/64990/1686088796-gig-safety-now 06-2023.pdf. Accessed 12 Feb. 2025.

[5] Creighton, Myra et al. "Federal Agencies Say Employer Use of AI and Hiring Algorithms May Lead to Disability Bias: 5 Key Takeaways," *JD Supra,* May 17, 2022, https://www.jdsupra.com/ legalnews/federal-agencies-say-employer-use-of-ai-3863045/. Accessed 12 Feb. 2025.

Grenda, Rianna@CPPA

From:	Elizabeth Banker <bankere@google.com>
Sent:	Wednesday, February 19, 2025 12:33 PM
To:	Regulations@CPPA
Subject:	Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments:	Google Cyber, Risk, ADMT Comments.pdf

This Message Is From an External Sender

WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

I am submitting the attached comments on the proposed regulations on CCPA Updates, Cyber, Risk, ADMT, and insurance. Please let me know if you have any questions or issues with the attachment.

Best,
Elizabeth

--

To help protect your privacy, Microsoft Office prevented automatic download of this picture from the Internet.

Elizabeth Banker [she/her]
Government Affairs & Public Policy
bankere@google.com | 415.523.0142

February 19, 2025

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

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

To whom it may concern:

Please find below Google's comments on the California Privacy Protection Agency's ("Agency") proposed regulations announced in the proposed rulemaking dated November 22, 2024[1], related to automated decisionmaking technology, risk assessments, and other updates to the existing regulations issued pursuant to the California Consumer Privacy Act ("CCPA"). We thank the Agency for the opportunity to provide comments on these proposed regulations (herein "Proposed Regulations") and we would welcome the opportunity to discuss these topics with you.

I. Introduction and General Considerations.

In our prior comments on proposed rulemaking under the CCPA, we suggested three overarching principles to guide the Agency in delivering effective privacy protections for Californians:

1. Prioritize clarity around obligations under the statute over introducing new, additional obligations not expressly required by the law;
2. Provide flexibility where possible about how to comply with the law in a manner that prioritizes substance over form; and
3. Seek to align rules with existing national and global standards to facilitate consumer understanding and promote privacy-preserving business practices.

These same priorities should guide the Agency in meeting its statutory obligations to issue regulations concerning the topics at issue in this proceeding, as detailed further below.

1. Prioritize clarity around obligations under the statute over introducing new, additional obligations not expressly required by the law. While the CCPA mandates that the Agency issue regulations "governing access and opt-out rights with respect to businesses' use of automated decision-making technology" and requiring businesses "whose processing of consumers' personal information presents significant risk to consumers' privacy or security" to conduct risk assessments,[2] this statutory mandate does not require the highly detailed requirements reflected in the Proposed Regulations. Instead, as we explain below, the Agency can meet its statutory mandate with higher-level rules that still serve sound policy goals and protect the privacy of California consumers.

[1] *See* California Privacy Protection Agency - Notice of Proposed Rulemaking (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations) (published Nov. 22, 2024).
[2] Cal. Civ. Code §§ 1798.185(a)(15), 1798.185(a)(14).

2. Provide flexibility where possible about how to comply with the law in a manner that prioritizes substance over form. The CCPA's stated purpose is to "strengthen[] consumer privacy, while giving attention to the impact on business."[3] This objective is best achieved through flexible standards that allow businesses to efficiently deliver on their legal obligations and build privacy and security programs that meet global norms. The Proposed Regulations diverge from this objective by taking a prescriptive approach that elevates form over substance. For example, businesses would be required to present elaborate "pre-use" notices before collecting personal information that *could* be processed for a wide range of decisions, many of them inconsequential to consumers, or to train systems that could be used for such purposes. Similarly, a highly detailed checklist for conducting risk assessments would be imposed on businesses even when the checklist has little relevance to the business's practices. These obligations may work against consumers' privacy interests by diverting compliance resources from substantive privacy programs to the creation of "cookie-cutter" notices and paper-pushing exercises. We urge the Agency to favor more flexible rules that protect consumers and serve the policy goals of the CCPA.

3. Where possible, seek to align rules with existing national and global standards to facilitate consumer understanding and promote privacy-preserving business practices. With respect to the implementation of the law, the CCPA directs that "[t]o the extent it advances consumer privacy and business compliance, the law should be compatible with privacy laws in other jurisdictions."[4] Despite this directive, the Proposed Regulations materially diverge from existing privacy laws, including Europe's General Data Protection Regulation[5] ("GDPR") and consumer privacy laws enacted by 19 other states, in ways that are neither supported by the CCPA statutory text nor beneficial to consumer privacy interests, business compliance needs, or other policy interests. The Proposed Regulations would require companies to adopt California-specific notices, user choices, and risk assessment processes while implementing different notices, choices, and risk assessment processes to ensure compliance with other state laws. This approach would undermine consumer understanding and impose substantial compliance costs. We urge the Agency to consider standards adopted by other states and internationally, both in the context of risk assessments and the triggers and requirements governing the use of ADMT, topics for which the Proposed Regulations are far outside of the consistent norms that have emerged in other jurisdictions.

Finally, it is critical that the Agency account for the Legislature's active consideration of the appropriate regulation of AI, including automated decisionmaking technologies, and ensure that its rules do not restrict broader legislative solutions to both regulate AI and promote its safe growth. Google strongly supports responsible development and deployment of AI and similar technology and has advocated for regulations to govern it.[6] As the Agency knows, the Legislature is actively considering the appropriate

[3] *Id.* § 1798.199.40(*l*).

[4] California Privacy Rights Act of 2020, Prop. 24 § 3(C)(8) (2020) (codified at Cal. Civ. Code § 1798.100).

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (GDPR).

[6] For more on Google's positions on responsible AI, *see A Policy Agenda for Responsible Progress in Artificial Intelligence*, GOOGLE (2023), https://www.google.com/url?q=https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/A_Policy_Agenda_for_Responsible_Progress_in_Artificial_Intelligence.pdf&sa=D&source=docs&ust=1736258974414893&usg=AOvVaw2uXAsqBo9mVJQUTJn9loYl; *Generative AI and Privacy Policy Recommendations Working Paper,* GOOGLE (June 2024),

regulation of many facets of AI, including automated decisionmaking technologies. Similarly, the Agency should be mindful of Governor Newsom's admonition that AI regulations should be empirically-grounded, protect the public from real threats, and not curtail beneficial innovation.[7]

For the Agency's consideration, below Google suggests revisions to the Proposed Regulations and describes how such changes would more closely align the Proposed Regulations with these principles.

II. The Agency Should Prioritize Issues Within Its Statutory Mandate and Avoid Expansive Restrictions on AI that Will Disrupt Efforts by the Legislature and Governor to Craft Nuanced AI Regulations.

Aspects of the Proposed Regulations would seek to regulate AI in ways that are out of step with the CCPA and sound policy considerations. For example, the Proposed Regulations would define "automated decisionmaking technology" (ADMT), many uses of which are subject to extensive notice, opt-out, and risk assessment obligations, to include the broadly defined concept of "artificial intelligence." The Proposed Regulations would also impose similar obligations on businesses that train "automated decisionmaking technology *or artificial intelligence*," thereby suggesting a potential intent to regulate the training of AI even when it is not used to make any decisions at all -- a result that reaches beyond the Agency's remit to issue regulations governing "businesses' use of [ADMT]," but not technologies that do not make decisions. Further, attempting to bolt AI-specific requirements onto the CCPA is particularly likely to have unexpected and undesirable consequences because the CCPA lacks critical foundational concepts for regulating AI, such as distinctions between high- and low-risk systems and between the obligations for developers and deployers of AI models.[8] The Agency should leave this delicate task to California lawmakers as part of their broader deliberations regarding the regulation of AI.

Suggested Changes: To keep its rulemaking consistent with the CCPA and avoid wading into critical AI policy debates, the Agency should delete "or artificial intelligence" from the definition of "train automated decisionmaking technology or artificial intelligence" in § 7001(fff) (and all subsequent references thereto). The Agency should also consider deleting the reference to "artificial intelligence" from the definition of ADMT set forth in § 7001(f)(1); alternatively, to the extent the Agency does maintain AI as a subset of ADMT, it should define that term in alignment with federal law.[9]

https://www.google.com/url?q=https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Google_Generative_AI_and_Privacy_-_Policy_Recommendations_Working_Paper_-_June_2024.pdf&sa=D&source=docs&ust=1736258974423961&usg=AOvVaw17C28UmWksl7HqgLpJgWHf.

[7] *See* Office of the Governor, Statement on Veto of S.B. 1047 (Sept. 29, 2024), https://www.gov.ca.gov/wp-content/uploads/2024/09/SB-1047-Veto-Message.pdf.

[8] *See, e.g.*, Artificial Intelligence Act, 2024 O. J. (L. 1689); Colorado AI Act, 2024 Colo. Legis. Serv. Ch. 198 (West) (codified at Colo. Rev. Stat. §§ 6-1-1701 - 1707).

[9] *See, e.g.*, National Artificial Intelligence Initiative, 15 U.S.C. § 9401 (defining AI as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action.; Cal. Gov't Code § 11546.45.5(a)(1) (defining AI as "an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments").

III. The Agency Should Refine the Triggers for ADMT Obligations and Risk Assessments to Focus on High-Risk Activities, Consistent with Global Norms.

Google agrees that automated decisions that have certain consequential effects on consumers, such as decisions that involve the provision or denial of credit, insurance, healthcare, educational enrollment, employment opportunities, or criminal justice, may deserve heightened protections and process. Focus on these types of impactful automated decisions would be consistent with the Agency's legislative mandate as well as laws adopted in other jurisdictions in the U.S. and abroad.

The Proposed Regulations, however, would reach far beyond such consequential decisions, imposing highly prescriptive obligations and triggering an obligation to conduct detailed risk assessments when using nearly *any* technology as even a *single factor* (even when backed by human intervention) to make comparatively insignificant decisions, such as decisions about what ads to show a consumer based on first-party data. They would also apply to the training of any technology that is "capable" of being used for myriad purposes and potentially create significant roadblocks to the use of ADMT for entirely consumer-protective purposes, including fraud prevention, security, and safety. The broad scope of these obligations goes well beyond the global norms upon which the CCPA was modeled, without a statutory mandate to do so, and with no clear benefit to consumers. If adopted as currently drafted, the Proposed Regulations would prioritize pro forma paper-pushing exercises and notices that consumers are unlikely to read or comprehend over more precise and streamlined requirements that can better protect against consumer harm. Additionally, as discussed below, the Proposed Regulations are likely to lead to a barrage of notices and related notice "fatigue," prompting disregard of ADMT notices, even when they warn of consequential decisions, and potentially other privacy-related notices.

As detailed below, we urge the Agency to instead impose ADMT-specific obligations and trigger an obligation to conduct risk assessments only when a business uses ADMT *alone* to make significant decisions that materially affect consumers' lives or livelihoods.

A. The Agency Should Regulate ADMT Only if It Is Used to Replace Human Decisionmaking Entirely.

The Proposed Regulations would regulate use of technologies to "substantially facilitate" human decisionmaking, defining that concept as "using the output of the technology as a key factor in a human's decisionmaking."[10] As noted in the Proposed Regulations, this broad scope includes common technologies, such as spreadsheets when used to assist humans in doing basic math such as regression analyses.[11] This approach is inconsistent with the CCPA and goes well beyond other privacy laws, which properly recognize that human intervention is already regulated by longstanding laws prohibiting discrimination on the basis of protected class and serves a critical backstop to preventing the sort of harms that automated decisionmaking regulation is designed to prevent. For example, the GDPR imposes special obligations on automated decisions only where such decisions are based "solely" on automated processing.[12]

[10] Proposed Regulations § 7001(f)(2).

[11] Proposed Regulations § 7001(f)(4).

[12] GDPR art. 22(1).

The CCPA gives the Agency authority to issue regulations governing “businesses’ use of automated decisionmaking technology.”[13] Implicit in this mandate is that the *technology* (not humans) actually *makes* decisions (and does not merely “substantially facilitate” the decisionmaking); decisions made with human intervention are not “automated” ones and thus fall outside the scope of ADMT rulemaking. Nor is there any policy justification for regulating, for example, employers using spreadsheets with computation functionality any more than those using analog calculators. Requiring the former to present prominent notice and, depending on their exact configuration, potentially an opt out, while allowing the latter to avoid the law’s obligations will lead to consumer confusion and substantial compliance costs with no corresponding consumer benefit.

Suggested Changes: To address these concerns and ensure that the regulations are consistent with the CCPA and its policy goals, we encourage the Agency to revise the definition of ADMT and limit the uses of ADMT that trigger special obligations as shown below.

§ 7001(f): “Automated decisionmaking technology” or “ADMT” means any technology that processes personal information and uses computation to execute a decision in a way that~~,~~ replaces human decisionmaking~~, or substantially facilitate human decisionmaking~~.

(1) For purposes of this definition, “technology” includes software or programs, including those derived from machine learning, statistics, or 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~~2) Automated decisionmaking technology includes profiling, when used to execute a decision that replaces human decisionmaking.
(~~4~~3) Automated decisionmaking technology does not include use of ~~the following~~ technologies~~, provided~~ that merely ~~the technologies do not execute a decision, replace human decisionmaking, or substantially~~ facilitate human decisionmaking or~~:~~ web hosting, domain registration, networking, caching, website-loading, data storage, firewalls, anti-virus, anti-malware, spam- and robocall-filtering, spellchecking, calculators, databases, spreadsheets, or similar technologies~~. A business must not use these technologies to circumvent the requirements for automated decisionmaking technology set forth in these regulations. For example, a business’s use of a spreadsheet to run regression analyses on its top-performing managers’ personal information to determine their common characteristics, and then to find co-occurrences of those characteristics among its more junior employees to identify which of them it will promote is a use of automated decisionmaking technology, because this use is replacing human decisionmaking. By contrast, a manager’s use of a spreadsheet to input junior employees’ performance evaluation scores from their managers and colleagues, and then calculate each employee’s final score that the manager will use to determine which of them will be promoted is not a use of automated decisionmaking technology, because the manager is using the spreadsheet merely to organize human decisionmakers’ evaluations~~.

§ 7200(a): A business that uses automated decisionmaking technology ~~in any of the following ways must comply with the requirements of this Article: (1) For~~ as the sole basis ~~F~~for making a significant decision concerning a consumer must comply with the requirements of this Article:

[13] Cal. Civ. Code § 1798.185(a)(15).

§ 7150(b): Each of the following processing activities presents significant risk to consumers' privacy: (3) Using automated decisionmaking technology as the sole basis to make ~~for~~ a significant decision concerning a consumer ~~or for extensive profiling~~.

B. The Agency Should Regulate Only Decisions that Have Consequential Effects.

Beyond regulating an unprecedented scope of technologies that play some role in facilitating decisionmaking, the Proposed Regulations would also impose rigid notice, opt-out, access, and risk assessment obligations on businesses that use technologies to make inconsequential decisions concerning consumers, e.g., the ads they are shown for basic consumer products using solely first-party data. While regulating ADMT used to make consequential decisions is consistent with global norms and backed by sound policy rationale, regulating "extensive profiling" and training of ADMT systems—even where simply "capable" of making these or other decisions—would reach much further, capturing common activities specifically *excluded* from heightened regulation by the statute, such as first-party advertising.[14] This broad scope is inconsistent with the CCPA, is contrary to norms that have emerged across other privacy regimes, and would undermine consumers' privacy interests.

Global privacy standards reflect a consensus that use of automated decisionmaking requires additional protections only when used to make decisions that produce "legal or similarly significant effects."[15] With respect to risk assessments specifically, beginning with the GDPR and since amplified by consumer privacy laws enacted by 19 states, a consensus has emerged that companies must undertake these assessments when processing is "likely to result in a high risk to the rights and freedoms" of individuals or "present a heightened risk of harm" to consumers.[16] The CCPA reflects a similar, well-grounded, limitation—the Agency is empowered to issue regulations concerning risk assessments only where businesses' processing of personal information "presents significant risk to consumers' privacy or security."[17] A global consensus has also developed around the types of activities that may meet this bar—specifically, in addition to processing to make decisions that produce legal or similarly significant effects, sales of personal data, certain processing of sensitive personal information, and sharing of personal data for activities that amount to cross-context behavioral advertising.[18] By subjecting use of ADMT for inconsequential decisions to the same heightened requirements as these other decisions, the Proposed Regulations would depart from this global standard and from the CCPA's mandate of compatibility with other privacy laws.[19]

Beyond this, the scope of decisions covered by the Proposed Regulations would result in consumers being inundated with confusing and redundant notices and choices for practices that do not meaningfully impact their lives. This approach will result in notice fatigue that may cause consumers to swipe away warnings without reading them. Reserving detailed notice requirements for use of ADMT for significant decisions that impact consumers' lives and livelihoods would help focus consumer

[14] Proposed Regulations § 7200(a)(2)(C).

[15] *See, e.g.*, GDPR art. 22; Maryland Online Data Protection Act § 14-4605(B)(7)(3), 2024 M.D. Laws 454; Florida Digital Bill of Rights, Fla. Stat. Ann. § 501.705(2)(e)(3) (West 2024); 4 Colo. Code Regs. § 904-3:9.02; Ky. Rev. Stat. Ann. § 367.3615(2)(e); 6 R.I. Gen. Laws Ann. § 6-48.1-5(e)(4).

[16] GDPR art. 35(1); *see also, e.g.*, Colorado Privacy Act, Colo. Rev. Stat. Ann. § 6-1-1309(1) (mandating assessments for processing that "presents a heightened risk of harm" to a consumer).

[17] Cal. Civ. Code § 1798.185(a)(14).

[18] *See, e.g.*, Colo. Rev. Stat. Ann. § 6-1-1309(2); Conn. Gen. Stat. Ann. § 42-522(a).

[19] California Privacy Rights Act of 2020, Prop. 24 § 3(C)(8) (2020) (codified at Cal. Civ. Code § 1798.100)

attention and foster meaningful understanding and engagement with controls where processing potentially presents material risk.

Similarly, obligations related to the use of ADMT should be triggered only on businesses that *actually use* ADMT to make significant decisions, rather than on every technology that merely *could* be used for such purposes. The rulemaking called for by the CCPA is notably limited to regulations regarding the "use" of automated decision-making technology,[20] not the "potential use" of automated decision-making technology, or the use of "technology" that is "capable of automated decision-making." Appropriately limiting triggers for ADMT obligations also makes good policy sense and is consistent with global privacy norms. Basic AI tools like chatbots, analytics technology, and even automated spreadsheets can be "capable" of being used to produce decisions that can have significant impacts on consumers. Nevertheless, global norms appropriately reserve special obligations for use of technologies to actually make such decisions. Similarly, basic photo editing tools that consumers have used for decades "could" be used to create a deepfake, and yet no privacy regulation passed to date has suggested that such commonly used tools should be subject to special regulation as a result.

Suggested Changes: The Agency should delete "extensive profiling" (§ 7200(a)(2) and § 7150(b)(3)(B)) and also delete training of ADMT or AI (§ 7200(a)(3) and § 7150(b)(4)) as triggers for ADMT or risk assessment obligations. To correspond with those changes, the Agency should modify the example set forth in § 7150(c)(4) as follows: "Business D provides a personal-budgeting application into which consumers enter their financial information, including income. Business D seeks to display advertisements to these consumers on different websites for payday loans that are based on evaluations of these consumers' personal preferences, interests, and reliability. Business D must conduct a risk assessment because it seeks to ~~conduct extensive profiling and~~ share personal information."

Finally, requirements in the Proposed Regulations tied to technology "capable of" particular processing should be deleted. For example, to the extent the Agency retains triggers for ADMT or risk assessments other than for "significant decisions," including related to training of ADMT, it should omit the opaque and overly broad "capable of" standard (and should also revise the example set forth in § 7150(c)(6) to make clear that training is only problematic if it is actually used to identify consumers) as follows:

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

(A) For a significant decision concerning a consumer;

(B) To establish individual identity; or

(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~~.

[20] Cal. Civ. Code § 1798.185(a)(15).

§ 7150(c)(6): "Business F is a technology provider. Business F seeks to extract faceprints from consumers' photographs to train Business F's facial-recognition technology. If Business F uses this facial-recognition technology to establish individual identity, it must conduct a risk assessment because it seeks to process consumers' personal information to train automated decisionmaking technology ~~or artificial intelligence~~ that is ~~capable of being~~ used to establish individual identity."

§ 7200(a)(3): "For training uses of automated decisionmaking technology, which are processing consumers' personal information to train automated decisionmaking technology that is intended to be ~~capable of being~~ used for any of the following:

(A) For a significant decision concerning a consumer;

(B) To establish individual identity; or

(C) For physical or biological identification ~~or profiling~~.~~; or~~

~~(D) For the generation of a deepfake."~~

C. Use of Personal Information to Select Ads Based on Solely First-Party Data Should Not Trigger ADMT or Risk Assessment Obligations.

If the Agency elects not to remove the concept of "extensive profiling" as a trigger for ADMT and risk assessment obligations entirely, it should, at minimum, omit "behavioral advertising" as an activity that triggers such obligations. The proposed definition of "behavioral advertising" in the Proposed Regulations excludes only contextual advertising—ads based solely on a consumer's personal information derived from the consumer's *current* interaction with the business—and expressly includes targeting advertising to a consumer based on the consumer's personal information obtained entirely from the consumer's activity on the businesses' own properties.[21] The Proposed Regulations' approach of imposing substantial notice, access, and opt-out obligations on such processing of personal information collected in a first-party context will inundate consumers with rote and potentially confusing and redundant notices that they will swipe away, which risks causing them to miss or ignore such notices for potentially high-risk and impactful processing, including when ADMT is used to make legal or other significant decisions about them.

More fundamentally, the Proposed Regulations would perversely treat first-party advertising as more privacy-invasive than practices such as selling personal information to data brokers or using sensitive information for unexpected purposes. That treatment, in turn, would lead consumers to conclude that they should fear first-party advertising more than the sale of their information or use of their sensitive personal information for unexpected purposes and incentivize businesses to rely on third-party, rather than first-party, advertising practices.

Under the Proposed Regulations, businesses engaged in advertising using solely their own first-party data would be required to present lengthy and unavoidable notices to all new visitors to their websites and mobile applications. This "pre-use" notice must include a litany of details that businesses are likely to struggle to explain (for instance, the "inputs" and "outputs" where processing simply entails activities like sending consumers customized offers based on past purchases) and consumers are unlikely to understand. Such businesses would also be required to present an explanation of consumers' rights to

[21] *See* Proposed Regulations § 7001(g).

opt out and a link to an opt out directly in this pre-use notice rather than merely behind a footer link. The mandated pre-use notice for companies engaged in first-party advertising appears intended to mimic the functionality of cookie banners in the EU, in that notice must be presented—and presumably acted upon in some way—*before* processing occurs.

By contrast, under current CCPA Regulations, businesses are permitted to sell or share personal information and to use sensitive personal information for unexpected purposes by default and must cease such activities only when a consumer makes an opt-*out* request. What's more, such businesses are required to explain these activities and opt-out rights only in their privacy policies and behind a footer link on their websites or settings in their apps,[22] and they face no obligation to provide more intrusive notices or just-in-time choices.

The Proposed Regulations thereby turn the statutory scheme established for potentially high-risk activities on its head by mandating far more intrusive and detailed requirements for a much lower risk activity: first-party advertising. There is no statutory or policy basis on which to require businesses engaged in solely first-party advertising to warn consumers of their practices while allowing those that sell personal information or use sensitive information for unexpected purposes to present less detailed and intrusive notices. What is more, such an approach would discourage privacy-friendly first-party practices and encourage potentially aggressive practices that are dependent upon third parties.

This treatment of first-party advertising would also be at odds with the text and structure of the CCPA. Both when enacted by the Legislature and when amended by the people of California adopting the California Privacy Rights Act ("CPRA"), the CCPA has imposed explicit obligations on a discrete and defined subset of advertising activities, namely "sharing"[23] (disclosing personal information for cross-context behavioral advertising[24] purposes) and (in the view of the California Attorney General) "sales"[25] of personal information by providing personal information to a third party for purposes of showing targeted advertising. Neither the original CCPA nor the CPRA suggested any intent to impose similar, let alone more onerous, obligations on businesses using personal information collected directly from consumers with whom they have a first-party relationship to show ads on their own properties. Indeed, both the CCPA and CPRA suggest an intent to *encourage* first-party advertising over advertising practices that involve disclosures of personal information to third parties. It would defy common sense, and the evident intent of the Legislature and the people of California, for the Agency to impose such an obligation on first-party advertising via regulation.

Finally, the approach to first-party advertising reflected in the Proposed Regulations would overwhelm consumers with redundant choices and conflicting information. Consider a hypothetical consumer (Mary) visiting the website of a hypothetical retailer (ACME Co.). If the Proposed Regulations were adopted, the first time Mary visited ACME's website, she would be forced to read a lengthy notice that

[22] Cal. Code Regs. tit. 11, §§ 7011, 7013, 7015.

[23] Cal. Civ. Code § 1798.140(ah).

[24] Cross-contextual behavioral advertising (first regulated by the CPRA) is defined as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly branded websites, applications, or services, other than the business, distinctly branded website, application, or service with which the consumer intentionally interacts." Cal. Civ. Code § 1798.140(k).

[25] *See* Cal. Civ. Code § 1798.140(ad); Press Release, Cal. Dep't of Just., Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act (Aug. 24, 2022), https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement.

somehow explains that ACME processes her information for the “specific” purpose of promoting ACME’s products to her, that she may opt out of such processing and how to do so, that ACME will not retaliate against her if she exercises her rights, and (in this same notice or via hyperlink) more detail about the ADMT, such as the parameters used and the intended outputs of such inputs. Even if ACME were to use information about Mary’s browsing activities only for security and fraud detection purposes, ACME would still need to explain these uses, potentially scaring her away from using ACME’s site despite collecting data only to protect Mary and consumers like her. After Mary read this notice and potentially chose to opt out, she would likely also encounter a “Your Privacy Choices” link on the footer of ACME’s site (assuming ACME also works with third parties to promote its products). Clicking on this link, Mary would see a separate explanation of ACME’s sale and share practices and would need to separately opt out of those disclosures. As noted above, in addition to the confusion Mary is likely to experience through these multiple notices and opt outs, she is also likely to conclude that the first-party advertising described in the intrusive pre-use notice is more concerning than the sale of her data to data brokers, contrary to the text and policy goals of the CCPA.

Suggested Changes: The Agency should remove the concept of “behavioral advertising” from the Proposed Regulations by striking “profiling a consumer for behavioral advertising” as a trigger for ADMT or risk assessments (i.e., strike § 7200(a)(2)(C) and § 7150(b)(3)(B)(iii) and in their entirety) and deleting the definition of “behavioral advertising” (i.e., strike § 7001(g)).

D. The Regulations Should Clarify the Scope of “Systematic Observation.”

If the Agency elects not to remove the concept of “extensive profiling” as a trigger for ADMT and risk assessment obligations entirely, it should revise the concept of “systematic observation” embedded within the definition of “public profiling” to ensure the that Proposed Regulations do not include location trackers that consumers choose to use to record their own movements. As drafted, the Proposed Regulations can be read to suggest that location technologies that consumers typically affirmatively chose to use—such as through mapping functionality or fitness apps—are in scope. Tracking that occurs through products consumers knowingly choose to activate, or affirmatively grant location access to, does not give rise to any of the concerns about observation not known to or chosen by consumers that the public profiling concept in the Proposed Regulations seems to be designed to address. Moreover, thanks to existing legal standards and requirements from commonly used operating systems and platforms, consumers must grant permission for their precise location to be tracked and are able to stop providing their precise location at any time. Introducing a new and conflicting set of notices and choices for location services would serve to confuse consumers rather than aid their understanding.

Suggested Changes: The Agency should revise the definition of “Systematic observation” in § 7001(eee) as follows: “means methodical and regular or continuous observation a consumer has not chosen to enable. This includes, for example, ongoing ~~methodical and regular~~ or continuous observation of individual consumers by businesses 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. It does not include services that allow consumers to record their own movements, such as location technologies that consumers enable on their mobile devices or in their cars.”

IV. The Agency Should Make ADMT Obligations Proportionate to Privacy Risks.

For the reasons explained above, the Proposed Regulations would create rigid rules governing AI development without an apparent benefit to consumers. History indicates that, when presented with complex and burdensome rules out of line with established norms, some companies rationally chose to limit offering services in certain jurisdictions to limit legal risk or avoid uncertainty.[26] Such a radical result is warranted only if necessary to protect consumers from demonstrable harm, which is a question more appropriate for the Legislature and Governor, which are actively considering the appropriate regulation of AI. The Agency can and should act to fulfill its narrow statutory duty to issue rules governing "access and opt-out rights with respect to businesses' use of automated decisionmaking technology" that processes personal information in a way that is consistent with the CCPA's statutory text and global privacy norms. This would result in far more flexible and straightforward rules than the Proposed Regulations.

While limiting the scope of ADMT obligations to technologies that are actually used to make truly consequential decisions (as outlined above) would address many of these concerns, we also suggest that the Agency revise the activities that trigger ADMT-specific notice, opt out, and access obligations as well as the obligations related to each in the ways described below.

A. The Agency Should Carve out Processing for Security, Fraud Prevention, and Safety from ADMT Obligations.

While the Proposed Regulations appropriately carve out uses of ADMT for security, fraud prevention, or safety purposes from the obligation to provide an opt out through the "security, fraud prevention, and safety exemption,"[27] the Agency should expand this exemption to ensure that businesses are incentivized to use ADMT as appropriate for such purposes, which will serve to maximally protect consumers. Achieving this involves two sets of changes. First, the Agency should exempt security, fraud prevention, and safety uses of ADMT from all ADMT-specific obligations, *except* that the protections of section 7201, as relevant to physical or biological identification only, should continue to apply even for security, fraud prevention, and safety purposes. Second, the Proposed Regulations should broaden the exemption to ensure that all ADMT processing for security, fraud prevention, and safety purposes is exempt, which will serve to encourage businesses to deploy these consumer-protective technologies, rather than dissuading their use through narrowly framed exceptions.

The same policy concerns that argue in favor of excluding processing for security, fraud prevention, and safety purposes from the ADMT opt-out requirement also support carving out processing for those purposes from ADMT pre-use notice and access obligations. Just as perpetrators of fraud or criminal conduct should not be able to lean on opt-out rights to avoid detection, businesses likewise should not be required to provide bad actors with explanations about the steps they take to detect and prevent harmful activities -- information that is fraught for abuse and likely to lead to more rather than fewer

[26] *See, e.g.,* Katie Collins, *Meta Follows in Apple's Footsteps by Restricting AI Releases in EU Countries*, CNET, (July 18, 2024, 11:10AM), https://www.cnet.com/tech/services-and-software/meta-follows-in-apples-footsteps-by-restricting-ai-releases-in-eu-countries/.

[27] *See* Proposed Regulations § 7221(b)(1).

attacks. While the Proposed Regulations appropriately provide that a business relying on this exemption is "not required to provide information that would compromise its use of" ADMT for these purposes in their pre-use notices,[28] suggesting *any* information must be provided in pre-use notices or in response to access requests for security, fraud prevention, or safety purposes may disincentivize use of ADMT even where its use serves to protect consumers. At best, this standard is likely to result in unhelpful high-level disclosures (e.g., simply stating that ADMT is used for security, anti-fraud, and safety purposes), which would do little to advance consumer understanding of ADMT. At the same time, it is appropriate to require companies to evaluate their ADMT technologies to ensure that they work as intended and do not inadvertently discriminate against consumers when used for physical or biological identification (and not an overly-broad notion of "significant decisions" or "extensive profiling") even when used for security and anti-fraud purposes. Thus, the security, fraud prevention, and safety exemption need not be extended to Section 7201, if its requirements are limited to use of ADMT for physical or biological identification.

The Agency should also ensure that the protective activities included in the scope of the exemption are sufficiently broad to ensure that businesses are not forced to provide opt outs or other rights as to activities that serve important security and safety goals. For example, the "necessary" qualifier in the present exemption problematically suggests that critical processing is not exempt unless the use of a particular ADMT is the *only* way to achieve the result – an impractically high bar, as alternative (even if inferior) options often exist. Instead, the Proposed Regulations should encourage the use of technology that businesses deem to be a sound way to achieve the goals of protecting consumers, regardless of whether they *could* use other methods to achieve the same result. Similarly, the Agency should make clear that processing for the prevention, detection, resistance, and investigation of all the listed purposes are exempted from ADMT notice, access, and opt out obligations (not just those related to detecting security incidents). Finally, the "fraud" prong of the exception should not be limited to malicious, deceptive, fraudulent, or illegal actions that are "directed at the business" as reflected in section 7221(b)(1) of the Proposed Regulations. Instead, processing to detect, prevent, resist, investigate, and prosecute such activities should be exempt regardless of the target of the attack—whether consumers, other businesses, or government organizations.

Suggested Changes: For the reasons outlined above, the Agency should make the following changes to sections 7200-7222 of the Proposed Regulations as well as the definition of "physical or biological identification or profiling."

First, the Agency should revise § 7200 to add a new subsection (b), as follows:

§ 7200. When a Business's Use of Automated Decisionmaking Technology is Subject to the Requirements of This Article.

(b) Notwithstanding subsection (a), use of ADMT solely for the security, fraud prevention, or safety purposes listed below ("security, fraud prevention, and safety exception") is exempt from sections 7220, 7221, and 7222 of these regulations:

> (1) To prevent, detect, resist, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of personal information;

[28] *See* Proposed Regulations § § 7220(c)(5)(C), 7222(b)(4)(D).

(2) To prevent, detect, resist, and investigate malicious, deceptive, fraudulent, or illegal actions and to prosecute those responsible for those actions; or

(3) To ensure the safety of natural persons.

Second, the Agency should revise § 7201 as follows:

§ 7201. Requirement for Physical or Biological Identification ~~or Profiling~~.

(a) A business that uses automated decisionmaking technology for purposes of physical or biological identification ~~or profiling for a significant decision concerning a consumer as set forth in section 7200, subsection (a)(1), or for extensive profiling of a consumer as set forth in section 7200, subsection (a)(2),~~ must comply with subsections (1) and (2) below:

(1) The business must conduct an evaluation of the automated decisionmaking technology used for physical or biological identification ~~or profiling~~ to ensure that it works as intended for the business's proposed use and does not discriminate based upon protected classes ("evaluation of the physical or biological identification ~~or profiling~~ technology"). For example, a business that uses ADMT to evaluate biometric information in order to identify consumers shopping in its stores ~~emotion-assessment technology on its customer service calls to analyze the customer service employees' performance at work~~ must conduct an evaluation to ensure that the ADMT ~~it~~ works as intended for this use and does not discriminate based upon protected classes.

(A) Alternatively, where a business obtains automated decisionmaking technology for ~~the~~ physical or biological identification ~~or profiling technology~~ from another person, the business must review that person's evaluation of the physical or biological identification ~~or profiling~~ technology, including any requirements or limitations relevant to the business's proposed use ~~of the physical or biological identification or profiling technology~~.

(2) The business must implement policies, procedures, and training to ensure that its use of the automated decisionmaking technology for ~~the~~ physical or biological identification ~~or profiling~~ works as intended ~~for the business's proposed use~~ and does not discriminate based upon protected classes.

Third, to correspond with the changes above, the Agency should edit the definition of "physical or biological identification or profiling" and make corresponding changes to each instance in the Proposed Regulations where such term is used, as follows:

§ 7001(gg). "Physical or biological identification ~~or profiling~~ means" "identifying ~~or profiling~~ a consumer using information that depicts or describes their physical or biological characteristics, or measurements of or relating to their body. This includes using biometric information~~, vocal intonation, facial expression, and gesture (e.g., to identify or infer emotion)~~."

Remove "or profiling" where the term is used elsewhere in the Proposed Regulations, including:

- **§ 7001(eee)** (definition of "systematic observation");
- **§ 7150(b)(4)(C)** (risk assessment triggers);
- **§ 7150(c)(2)** (risk assessment examples, and adjust example to a scenario involving physical or biological identification); and
- **§ 7200(a)(3)(C)** (training uses of automated decisionmaking technology).

Fourth, The Agency should remove the existing security, fraud prevention, and safety exception to opt-out obligations in § 7221(b)(1) to correspond with the broader security, fraud prevention, and safety exception suggested for § 7200 above, as shown below:

§ 7221. Requests to Opt-Out of ADMT.

(b) A business is not required to provide consumers with the ability to opt-out of a business's use of automated decisionmaking technology for a significant decision concerning a consumer as set forth in section 7200, subsection (a)(1); for work or educational profiling as set forth in section 7200, subsection (a)(2)(A); or for public profiling as set forth in section 7200, subsection (a)(2)(B), in the following circumstances:

> ~~(1) The business's use of that automated decisionmaking technology is necessary to achieve, and is used solely for, the security, fraud prevention, or safety purposes listed below ("security, fraud prevention, and safety exception"):~~
>
> > ~~(A) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information;~~
> >
> > ~~(B) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions; or~~
> >
> > ~~(C) To ensure the physical safety of natural persons.~~

Fifth, the Agency should make corresponding numbering changes to the remaining exemptions to reflect the removal of § 7221(b)(1).

B. The Agency Should Either Omit the Pre-Use Notice Requirement or Adjust It to Harmonize with Other CCPA Notices.

While we agree that meaningful and understandable notices are needed to inform consumers about their rights and companies' information practices, the pre-use notices that are required for an expansive range of situations are inconsistent with the CCPA and have disproportionately detailed and prescriptive content and presentation requirements.

The Proposed Regulations would require businesses to provide notice "prominently and conspicuously" *before* using ADMT to process consumers' personal information. As described above, this notice seems to be modeled off EU-style cookie banners, requiring consumers to see the notice (and presumably take some action) prior to their personal information being processed. While the CCPA tasks the Agency with adopting rules governing ADMT opt *outs*, this approach threatens to instead create a *de facto* opt-*in* standard, which is counter to the statutory mandate and unlike any ADMT rule adopted in any other jurisdiction.

Moreover, the pre-use notice would be the *fifth* independent notice mandated under the CCPA; businesses are already required to provide (and link to) detailed privacy policies with particular disclosures mandated by existing CCPA regulations and California "notices at collection," as well as additional notices if they sell or share personal information, use sensitive personal information for unexpected purposes, or engage in financial incentive programs.[29] This patchwork of notices will cause notice fatigue by desensitizing consumers with numerous and distracting notifications. If the Agency

[29] Cal. Code. Regs. tit. 11, § 7010.

determines some form of ADMT notice is necessary, it should adjust the requirement to be consistent with the obligations imposed on businesses that sell personal information—a prominent footer link behind which consumers can easily find information about how to opt-out. This way, consumers who are interested in learning more about a business's ADMT practices and want to exercise their rights can easily find such information.

Suggested Changes: We suggest the Agency strike § 7220 (Pre-use Notice Requirements) and the corresponding reference in § 7010(c) and (d) entirely. If the Agency determines some more limited form of ADMT notice falls within its legislative mandate, we recommend it: (1) remove the detailed obligations set forth in the draft, allowing businesses to communicate with consumers in ways that match their business practices, and (2) limit the applicability of the pre-use notice to scenarios in which businesses use ADMT to make significant decisions, as addressed above.

We further urge the Agency to treat any required ADMT-specific notice as similar to other notices required under the CCPA, such as the notice of the consumer's right to opt-out of sale/sharing in § 7013 or to limit the use of their sensitive information in § 7014, by making the following changes:

§ 7220. ADMT ~~Pre-use~~ Notice ~~Requirements~~.

(a) A business that uses automated decisionmaking technology as set forth in section 7200, subsection (a), must provide consumers with an ADMT ~~Pre-use~~ Notice. The ADMT ~~Pre-use~~ Notice must inform consumers about the business's use of automated decisionmaking technology and consumers' rights to opt-out of ADMT and to access ADMT, as set forth in this section.

(b) The ADMT ~~Pre-use~~ Notice must:

(1) Comply with section 7003, subsections (a)–(~~b~~d);

~~(2) Be presented prominently and conspicuously to the consumer before the business processes the consumer's personal information using automated decisionmaking technology;~~

~~(3) Be presented in the manner in which the business primarily interacts with the consumer;~~

(2) Be presented to consumers as follows:

(A) A business shall post the ADMT Notice on the internet webpage to which the consumer is directed after clicking on a link entitled "ADMT Notice." The notice shall include the information specified in subsection (c) or be a link that takes the consumer directly to the specific section of the business's privacy policy that contains the same information.

(B) Alternatively, a business may include the information specified in subsection (c) behind the Alternative Opt-Out Link on its internet webpage.

(C) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their use of ADMT and their right to opt out.

(c) The ADMT ~~Pre-use~~ Notice must include the following:

(1) A plain language explanation of the ~~specific~~ purposes for which the business ~~proposes to~~ uses the automated decisionmaking technology. The business must not describe the purpose in generic terms, such as “to improve our services.”

~~(A) For training uses of automated decisionmaking technology set forth in section 7200, subsection (a)(3), the business must identify for which specific uses the automated decisionmaking technology is capable of being used, as set forth in section 7200, subsections (a)(3)(A)–(D). The business also must identify the categories of the consumer’s personal information, including any sensitive personal information, that the business proposes to process for these training uses.~~

Finally, the Agency should strike § 7220(c)(5) in its entirety. The detailed information that it calls for regarding how ADMT operates is likely to confuse consumers without meaningfully advancing the core purpose of the ADMT notice: to alert them to significant applications of ADMT and their related opt-out and access rights.

B. The Agency Should Clarify that ADMT Opt Outs Do Not Require Undoing AI Models.

Section 7221(n) of the Proposed Regulations would mandate that businesses “neither use nor retain” information “previously processed” by the ADMT if a consumer opts out after such processing has occurred. Unlike other opt-out rights provided for by the CCPA that are entirely forward-looking (e.g., to stop selling or sharing the consumer’s personal information, or using their sensitive personal information for non-exempted purposes going forward), this language might be read to suggest a backwards-looking obligation. In its most extreme form, it might even be read to suggest an obligation to delete models trained on the consumer’s personal information—an undertaking so massively expensive and burdensome, it could undermine businesses’ ability to offer many services to California consumers.

The potentially onerous backward-looking nature of this requirement would be disproportionate to the potential risks to consumers and would harm millions of other active users of the affected services. AI models generally improve based on the volume of information they can train on such that individual-level inputs bear minimal import on the eventual outcome. Typical model training also relies on information that, even if not completely de-identified, cannot easily be attributed back to an individual or reasonably permit reidentification. Thus, the expensive and potentially unachievable standard potentially set by the backward-looking component of the ADMT opt out does not mitigate a meaningful privacy risk borne by consumers. The operational challenges associated with such an undertaking also illustrate why opt-out rights in privacy laws are universally forward-looking. Just as the statute treats the ADMT opt out as akin to other CCPA opt-out rights, the Proposed Regulations should reflect that same standard, providing that when a consumer opts out of ADMT, the business’s only obligation is to cease processing that consumer’s personal information for such purposes going forward.

Finally, the changes proposed below also resolve an ambiguity in the present drafting, which can be read to suggest that a business may not make *any* use of the information “previously processed” by the ADMT, even though the consumer may wish for such information to continue to be used for non-ADMT purposes, such as to maintain their account with the business or provide services the consumer requests.

Suggested Changes: The Agency should omit the potentially backward-looking component of the ADMT opt out by amending § 7221(m)-(n) as shown:

§ 7221. Requests to Opt-Out of ADMT.
(m) If the consumer submits a request to opt-out of ADMT ~~before the business has initiated that processing, the business must not initiate processing of the consumer's personal information using that automated decisionmaking technology.~~
~~(n) If the consumer did not opt-out in response to the Pre-use Notice, and submitted a request to opt-out of ADMT after the business initiated the processing~~, the business must comply with the consumer's opt-out request by~~: (1) C~~ceasing to process ~~the consumer's~~ personal information of that consumer collected following the consumer's opt-out request using that automated decisionmaking technology as soon as feasibly possible, but no later than 15 business days from the date the business receives the request.~~ For personal information previously processed by that automated decisionmaking technology, the business must neither use nor retain that information; and (2) Notifying all the business's service providers, contractors, or other persons to whom the business has disclosed or made personal information available to process the consumer's personal information using that automated decisionmaking technology, that the consumer has made a request to opt-out of ADMT and instructing them to comply with the consumer's request to opt-out of ADMT within the same time frame.~~

C. The Agency Should Simplify the ADMT Access Right to Adhere to the CCPA's Mandate.

Even if limited to truly consequential decisions as outlined in Section III, above, the granularity of the ADMT access right contemplated under the Proposed Regulations exceeds the bounds of access rights under U.S. and global privacy laws and will do little to advance consumer understanding, particularly given access rights already provided for under the CCPA. For example, the Proposed Regulations would require businesses to reconstruct the logic and parameters that produced the requesting consumer's particular outputs and how they were applied at an individual level.[30] Providing such information will do little to help consumers who already have the right to access information inferred or generated using ADMT thanks to the CCPA and existing regulations, which grant substantial rights to access information about a company's processing activities, including a copy of the "specific pieces" of personal information collected about them.[31]

The specificity required to respond to access requests in the Proposed Regulations would also have perverse outcomes by discouraging businesses from using ADMT despite the efficiency, personalization, economic, and other benefits of such technology. Moreover, efforts to comply would contradict other CCPA obligations and privacy principles, resulting, for example, in excessive personal information retention for the sole purpose of responding to ad hoc requests. Such storage conflicts with data minimization principles, could increase consumers' risk in the event of data breaches, and would be extremely costly for businesses.

The Agency has not demonstrated, and cannot demonstrate, a benefit to consumers from obtaining highly detailed and technical information concerning how ADMT was used to make even inconsequential decisions about them when consumers already have or will have 1) broad rights to

[30] Proposed Regulations § 7222(b).
[31] *See, e.g.*, Cal. Code. Regs. tit. 11, § 7024.

access their personal information, 2) the right to opt out of the use of ADMT using their personal information to make consequential decisions, and 3) notice explaining such uses. At the same time, the costs businesses would incur to translate figures and calculations into individualized plain-language explanations in response to individual consumer requests would be immense. To meet the statute's goals, we therefore suggest that the Agency 1) permit more flexibility in how businesses respond to access requests, 2) remove any requirement to provide access to the logic or outcome of ADMT when ADMT is used only for fraud or security purposes or other purposes that are subject to exemptions under the CCPA as addressed in Section IV(A) above and 3) remove the suggestion that businesses must provide special access concerning ADMT when humans are involved in the decisionmaking or where ADMT is used other than for significant decisions for the reasons set forth in Section III above.

Suggested Changes: To reflect the considerations outlined above, the Agency should streamline the requirements for the ADMT access response as follows:

§ 7222. Requests to Access Information about ADMT.

(a) Consumers have a right to access the information about ADMT described in subsection (b) when a business uses automated decisionmaking technology to make a significant decision about them as set forth in section 7200, subsection~~s~~ (a)(1)~~--(2). A business that uses automated decisionmaking technology for these purposes must provide a consumer with information about these uses when responding to a consumer's request to access ADMT, except as set forth in subsection (a)(1)~~.

(1) A business that uses automated decisionmaking technology for other purposes ~~solely for training uses of automated decisionmaking technology, as set forth in section 7200, subsection (a)(3), is not required to provide a response to a consumer's request to access ADMT. The business~~ must still comply with section 7024.

(b) When responding to a consumer's request to access information about how ADMT was used to make a significant decision about them, a business must provide plain language explanations of the following information to the consumer:

(1) The specific purpose(s) for which the business used automated decisionmaking technology with respect to the consumer. The business must not describe the purpose in generic terms, such as "to improve our services."

(2) The likely outcome~~put~~ of the business' use of the automated decisionmaking technology with respect to the consumer, or a summary of possible outcomes. ~~If the business has multiple outputs with respect to the consumer, the business may provide a simple and easy-to-use method by which the consumer can access all of the outputs.~~

~~(3) How the business used the output with respect to the consumer.~~

~~(A) If the business used the output of the automated decisionmaking technology to make a significant decision concerning the consumer as set forth in section 7200, subsection (a)(1), this explanation must include the role the output played in the business's decision and the role of any human involvement.~~

~~(i) If the business also plans to use the output to make a significant decision concerning the consumer as set forth in section 7200, subsection (a)(1), the business's explanation must additionally include how the business plans to use the output to make a decision with respect to the consumer, and the role of any human involvement.~~

~~(B) If the business used automated decisionmaking technology to engage in extensive profiling of the consumer as set forth in section 7200, subsection (a)(2), this explanation must include the role the output played in the evaluation that the business made with respect to the consumer.~~

~~(i) If the business also plans to use the output to evaluate the consumer as set forth in section 7200, subsection (a)(2), the business's explanation must additionally include how the business plans to use the output to evaluate the consumer.~~

(3~~4~~) How the automated decisionmaking technology is designed to work~~ed~~ with respect to ~~the~~ consumers. ~~At a minimum,~~ For example, this explanation may ~~must~~ include subsections (A) and (B):

(A) How the logic, including its assumptions and limitations, ~~was~~ is applied to ~~the~~ consumers; and

(B) The key parameters that affect~~ed~~ the output of the automated decisionmaking technology with respect to ~~the~~ consumers~~, and how those parameters applied to the consumer~~

~~(C) A business also may provide the range of possible outputs or 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.~~

~~(D)~~ (C)~~A business relying upon the security, fraud prevention, and safety exception to providing a consumer with the ability to opt-out as set forth in section 7221, subsection (b)(1), is not required to~~ No business is required to provide information that would compromise its use of automated decisionmaking technology for ~~these~~ security, fraud prevention, or safety purposes or for other purposes consistent with an exception to the CCPA.

(c) If the business's ADMT practices subject to this Section 7222 are the same for all consumers, the business:

(1) need not provide an individualized response to the consumer's request to access information about ADMT and may instead provide a standard disclosure containing the information required by this Section; and

(2) need not verify the identity of the person making the request.

With the changes above, the Agency could maintain the remainder of § 7022, except to make: 1) harmonizing changes to refer to "access information about ADMT" throughout and 2) numbering changes as required. We also suggest the Agency update the corresponding definition:

§ 7001(mm) "Request to access information about ADMT" means a consumer request that a business provide information to the consumer about the business's use of automated decisionmaking technology with respect to the consumer, pursuant to Civil Code section 1798.185(a)(15) and Article 11 of these regulations.

V. The Agency Should Simplify the Requirements Related to Risk Assessments.

Google agrees that risk assessments are a foundational tool to help companies evaluate data processing activities, identify potential risks to consumers, and ensure responsible processing of personal information. Google supports obligations for businesses to carefully consider and document the impact of processing that presents a heightened risk of harm to consumers. Indeed, such assessments are integral to Google's own privacy review process (including additional review for personal information processing that may pose a higher risk), which predates statutory mandates to engage in them. While the Proposed Regulations align with these important data governance and consumer-protective principles in some respects, the unprecedented level of detail and analysis mandated for each risk assessment and procedural obligation reflected in the Proposed Regulations go beyond those required by the statute and other regimes such as the GDPR and do not advance consumer privacy interests. These requirements would place an intensive compliance burden on businesses with little additional benefit to consumers. In addition to being limited to ADMT that is used for significant decisions as set forth in Section III above, Article 10 should also be revised to harmonize obligations for conducting risk assessments with similar privacy regimes, and to prioritize a substantive review that considers and protects consumers' interests over papering exercises.

A. The Content Mandated for Risk Assessments Should Focus on Weighing Benefits Against Potential Risks Over Highly Prescriptive Box-Checking Exercises.

The CCPA wisely specifies that risk assessments conducted pursuant to the Agency's regulations "weigh[] the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing[.]"[32] But the Proposed Regulations devote over six pages to required content including potentially irrelevant details and hypothetical harms that exceed this mandate. In addition, this approach is at odds with the numerous jurisdictions in the U.S. and abroad that require risk assessments but do not find it worthwhile to demand this detail and rigidity.

For example, the Colorado Privacy Act Rules provide broad guidance about operational elements of processing to be evaluated in a risk assessment, together with examples of what considerations the assessments "may" include. The Rules go on to state that "the depth, level of detail, and scope" of the assessment "should take into account the scope of risk presented," the volume and nature of personal information processed, the processing activities, and the complexity of the safeguards.[33] Similarly, the GDPR provides broad guidelines for what should be included in a data protection impact assessment.[34]

In contrast, the Proposed Regulations mandate a laundry list of operational elements a business "must" document in each risk assessment, regardless of the context, such as retention periods for each category of personal information, copies of planned disclosures, and how they will be presented. Further, some of the information required, such as the expected profits of an activity, is unlikely to be measurable, particularly because often the benefit of processing *personal* information cannot be disentangled from the value of the service itself. It is not clear how such information, particularly an estimate of possible profit from a specific data use, identifies potential harms or provides additional protection to consumers. Further, the Proposed Regulations would require any business that makes its

[32] Cal. Civ. Code § 1798.185(a)(14)(B).
[33] 4 Colo. Code Regs. §§ 904-3:8.02(C), 8.04(A)(4).
[34] GDPR art. 35(7).

ADMT *or* AI technology available to others and engages in “training” (i.e., improving that technology) to provide “all facts necessary” to the recipients of its technology to conduct its own risk assessment. Requiring such extensive information to be included in risk assessments and to be provided to other businesses that use a business’s technology would prioritize complicated pro forma exercises over careful evaluation and remediation of risks and run contrary to the CCPA instructions.

Finally, we propose adjustments to the rigid timing requirements contemplated in the Proposed Regulations to provide flexibility for the varied processing activities of businesses, without adverse impact on consumers.

Suggested Changes: Google respectfully urges the Agency to adopt a more principles-based and flexible set of risk assessment requirements that hews more closely to the statutory language and is also modeled on the requirements in other jurisdictions.

As to § 7152, one path to accomplishing this would be to replace the present draft in its entirety with a streamlined set of requirements as shown below:

§ 7152 Risk Assessment Requirements.
(a) If a business engages in activities covered under § 7150, the business must conduct a risk assessment to determine whether the risks to consumers’ privacy from the processing of personal information outweigh the benefits to the consumer, the business, other stakeholders, and the public from that same processing.
(b) The risk assessment must include:

1. a summary of the processing and the purposes of such processing;
2. the categories of personal information to be processed, including any categories of sensitive personal information;
3. an assessment of the benefits of the processing;
4. an assessment of the potential risks to the rights of consumers associated with such processing;
5. a description of the safeguards that the business plans to implement to minimize the negative impacts of the processing; and
6. a determination of whether the business will initiate the processing in light of the identified risks.

If the Agency does not adopt a more streamlined and principles-based description of risk assessment contents, it should, at a minimum edit § 7152 as follows:

§ 7152 Risk Assessment Requirements.

- Strike subsection (a)(2)(B) in its entirety.
- Edit subsection (a)(3) to read: “The business must identify the relevant ~~following~~ operational elements of ~~its~~ the processing activity, which may include:
- Edit subsection (a)(3)(B) to read: “An estimate of ~~H~~how long the business will retain ~~each category of~~ the personal information, and any criteria used to determine that retention period.
- Strike subsection (a)(3)(E) in its entirety.
- Strike subsections (a)(3)(F) and (G) and replace with: “the technology, service providers, and contractors to be used in the processing.”
- Edit subsection (a)(4) to read: “The business must ~~specifically~~ identify the expected ~~the~~ benefits to the business, the consumer, other stakeholders, and the public from the processing of the

personal information. For example, a business must not identify a benefit as “improving our service,” because this does not identify the specific improvements to the service nor how the benefit resulted from the processing. ~~If the benefit resulting from the processing is that the business profits monetarily (e.g., from the sale or sharing of consumers’ personal information), the business must identify this benefit and, when possible, estimate the expected profit.~~”

- Edit subsection (a)(5) to read: “The business must ~~specifically~~ identify known ~~the~~ negative impacts to consumers’ privacy associated with the processing, including the~~. The business must identify the~~ sources and causes of these negative impacts~~, and any criteria that the business used to make these determinations~~.
- Edit subsection (a)(6) to read as follows: “The business must identify the safeguards that it plans to implement to address the negative impacts identified in subsection (a)(5),”. ~~The business must specifically identify how these safeguards address the negative impacts identified in subsection (a)(5), including to what extent they eliminate or reduce the negative impacts; and identify any safeguards the business will implement to maintain knowledge of emergent risks and countermeasures~~” and strike subsection (a)(6)(B) entirely.

The Agency should further edit § 7153 to better align the section’s obligations with the scope set out by the title of the section and to account for the differences between businesses that offer ADMT technology and businesses that obtain ADMT from other businesses. The Agency should also revise § 7155 to streamline the timing requirements for risk assessment updates.

§ 7153. Additional Requirements for Businesses that Process Personal Information to Train Automated Decisionmaking Technology ~~or Artificial Intelligence~~.

(a) Taking into account the nature of processing and the information available to the business, ~~A~~ a business that makes automated decisionmaking technology ~~or artificial intelligence~~ available to another business (“recipient-business”) for any processing activity set forth in section 7150, subsection (b) and that trains such automated decisionmaking technology using personal information collected from the recipient-business, must provide, upon request, ~~all~~ facts reasonably necessary to the recipient-business for the recipient-business to conduct its own risk assessment.
(b) A business that trains automated decisionmaking technology ~~or artificial intelligence~~ as set forth in section 7150, subsection (b)(4) and permits a recipient-business ~~another person~~ to use that automated decisionmaking technology ~~or artificial intelligence~~, must provide to the ~~person~~ recipient-business an ~~plain language~~ explanation of any requirements or limitations that the business identified as reasonably relevant to the permitted use of automated decisionmaking technology ~~or artificial intelligence~~.
(c) The requirements of this section apply only to automated decisionmaking technology ~~and artificial intelligence~~ trained using personal information.

§ 7155. Timing and Retention Requirements for Risk Assessments.
(a) A business must comply with the following timing requirements for conducting and updating its risk assessments:

(1) A business must conduct and document a risk assessment in accordance with the requirements of this Article before initiating any processing activity identified in section 7150, subsection (b).

> (2) A~~t least once every three years, a~~ A business must review, and update as necessary, its risk assessments as often as appropriate to ensure that they remain accurate in accordance with the requirements of this Article, including ~~.~~
> ~~(3) Notwithstanding subsection (a)(2) of this section, a business must immediately update a risk assessment~~ whenever there is a material change relating to the processing activity. A change relating to the processing activity may be ~~is~~ material if it significantly diminishes the benefits of the processing activity as set forth in section 7152, subsection (a)(4), creates significant new negative impacts or significantly increases the magnitude or likelihood of previously identified negative impacts as set forth in section 7152, subsection (a)(5), or significantly diminishes the effectiveness of the safeguards as set forth in section 7152, subsection (a)(6).

B. The Agency Should Simplify the Procedures for Risk Assessment Submissions.

Google is encouraged by the Agency's proposed staging of risk assessment submissions to the Agency, including certifications and abridged assessments. However, more should be done to both reduce the paperwork burden on the Agency and allow businesses to remain focused on mitigating risks associated with potentially high-risk processing. Limiting the proactive submission requirement to certifications would help achieve these goals. There is no need, as the Proposed Regulations presently contemplate, to require businesses to proactively provide abridged versions of risk assessments to the Agency, particularly because, both the Attorney General and the Agency will have the right to request unabridged versions at any time (similar to the standards set in other jurisdictions). Requiring businesses to prepare and submit abridged versions of their risk assessments would necessitate papering exercises for purposes that do not mitigate risk to consumers. The abridging process would require businesses to take additional time to attempt to summarize the complete assessment and, even with their best efforts, may result in the Agency perceiving the shorter version as misleading or incomplete. Given the challenge of summarizing these complex and lengthy documents, this process is likely to encourage the use of templates that do not advance the Agency's understanding of businesses' processing activities. We therefore suggest the Agency rely on its well-conceived certification requirement and not additionally require submission of an abridged assessment.

In addition, we encourage the Agency to extend the timeline for a business to provide a complete risk assessment to the Agency or the Attorney General's Office in response to a request. Other states, including Colorado, provide businesses with 30 days to submit a risk assessment after receiving a regulator's request. The Proposed Regulations contemplate a window of just 10 business days. Businesses would benefit from uniformity and more time because disclosures to regulators often necessitate coordination between multiple stakeholders within an organization. Relatedly, other U.S. states explicitly provide that risk assessments submitted upon regulator request are confidential and exempt from public inspection, and that any submission is not a waiver of attorney-client or work-product protections that might otherwise exist. Documenting these protections will further motivate businesses to provide complete and forthcoming risk assessments when requested.

Finally, we respectfully urge the Agency to reconsider requiring an individual executive to be named as responsible for approving a risk assessment in the proactive submission. Concerns about individual liability could have a chilling effect and dissuade input from senior employees. Further, while the Agency notes in its initial statement of reasons that such requirement is "necessary to ensure accountability" and designed to ensure that businesses maintain accurate records of assessment review and approval as well as identifying who is responsible for the review and approval, businesses are already motivated and equipped to handle these procedures internally without mandating names be included in proactive submissions. In any event, the Agency would have access to information about who was involved in conducting the risk assessment if it requested a complete risk assessment.

Suggested changes: The Agency should strike Sections §§ 7157(b)(2) and 7157(b)(3) regarding abridged and unabridged risk assessments in their entirety. We further encourage the Agency to simplify the risk assessment procedural requirements by adopting the following further changes to § 7157(b) and changes to § 7157(c) and (d):

§ 7157. Submission of Risk Assessments to the Agency.

(b) Risk Assessment Materials to Be Submitted. The first submission and subsequent annual submissions of the risk assessment ~~materials~~ certifications to the Agency must include the following:

(1) Certification of Conduct. The business must submit a written certification that the business conducted its risk assessment as set forth in this Article during the months covered by the first submission and subsequent annual submissions to the Agency on a form provided by the Agency.

(A)~~The business must designate a qualified individual with authority to certify the conduct of the risk assessment on behalf of the business. This individual must be the business’s highest-ranking executive who is responsible for oversight of the business’s risk-assessment compliance in accordance with this Article (“designated executive”).~~

~~(B)~~The written certification must include:

(i) Identification of the months covered by the submission period for which the business is certifying its conduct of the risk assessment and the number of risk assessments that the business conducted and documented during that submission period;

(ii) An attestation that the risk assessments have been ~~designated executive has~~ reviewed, understood, and approved by appropriate stakeholders within the business~~’s risk assessments that were conducted and documented as set forth in this Article~~;

(iii) An attestation that the business initiated any of the processing set forth in section 7150, subsection (b), only after the business conducted and documented a risk assessment as set forth in this Article~~; and~~

~~(iv) The designated executive’s name, title, and signature, and the date of certification~~.

(c) Method of Submission. The risk assessment certifications ~~materials~~ must be submitted to the Agency through the Agency’s website at https://cppa.ca.gov/.

(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.

(1) Risk assessments are confidential and exempt from public inspection and copying under the California Public Records Act.

(2) The disclosure of a risk assessment pursuant to a request from the Agency or the Attorney General under this subsection does not constitute a waiver of any

attorney-client privilege or work-product protection that might otherwise exist with respect to the assessment and any information contained in the assessment.

* * * * *

We appreciate the opportunity to provide comments on the Proposed Regulations, and we look forward to continued collaboration with the Agency on these important issues.

Sincerely,

Will DeVries
Director, Regulatory Affairs - Privacy Advisory

Grenda, Rianna@CPPA

From: Ray Lehmann <rlehmann@laweconcenter.org>
Sent: Wednesday, February 19, 2025 1:26 PM
To: Regulations@CPPA
Cc: Kristian Stout
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: ICLE CPPA Comments.pdf

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Please receive the attached comments of the International Center for Law & Economics on Updates to Existing CCPA regulations; Cybersecurity Audits; RiskAssessments; Automated Decisionmaking Technology, and Insurance Companies.

--
R.J. Lehmann
Executive Editor and Senior Fellow
International Center for Law & Economics
rlehmann@laweconcenter.org
[redacted] (m)
727-914-3262 (h)

International
Center for
Law & Economics

Comments of the International Center for Law & Economics

Updates to Existing CCPA regulations; Cybersecurity Audits; Risk Assessments; Automated Decisionmaking Technology, and Insurance Companies (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations)

February 19, 2025

Authored by:

Kristian Stout (Director of Innovation Policy, International Center for Law & Economics)

Subiksha Ramakrishnan (Innovation Fellow, International Center for Law & Economics)

I. Introduction

We thank the California Privacy Protection Agency ("CPPA") for the opportunity to comment on the proposed regulations for automated decisionmaking technologies ("ADMT"). These comments focus on the significant risks posed by the CPPA's expansive approach to ADMT regulation, which would impose substantial compliance burdens, while potentially stifling innovation in artificial intelligence ("AI"). We respectfully suggest that the CPPA adopt a more targeted framework that focuses on marginal risks posed by truly consequential uses of ADMT, while allowing beneficial low-risk applications to continue to drive economic growth and technological advancement.

U.S. AI regulation is evolving at an unprecedented pace. In 2024 alone, 45 states, Puerto Rico, the U.S. Virgin Islands, and the District of Columbia all introduced AI-related bills, reflecting the fragmented and fluid nature of AI rules across U.S. jurisdictions.[1] This patchwork of state-level efforts underscores the significant variation in focus, with some laws targeting "high-risk" AI systems, others addressing algorithmic discrimination, and others still emphasizing consumer transparency and governance frameworks.

This rapid introduction of new measures has served to create substantial uncertainty for businesses in the emerging AI-services sector, particularly those that operate nationally. The CPPA's draft regulations risk exacerbating this issue by imposing a broad and inflexible framework at a time when ADMT and other AI technologies and governance models are still taking shape. A sweeping, one-size-fits-all approach could quickly become outdated, hindering innovation and California's leadership as a technology hub. A more agile and incremental strategy would allow California to adapt alongside the evolving landscape, rather than lock in rules that may fail to account for future developments in AI capabilities and risks.

A better approach to responsible ADMT regulation would be incremental and sector-specific.[2] Such an approach was advocated by the congressional Bipartisan Artificial Intelligence Task Force, which recommended identifying novel issues and addressing AI challenges within specific sectors by using existing regulatory frameworks where feasible.[3] By leveraging sector-specific expertise and regulatory structures, policymakers can craft targeted solutions that promote innovation while safeguarding against risks.[4]

[1] *See* Tatiana Rice *et al.*, *U.S. State AI Legislation*, FUTURE PRIV. FORUM (2024), at 3, *available at* https://fpf.org/wp-content/uploads/2024/09/FINAL-State-AI-Legislation-Report-webpage.pdf; *Artificial Intelligence 2024 Legislation*, NAT'L. CONF. STATE LEGIS. (Sep. 9, 2024), https://www.0.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation.

[2] *See* Jay Obernolte & Ted W. Lieu, *Report of the Bipartisan House Task Force Report on Artificial Intelligence* (Dec. 2024), vi-vii, 85, *available at* https://republicans-science.house.gov/_cache/files/a/a/aa2ee12f-8f0c-46a3-8ff8-8e4215d6a72b/E4AF21104CB138F3127D8FF7EA71A393.ai-task-force-report-final.pdf.

[3] *Id.* at 6, 30.

[4] *Id.* at 7, 17.

A sectoral approach recognizes that ADMT and AI applications vary significantly across industries, with different risk profiles and operational contexts requiring tailored oversight. For instance, AI used in health-care diagnostics requires different safeguards than AI used for retail inventory management or marketing analytics. Financial services AI applications may need specific controls around fairness and transparency in lending decisions, while manufacturing AI might prioritize safety and reliability metrics. By working within existing industry-specific regulatory frameworks and expertise, a sectoral approach can more effectively address genuine risks, while preserving beneficial innovation.

This targeted approach would almost certainly be more effective than one-size-fits-all regulation. The National Telecommunications and Information Administration (NTIA) under former President Joe Biden and other key stakeholders have likewise endorsed sector-specific approaches, which can more easily avoid imposing inappropriate requirements across dissimilar use cases. By contrast, the CPPA's approach risks creating requirements that are simultaneously too stringent for low-risk applications and insufficiently stringent for truly high-risk uses.

Adopting an incremental approach would also allow policymakers to address genuine ADMT and AI-related risks as they emerge without stifling progress. In contrast, the CPPA's current draft regulations risk establishing a rigid framework that could place particularly undue burdens on small businesses and startups that may increasingly depend on AI tools to maintain their competitive edge and productivity. In a moment when this policy field remains fluid, California has an opportunity to lead by example, by championing innovation while addressing harms through a measured and iterative regulatory framework.

The remainder of these comments will address some specific concerns and suggest paths forward.

II. Core Concerns with the CPPA Draft

A. Overly Broad Scope and Definitions

The draft regulations introduce several problematically broad definitions that could sweep a vast range of technologies and business practices into their ambit. The definition of "AI" includes any "machine-based system that infers, from the input it receives, how to generate outputs that can influence physical or virtual environments."[5] Even more concerning, the definition of "automated decision-making technology" includes not just those systems that make or replace human decisions, but also any technology that "substantially facilitates human decision-making."[6]

This vague standard is expanded further to include any use of such technology's output as a "key factor in a human's decision-making."[7] The regulations compound this scope with a broad definition

[5] *Proposed Regulations* § 7001 (c), CALIF. PRIV. PROT. AGENCY (2024), *available at* https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf.

[6] *Id.* § 7001(f).

[7] *Id.*

of "behavioral advertising," which would include any targeting based on consumer activity, both across and within a business's own services.[8]

These overlapping and expansive definitions create significant interpretive challenges. For example, even basic spreadsheet analyses that inform business decisions could qualify as ADMT if they are deemed to "substantially facilitate" those decisions. Similarly, the broad scope of "behavioral advertising" could mean that simply remembering a customer's preferences on a business's own website triggers broad regulatory obligations. When combined with the regulations' extensive compliance requirements, these definitions threaten to capture routine business operations far beyond what might be necessary to protect consumer privacy.

The CPPA's proposed expansive definition of ADMT would also capture a broad array of routine AI applications, including customer profiling, behavioral advertising, and operational-efficiency tools.[9] While the intent to protect consumers is clear, this overly broad definition fails to account for the heterogeneity of AI systems and the nuanced ways they may function across industries. This risks imposing premature and disproportionate obligations on businesses and stifling innovation at a time when AI development remains in its infancy.

Indeed, despite the marketing hype, AI is not a single monolithic technology, but rather a diverse collection of tools deployed across different layers of an "AI stack."[10] Treating all forms of AI—whether low-risk tools like chatbots or high-impact systems like automated credit decisions—as equivalent under a single regulatory framework would be both analytically unsound and practically counterproductive. The CPPA proposal fails to distinguish between consequential decisions with a direct impact on consumer rights and routine, low-risk AI applications that may help to improve business efficiency or customers' experience.[11]

This overreach creates significant uncertainty for businesses, particularly small and mid-sized firms. Many of these firms are beginning to rely on AI tools for operational efficiency, marketing, and customer service, and the costs of compliance under such a sweeping definition would be prohibitive. To date, AI adoption by small businesses has proven transformative, improving profitability, reducing operational burdens, and enabling competitiveness against larger firms.[12]

[8] CPPA, *supra* note 5, § 7001(g).

[9] CPPA, *supra* note 5, § 7001(m) (6).

[10] *See* Lazar Radic & Kristian Stout, *What Is the Relevant Product Market in AI?*, CONCURRENCES (Aug. 16, 2024), at 109, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4927505.

[11] *Id.* at 110.

[12] *See Empowering Small Business: The Impact of Technology on U.S. Small Business*, U.S. CHAMB. COMMER. TECH. ENGAGEM. CTR. (Sep. 14, 2023), at 3, *available at* https://www.uschamber.com/assets/documents/The-Impact-of-Technology-on-Small-Business-Report-2023-Edition.pdf; *Open Source AI is Leading to Breakthroughs in Healthcare, Education, and Entrepreneurship*, META (Dec. 11, 2024), https://about.fb.com/news/2024/12/open-source-ai-is-leading-to-breakthroughs-in-healthcare-education-and-entrepreneurship.

Subjecting these businesses to ambiguous and burdensome regulatory requirements will disproportionately harm their ability to innovate and adopt new technologies.

AI's productivity benefits are particularly important for workers with fewer skills or resources, as it automates tasks, enhances lower-skilled workers' output, and increases efficiency.[13] Regulations that fail to differentiate among AI systems based on their risk levels or use cases may inadvertently discourage the adoption of AI technologies across the board, ultimately hindering the productivity and growth of small businesses. This is especially concerning, given that many of these firms lack the legal and financial resources to navigate compliance with overly broad regulations.

Some models for AI governance provide a more nuanced approach by focusing on marginal risks, rather than imposing broad, preemptive restrictions. For instance, the Biden administration's NTIA recommended evaluating the "marginal risks" introduced by specific AI systems relative to existing alternatives, focusing on empirically demonstrable harms rather than speculative risks.[14] This framework seeks to assess the incremental risks and benefits that AI technologies may pose in specific contexts, thereby ensuring that only systems with significant and observable harmful effects would face heightened scrutiny. Unlike the CPPA's sweeping definition of ADMT, the NTIA's approach provides a structured, evidence-based pathway to understand AI risks without stifling innovation.

Moreover, broadly defining AI and ADMT could lead to unintended consequences for competition and innovation. As noted above, the heterogeneity of AI services and markets makes any attempt to regulate "AI" as a singular entity analytically untenable.[15] The rigidity of the CPPA's current proposal could discourage investment in AI development and adoption within the state, pushing innovation to other jurisdictions with clearer, risk-adjusted regulatory environments.[16] Indeed, we have already seen a similar flight to more flexible jurisdictions in response to the EU's AI Act.[17]

Ultimately, the CPPA draft's overly broad definition of ADMT is premature. Policymakers should adopt a narrower, risk-based framework focusing on truly consequential uses of ADMT (which may or may not involve AI), while allowing routine and low-risk applications to continue delivering economic and societal benefits. A more targeted approach would align California's efforts with evolving federal and global frameworks, while preserving the state's position as a leader in AI development and innovation.

[13] *See* Julian Jacobs, *Evidence Shows Productivity Benefits of AI, Center for Data Innovation*, CENT. DATA INNOV. (Jun. 11, 2024), https://datainnovation.org/2024/06/evidence-shows-productivity-benefits-of-ai.

[14] *See* Kristian Stout *et al.*, *NIST AI 800-I, Managing Misuse Risk for Dual-Use Foundation Models*, INT'L CTR. L. & ECON. (2024), at 8-13, *available at* https://laweconcenter.org/wp-content/uploads/2024/09/NIST-AI-comments-final.pdf.

[15] *See* Radic & Stout, *supra* note 10, at 108, 113, 131.

[16] *See* Rachel Curry, *How AI Regulation in California, Colorado and Beyond Could Threaten U.S. Tech Dominance*, CNBC (Nov. 21, 2024), https://www.cnbc.com/2024/11/21/how-ai-laws-in-california-states-threaten-us-tech-dominance.html.

[17] Pascale Davies, *Why OpenAI's Voice Mode, Meta's Llama and Apple's AI Won't be Coming to Europe Yet*, EURONEWS (Aug. 10, 2024), https://www.euronews.com/next/2024/10/08/why-openais-voice-mode-metas-llama-and-apples-ai-wont-be-coming-to-europe-yet.

B. Legal and Jurisdictional Concerns

The CPPA's expansive proposed regulations raise serious questions about their alignment with the original intent of the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).[18] These laws were designed to give consumers greater control over their personal data and to safeguard their privacy in an era of rapid technological change. The draft regulations on ADMT, however, appear to exceed this mandate by broadening the scope to include virtually any AI-driven system, irrespective of its risk profile or actual impact on consumer rights.

This approach contrasts sharply with more targeted regulatory frameworks. For example, as noted above,[19] the NTIA's marginal-risk framework focuses on assessing AI systems' incremental risks and benefits, ensuring that only applications with significant observable negative effects face heightened scrutiny.[20] In contrast, the CPPA draft fails to distinguish between high-stakes systems and routine, low-risk applications like customer profiling and advertising optimization.[21]

Apart from the direct effects of the CPPA's approach on consumers and businesses, its conflicts with emerging frameworks that favor sectoral regulation over comprehensive rules and will lead to other headaches for U.S. firms. While federal agencies and legislators are moving toward targeted, industry-specific approaches that account for differing risk profiles and use cases,[22] the CPPA's regulations would impose broad requirements across all sectors. This creates practical compliance challenges for businesses that must navigate both federal and state requirements, and leads to potential federal preemption issues. For example, a business developing AI tools for health care might need to comply with sector-specific guidelines from the U.S. Food and Drug Administration (FDA), while simultaneously meeting California's sweeping ADMT requirements. The potential for contradictory obligations or duplicative compliance burdens is significant.

[18] *See* Kayla N Bushey, *One Size Dose Not Fit All: How the California Privacy Rights Act Will Not Improve Employee Data Collection and Privacy Rights*, 32(1) CATH. U. J.L. & TECH. (2023), https://scholarship.law.edu/jlt/vol32/iss1/8; California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 *et seq*.; Maria Korolov, *California Consumer Privacy Act (CCPA): What You Need to Know to be Compliant*, CSO (Jul. 7, 2020), https://www.csoonline.com/article/565923/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html.

[19] Stout, *supra* note 14.

[20] Stout, *supra* note 14 at 9.

[21] *See* Sebastião Barros Vale & Gabriela Zanfir-Fortuna, *Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities*, (May 2022), at 21, https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf; *Draft Risk Assessment and Automated Decisionmaking Technology Regulations*, CALIF. PRIV. PROT. AGENCY (2024), at 3-4, *available at* https://cppa.ca.gov/meetings/materials/20240308_item4_draft_risk.pdf.

[22] Kristian Stout, *The AI Legislative Puzzle*, TRUTH MARK. (Nov. 7, 2024), https://truthonthemarket.com/2024/11/07/the-ai-legislative-puzzle; Stout, *supra* note 14 at 8; Obernolte & Lieu, *supra* note 2 at 17, 21, 70.

C. Disproportionate Impact on Business Innovation

1. *Impact on small businesses*

Small businesses form the backbone of California's economy, and their ability to compete increasingly depends on AI tools. AI technologies already play a critical role in helping small businesses to remain efficient and competitive in a fast-moving digital marketplace. Surveys suggest that 95% of small businesses already use at least one technology platform to streamline their operations, with nearly a quarter adopting AI to improve marketing, customer communications, and overall business performance.[23] For these businesses, AI adoption has led to measurable increases in profit margins, sales, and operational efficiency.[24]

AI tools can help to level the playing field by providing affordable and scalable solutions. AI-powered platforms can help small businesses to better understand customer behavior, optimize advertising strategies, and reach new audiences. AI-driven tools for inventory management, payroll, and customer-relationship management can enhance operational efficiency, allowing business owners to focus on growth rather than administrative burdens.[25]

The CPPA's broad regulations, however, risk undermining these gains by subjecting routine AI tools to onerous compliance requirements. Unlike large corporations with dedicated legal teams, small businesses often lack the resources to navigate complex regulatory frameworks. The cost of compliance could become a barrier to adopting AI technologies, particularly given that AI tools provide the greatest productivity benefits to more modestly resourced workers and businesses.[26] This regulatory burden would not only stifle innovation but could also exacerbate existing challenges that small businesses already face, such as inflation and workforce shortages.[27]

2. *Disruption to the digital-advertising ecosystem*

The regulations particularly threaten the digital-advertising ecosystem by conflating behavioral advertising with consequential decisionmaking systems. While behavioral advertising uses AI-driven analysis, such systems do not make decisions about individuals and therefore operate in a fundamentally different way from the high-stakes systems used for credit approvals or employment decisions. Treating these tools as equivalent would impose an inappropriate framework on an industry vital to the digital economy.

Further, behavioral advertising underwrites many free online services that consumers rely on daily. The CPPA's overly broad definition could force advertising platforms and smaller advertisers to abandon targeted advertising strategies, threatening ad-supported business models and reducing

[23] U.S. Chamber, *supra* note 12 at 3, 4.

[24] *Id.* at 2, 23.

[25] *Id.* at 5.

[26] Jacobs, *supra* note 13.

[27] U.S. Chamber, *supra* note 12 at 2, 15.

access to free digital services. Such regulatory overreach would have a chilling effect, as prescriptive and expansive rules often stifle innovation by discouraging investment in those areas where the regulatory landscape is most uncertain or unduly burdensome.[28]

Moreover, the proposed regulations fail to recognize that behavioral advertising primarily involves optimizing ad delivery based on anonymized data, rather than making binding decisions with significant effects on consumers' lives. These are typically low-risk, reversible decisions ill-suited for a regulatory framework designed to mitigate the potential harms of high-risk AI systems. Small businesses, in particular, stand to lose the most from these regulations, as many rely on targeted advertising to reach niche markets in a cost-effective manner.

3. Broader economic consequences

The CPPA's proposed regulations carry significant risks for innovation and U.S. technological competitiveness, with California standing to lose the most. The state is uniquely positioned as a nexus of AI innovation, hosting the world's leading AI research institutions, most of the top AI companies, and a dense network of AI startups and talent. This ecosystem has made California the primary locus of U.S. leadership in AI. Stringent state-level AI regulations, however, could undermine this position by creating a fractured regulatory landscape that increases costs and reduces investment in the sector.[29] California-based companies would face a difficult choice: either accept higher compliance burdens than their global competitors, or relocate key operations to more business-friendly jurisdictions.

The stakes are particularly high given the intense global competition in AI development. Other regions are actively working to attract AI companies and talent.[30] While California's existing ecosystem provides significant advantages, regulatory costs can shift the calculus for both established companies and startups alike. Development teams might relocate to states with clearer regulatory frameworks, while investors might redirect capital to jurisdictions where compliance burdens are more predictable. This regulatory arbitrage could gradually erode California's advantage as the world's preeminent AI hub.

[28] *See* Michael Genest *et al.*, *Comments on August 2024 CPPA SRIA*, CAPITOL MATRIX CONSULT. (Nov. 1, 2024), *available at* https://advocacy.calchamber.com/wp-content/uploads/2024/11/CMC_comments_on_CCPA_SRIA_11-1.pdf; *California Consumer Privacy Act*, INTERACT. ADVERT. BUR., https://www.iab.com/topics/privacy/ccpa (*last visited* Dec. 27, 2024); Betsy Vereckey, *Does Regulation Hurt Innovation? This Study Says Yes*, MIT SLOAN SCH. MANAG. (Jun. 7, 2023), https://mitsloan.mit.edu/ideas-made-to-matter/does-regulation-hurt-innovation-study-says-yes.

[29] *See* Chris Edwards, *Entrepreneurs and Regulations: Removing State and Local Barriers to New Businesses*, CATO INST. (May 5, 2021), https://www.cato.org/policy-analysis/entrepreneurs-regulations-removing-state-local-barriers-new-businesses; Curry, *supra* note 16; U.S. Chamber, *supra* note 12.

[30] *See UAE Establishes Global Leadership in Artificial Intelligence, High-Tech Innovation*, EMIR. NEWS AGENCY (Sep. 28, 2024), https://www.wam.ae/en/article/b5exntj-uae-establishes-global-leadership-artificial; *The U.A.E.'s Big Bet on Artificial Intelligence*, U.S.-UAE BUS. COUNC. (Feb. 2024), *available at* https://usuaebusiness.org/wp-content/uploads/2024/02/SectorUpdate_AIReport_Web.pdf.

The regulations could have a particularly severe adverse impact on AI research and development. California's research institutions and companies are at the forefront of developing cutting-edge AI applications like large language models (LLMs), generative-AI tools, and advanced-automation systems. These innovations require extensive experimentation and rapid iteration to achieve technological breakthroughs. The CPPA's broad definition of ADMT could be interpreted to cover many of these research and development activities, creating uncertainty about compliance obligations during the development process. This ambiguity could force researchers and developers to slow their progress significantly or implement burdensome compliance processes even during early experimental phases.

The implications extend beyond individual research projects to the broader AI-development ecosystem. Researchers might avoid pursuing promising lines of inquiry where the regulatory implications are unclear. Companies might relocate their R&D operations to jurisdictions with clearer frameworks for AI development. Even routine product improvements and testing could face delays and added costs as businesses navigate the new compliance requirements.

The measurable impact of such overregulation is well-documented. Excessive regulation consistently reduces innovation by increasing costs and discouraging risk taking by entrepreneurs and businesses alike.[31]

III. Conclusion

The CPPA's draft regulations on ADMT require significant refinement to achieve a better balance of consumer protection with innovation and economic competitiveness. A targeted approach focused on "consequential decisions" would align with effective practices, while equipping the CPPA the tools to protect consumers. This narrower scope would also reduce compliance burdens for routine, low-risk AI applications while maintaining oversight where it matters most.

An incremental, evidence-based approach should guide California's regulatory framework. Overregulation can stifle innovation and create barriers for startups, who are critical to the AI ecosystem.[32] The CPPA can ensure its rules evolve with the rapidly changing AI landscape by avoiding premature codification of broad mandates that could quickly prove obsolete.

Broader governance of AI systems should take account of the need for a holistic, nationwide framework.[33] A fragmented patchwork of state-level regulations will create compliance challenges for businesses operating across jurisdictions, thereby reducing investment and deterring innovation.[34] By harmonizing with emerging federal policies—or deferring broad regulations until the federal

[31] *See* Philippe Aghion *et al.*, *The Impact of Regulation on Innovation* (Nat'l Bureau of Econ. Rsch. Working Paper No. 28381, 2021), https://www.nber.org/papers/w28381.

[32] *Id.*

[33] *See, e.g.*, Stout, *supra* note 14 at 3; Vale & Zanfir-Fortuna, *supra* note 21.

[34] *See* Chinmayi Sharma & Alan Z. Rozenshtein, *Regulatory Approaches to AI Liability*, LAWFARE (Sep. 24, 2024), https://www.lawfaremedia.org/article/regulatory-approaches-to-ai-liability.

consensus is clearer—California can provide clarity to AI developers while maintaining appropriate consumer protections.

A sectoral approach would enable more effective and efficient oversight. The diverse industries that employ AI services face distinct challenges: financial services must prioritize algorithmic fairness, health-care applications must emphasize privacy and accuracy, and retail applications might focus on improved customer service. By working within existing regulatory frameworks, the CPPA could better calibrate requirements to actual risks and operational realities. This would allow for nuanced oversight of high-risk applications, while avoiding laying unnecessary burdens on beneficial, low-risk AI tools.

California's unique position as the world's leading AI-development hub means it has the most to gain from getting these regulations right. The state can maintain its leadership position while protecting consumers by adopting targeted regulations that address genuine risks, and without creating unnecessary barriers to innovation. By narrowing the focus of ADMT regulations, adopting an incremental strategy, and prioritizing harmonization with federal initiatives, California can strike the right balance between safeguarding consumer rights and fostering a thriving, competitive AI ecosystem.

Grenda, Rianna@CPPA

From:	Lartease Tiffith <lartease@iab.com>
Sent:	Tuesday, February 18, 2025 1:30 PM
To:	Regulations@CPPA
Subject:	IAB's Comments on CPPA's Proposed Regulations on Automated Decision-Making Technology
Attachments:	IAB's Comments on CPPA ADMT Regs.pdf

Dear Regulations Team,

On behalf of the Interactive Advertising Bureau (IAB), please find attached our written comments regarding the California Privacy Protection Agency's proposed regulations on Automated Decision-Making Technology. We appreciate the Agency's continued efforts to protect consumer privacy, and we welcome the opportunity to discuss these matters further.

Should you have any questions or require additional information, please feel free to reach out at your convenience. Thank you for your time and consideration.

Sincerely,

Lartease Tiffith

Lartease M. Tiffith, Esq.
Executive Vice President, Public Policy
700 K Street NW, Suite 300
Washington, DC 20001
lartease@iab.com

February 18, 2025

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

Re: Concerns and Suggested Amendments to CPPA's Proposed Regulations on Automated Decision-Making Technology (AMDT)

Dear Members of the California Privacy Protection Agency:

On behalf of the Interactive Advertising Bureau (IAB), I write to express significant concerns regarding the California Privacy Protection Agency's (CPPA) proposed regulations on Automated Decision-Making Technology (AMDT) under the California Privacy Rights Act (CPRA). IAB represents over 700 leading media companies, brand marketers, agencies, and technology companies that are responsible for selling, delivering, and optimizing digital advertising and marketing campaigns. Together, our members account for 86 percent of online advertising expenditures in the United States.

IAB is committed to professional development and elevating the knowledge, skills, expertise, and diversity of the workforce across the digital advertising and marketing industry. Through the work of our public policy office in Washington, D.C., IAB advocates for our members and promotes the value of the interactive advertising industry to legislators and policymakers.

While we appreciate the Agency's efforts to address privacy and transparency in automated decision-making, several provisions in the draft regulations require revisions to align with practical implementation realities and to avoid unnecessarily burdensome requirements that could negatively impact businesses, stifle innovation, and impose undue burdens on the advertising and media industries. Below, we outline specific concerns, recommended amendments with redline text, and rationales to support these changes.

1. <u>Overbroad Definition of ADMT (§ 7001)</u>

The draft regulations define ADMT as technology that "substantially facilitates human decision-making," encompassing activities that do not independently or materially affect consumers. This creates unnecessary ambiguity and compliance burdens.

Proposed Amendment:

> **"Automated Decision-Making Technology (ADMT)" 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 decision-making, or substantially**

> **facilitate human decision-making. For purposes of this definition, ADMT does not include systems that perform procedural tasks, detect patterns, or provide insights for human decision-making without directly affecting the outcome of a decision."**

Rationale:
This revision narrows the scope of ADMT to align with the statutory intent, focusing on systems that make decisions materially impacting consumers' rights or opportunities. Broad definitions unnecessarily include low-risk activities, such as preparatory tools or insight generation, which have no direct effect on consumers, yet would create unnecessary compliance burdens.

2. Implementation Timeline

The lack of a reasonable implementation period imposes undue challenges on businesses striving to comply with new, complex obligations.

Proposed Amendment:

> **"Civil and administrative enforcement of the provisions set forth in Articles 1, 9, 10, and 11 shall not commence until two years from the date the provisions are finalized."**

Rationale:
A two-year implementation period ensures businesses have adequate time to adapt their systems, implement necessary changes, and train employees. This approach aligns with global best practices for rolling out significant regulatory changes, preventing rushed compliance that could compromise effectiveness and fairness.

3. Overbroad Definitions – Behavioral Advertising and Artificial Intelligence

a. Behavioral Advertising (§ 7001)

Including behavioral advertising within "extensive profiling" under ADMT is problematic. Behavioral advertising involves algorithmic ad placement based on data, but the ad delivery systems themselves do not execute decisions about individuals.

Proposed Amendment:

> **Strike the definition of "Behavioral Advertising" entirely and revise extensive profiling to apply only to "cross-context behavioral advertising."**

Rationale:
This revision aligns the regulations with the original intent of CCPA. Personalized advertising offers significant benefits, particularly to small businesses, by enabling cost-effective, targeted outreach. Overregulating low-risk activities like behavioral advertising will stifle innovation,

increase costs, and reduce consumer access to free or reduced-cost services. Furthermore, Imposing opt-out and risk assessment requirements burdens businesses and consumers without addressing meaningful privacy risks.

b. Artificial Intelligence (§ 7001)

The proposed definition of AI unnecessarily conflates AI-related concepts and exceeds CPPA's regulatory authority.

Proposed Amendment:

> **Remove "Artificial Intelligence" from the scope of ADMT definitions and obligations.**

Rationale:
CPRA is focused on addressing privacy concerns, not regulating AI broadly. Including AI as part of ADMT creates unnecessary complexity and fragmentation, especially as AI governance frameworks already exist in California.

4. Scope of ADMT Obligations (§ 7200)

The draft regulations expand ADMT requirements to non-decision-making activities like training models and behavioral advertising, which exceed the intended scope of ADMT.

Proposed Amendment:

> **Limit ADMT obligations to decisions that materially affect consumers' legal or financial rights, such as access to housing, employment, or healthcare. Exclude training models and behavioral advertising from these requirements.**

Rationale:
Focusing on high-risk, impactful decisions ensures the regulations are targeted and effective. Including training models and advertising undermines the clarity and usability of the framework, creating unnecessary burdens without improving consumer protection.

5. Risk Assessments and Significant Decisions (Article 10, § 7150(b)(3)(A))

The current definition of "significant decision" under § 7150(b)(3)(A) diverges from existing frameworks in other states by including decisions with non-material impacts. For example, profiling that does not involve financial, housing, or employment consequences should not trigger a risk assessment.

Proposed Amendment:

Revise the definition of "significant decision" to align with existing standards:

> **"Significant decision" means a decision using information that results in access to, or the provision or denial of, financial or lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, healthcare services, or essential goods or services.**

Rationale:
The amendment refines the scope of significant decisions to align with global and domestic privacy frameworks, such as the GDPR and Colorado's CPA. Limiting the focus to decisions with real-world impacts ensures regulatory efforts prioritize high-risk activities without burdening businesses with unnecessary assessments for low-risk activities.

6. Extensive Profiling in Public Spaces (Article 10, § 7150(b)(3)(B)(ii))

Requiring risk assessments for profiling in publicly accessible spaces conflicts with CPRA exemptions for publicly available information. Expanding the definition to include locations like shopping areas or stadiums imposes disproportionate burdens on businesses without commensurate privacy benefits.

Proposed Amendment:

Strike § 7150(b)(3)(B)(ii). If retained, limit its scope as follows:

> **"Publicly accessible space" refers exclusively to physical spaces with no reasonable expectation of privacy and excludes activities conducted on the internet or other digital platforms.**

Rationale:
Data collected in public spaces, such as foot traffic counts or aggregated location analytics, generally lacks specificity that could harm consumer privacy. Including such data in risk assessments creates disproportionate compliance costs for businesses and ignores existing legal protections for personally identifiable information. Limiting the definition of publicly accessible spaces ensures consistency with CPRA's objectives while reducing unnecessary burdens.

7. AI/ADMT Training (Article 10, § 7150(b)(4))

Including training models under heightened obligations such as risk assessments is impractical and inconsistent with existing AI regulatory frameworks. For example, training processes do not directly impact consumers and should not be classified as decision-making.

Proposed Amendment:

Strike § 7150(b)(4) entirely. If not removed, limit its application:

> **Training processes using ADMT shall not require risk assessments unless explicitly used for significant decision-making purposes as defined in § 7150(b)(3)(A).**

Rationale:
Training models are foundational to AI systems and operate on generalized, anonymized data. Applying risk assessment obligations to these processes unnecessarily conflates data processing and decision-making. This distinction is critical for enabling innovation while maintaining consumer privacy, as supported by frameworks like the EU's AI Act, which separates high-risk applications from foundational processes.

8. Explainability Requirements (Article 11, § 7220(c)(5))

Mandating plain language explanations of ADMT logic and key parameters creates undue burdens on businesses, especially when dealing with complex AI models. This requirement risks disclosing proprietary information and creating consumer confusion.

Proposed Amendment:

Strike § 7220(c)(5) and revise § 7220(c) to exempt trade secrets:

> **"Nothing in this section shall be construed to require disclosure of proprietary information, trade secrets, or other confidential business practices."**

Rationale:
Transparency requirements should balance consumer understanding with business confidentiality. The current proposal undermines this balance by requiring disclosures that compromise intellectual property while offering limited benefit to consumers. Exempting trade secrets aligns with global privacy standards, such as the GDPR, which emphasizes proportionality in transparency obligations.

9. Submission of Risk Assessments (Article 11, § 7157(b))

The draft's annual submission requirement for risk assessments is misaligned with state laws and could lead to assessments being designed for compliance rather than meaningful risk evaluation.

Proposed Amendment:

Amend § 7157(b) to limit submissions to high-risk activities only:

> **Businesses shall submit risk assessments solely for high-risk activities, including the sale of sensitive personal data or decisions resulting in legal or similarly significant effects on consumers.**

Rationale:
Privacy frameworks such as Colorado's CPA and Virginia's CDPA require risk assessments only for high-risk processing activities, ensuring regulatory efforts focus on areas where consumer harm is most likely. Limiting routine submissions to high-risk activities reduces unnecessary administrative burdens while maintaining meaningful oversight.

10. Cybersecurity Audits (§ 7123)

a. Redundancy and Inflexibility

The requirement that cybersecurity audits conform exclusively to CPPA's framework forces duplicative efforts.

Proposed Amendment:

> **"A business may satisfy the obligations set forth in Section 7120 by completing an audit using a recognized framework such as ISO 27001, SOC 2, or NIST CSF."**

Rationale:
Recognizing existing frameworks reduces compliance costs and avoids redundancy while maintaining rigorous security standards.

b. Outdated Controls

Prescriptive controls (e.g., MFA) risk obsolescence as technology evolves.

Proposed Amendment:

> **Focus on outcomes: "Organizations must demonstrate that their security practices achieve confidentiality, integrity, and availability of personal information."**

Rationale:
Outcome-based approaches align with global best practices, ensuring flexibility and long-term relevance.

c. Confidentiality Concerns

Submitting full audits without redacting sensitive information poses significant risks.

Proposed Amendment:

> **"Nothing in this article shall be construed as requiring a business to disclose trade secrets or other sensitive security information."**

Rationale:
Confidentiality safeguards protect trade secrets and mitigate the risk of exposing businesses to vulnerabilities.

11. <u>Trade Secret Protections (§ 7220, § 7222)</u>

Pre-use and access requirements risk exposing proprietary algorithms and methodologies.

Proposed Amendment:

> **"Nothing in this article shall require a business to disclose proprietary algorithms, trade secrets, or sensitive methodologies."**

Rationale:
These protections encourage innovation and prevent competitive disadvantages while ensuring businesses can comply without compromising critical assets.

* * *

IAB commends the CPPA's efforts to protect consumer privacy while fostering transparency in automated decision-making. However, the proposed regulations require significant revisions to ensure consistency with legislative intent, minimize unnecessary burdens, and promote innovation.

We respectfully request the Agency to consider the redlined amendments outlined above and would welcome the opportunity to engage further in this process.

Thank you for your attention to these critical issues. Please do not hesitate to contact me at lartease@iab.com with questions about these issues.

Sincerely,

[redacted]

Lartease M. Tiffith, Esq.
Executive Vice President for Public Policy
Interactive Advertising Bureau

Grenda, Rianna@CPPA

From: Austin Heyworth <austin@heygovt.com>
Sent: Thursday, February 13, 2025 3:00 PM
To: Regulations@CPPA
Subject: InternetWorks - CPPA ADMT Rulemaking Comments
Attachments: CA CPPA ADMT IW Comments - 2.13.25 - FINAL.docx.pdf

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

CPPA team, please find attached comments on behalf of InternetWorks for the open comment period for the ADMT rulemaking.

Thank you for considering.

Austin Heyworth
(626)818-6322
Austin@heygovt.com

Internet.Works

February 13, 2025

VIA EMAIL TO:

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

Re: Comments On Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies

Dear Board Members:

Internet Works (IW) is a trade association of diverse members working together to right-size technology policy, especially for middle tech companies, and promote trust and safety online. Our goal is to ensure our users are represented in important policy conversations and that state and federal policies continue to promote innovation, protect freedom of expression, and maintain choice in products and services. Our trade association is comprised of 21 companies, all of which directly support millions of small businesses and entrepreneurs, with a substantial number based in California.

IW appreciates the opportunity to provide feedback on the proposed regulations related to automated-decision systems and mandatory risk assessments. While this effort to enhance transparency and protect consumer rights is laudable, we have concerns about the scope, practical implementation, and unintended consequences of the proposed framework. We also encourage the view that the tech community is not a monolith. Middle tech companies play a critical role in the broader AI landscape, leveraging AI to drive innovation, boost productivity, and expand access to products and services - all of which impact the industry's competitive dynamics and ability to serve consumers.

As such, we support a balanced regulatory framework that provides legal certainty to both the entities developing and integrating or deploying AI. This includes standards for fair collection of data, sharing of information, and responsibilities across the AI value chain. Above all, there should be a risk-based approach which recognizes the tradeoffs that come with heightened regulatory obligations that may not have a clear policy benefit.

IW offers the following policy considerations for consideration:

Definition of ADMT

In general, IW encourages a narrowed definition which focuses on high-risk tools with significant consumer impact, excluding routine or low-risk applications. The revised definition of "Automated Decision System" (ADS) in § 11008.1 is overly expansive and vague. By defining an ADS as any "computational process" that "makes a decision or facilitates human decision-making," it could encompass basic tools like search results or basic binary screener questions, which are not AI-driven. The inclusion of "statistics" and general "data processing techniques" further broadens the scope unnecessarily, capturing systems that do not rely on AI or machine learning. Further, the lack of clarity on what constitutes "screening" raises compliance challenges, especially for employers using third-party vendors for criminal history checks or background screening. Without explicit definitions, businesses may struggle to assess whether their systems align with regulations, exposing them to potential legal risks despite best efforts to comply. Clarification is needed to focus on technologies that genuinely involve algorithmic decision-making and carry a clear and obvious risk of bias or discrimination. Without doing so, the uncertainty for businesses about whether simple, low-risk automation tools fall under regulation is going to stall innovation and product development.

The currently proposed definition can be construed to encompass any software that processes personal data to execute, replace, or facilitate human decision-making and risks capturing routine tools like customer service chatbots or data analysis software. This broad scope creates unnecessary regulatory burdens and could stifle innovation. More specifically, in section §7001(f), the scope of what technology falls under the definition of "automated decision-making technology" is unreasonably broad, which will result in confusion for consumers and overly burdensome compliance efforts for companies. Further, "substantially facilitate human decision making" in section (§7001(f)(2)) should be removed from the ADMT definition or should be further narrowed and defined.

Exemptions for safety, security, and fraud prevention are essential but require clearer boundaries to prevent misuse. Similarly, safeguards for workplace and educational ADMT should balance consumer rights with operational needs. The proposed rules should maintain focus on consumer personal information and exclude business characteristics, business data, and business products.

We suggest the following definition of ADMT:

> "Automated decision making technology" means any solely automated technology that processes personal information and uses machine learning for the primary purpose of making a significant decision about a consumer without any human involvement."

Covered Uses of ADMT & "Significant Decision" Definition

The triggers for ADMT regulation –such as "significant decisions concerning the consumer" or "extensive profiling" – are defined so broadly that nearly any automated process involving consumer data could fall within scope. This creates ambiguity for businesses and risks overregulation, potentially stifling innovation without clear evidence of harm. For example, including first-party behavioral advertising alongside cross-context behavioral advertising under extensive profiling creates a disproportionate burden on businesses engaged in routine, non-invasive advertising practices.

Requiring pre-use notices and opt-outs for decisions affecting rights or access to goods, services, or opportunities is laudable but impractical in dynamic settings like searching through online marketplaces or community forums. For example, adherence to user guidelines in stipulated terms of service agreements are often enforced with automated tools. Requiring pre-notices and opt-outs in this context can negatively impact user safety. This is a critical function and may undermine platforms' ability to keep users safe and to promptly identify and action problematic content. Further, delays could harm consumers by slowing access to essential services like lending or healthcare. While spam filters, spreadsheets, and firewalls are excluded, the caveat that exempt tools used to circumvent regulations will fall under the rules creates uncertainty. Clearer guidance is needed to delineate exempt and non-exempt tools.

Opt-Out Rights

The benefit of many products is that they use automated processes to provide insights, recommendations, and more to meet consumer needs. In other words, the inherent value of the product is that the ADMT behind it is continually improving and adapting to users' preferences. It should be made clear, or the flexibility should be afforded in pre-use notices to make clear, that if a person chooses to opt out of a certain ADMT that is inherent to the value of the product, then an opt out is legally effectuated by no longer using the product in question. It would be unreasonable for this to be considered retaliation when this occurs. The requirement for detailed explanations of ADMT logic may overwhelm consumers with technical jargon and dilute the impact of meaningful privacy disclosures. Creating an alternative process to accommodate consumers who opt out may be impossible or, at least, dramatically more costly to implement. We encourage the agency to reconsider whether opt-outs will achieve the intended policy objectives.

The limitations on opt-outs will undoubtedly denigrate certain product offerings and consumer experiences. Businesses may struggle with the operational complexities of stopping ADMT processing and ensuring all shared data is retrieved from third parties. Above all, we encourage emphasis on consumer clarity through pre-use notices to enhance consumer understanding and usability.

Risk Assessments

In general, risk assessments should prioritize risk based on context and function, not gathering excessive technical or business details. Requirements to disclose intended outputs, logic, or expected profits are impractical, exceeding GDPR standards and imposing compliance burdens. Many businesses, especially developers, lack full visibility into AI deployment. These detailed obligations increase compliance costs and force companies to tailor assessments specifically for California, requiring new expertise and diverting resources from core operations. Streamlining risk assessments to focus on high-level, relevant risks would reduce unnecessary burdens, including by striking section 7157(b)(2-5). The regulation also improperly classifies economic impacts (e.g., price changes) as privacy risks, which should be removed.

We encourage a reduced frequency of risk assessment submissions to every three years to minimize administrative burden while ensuring robust privacy oversight. Assessments should focus on high-risk processing activities rather than applying a blanket requirement across broadly defined categories. The draft's requirement to evaluate the risks of ADMT against potential benefits, including business profits, lacks clarity on how such evaluations will be standardized. This could lead to inconsistent or subjective assessments.

Mandating annual risk assessments and executive certifications imposes significant administrative costs.

Not all sharing of personal information should necessitate a risk assessment. For instance, most organizations share minimal personal information with third parties for advertising purposes. Requiring extensive risk assessments for such de minimis data-sharing activities diverts focus from more critical and high-risk data-sharing practices. The inclusion of behavioral advertising under "extensive profiling" is overly broad, particularly when it involves first-party data. Behavioral advertising differs significantly from physical surveillance and should not be equated with it.

The proposed balancing test imposes significant administrative burdens on businesses while offering limited consumer privacy benefits. We disagree with the assumption implied in the draft rules that all personal data processing has potential negative impacts on consumer privacy, which is not always the case. Many processing activities, particularly those with minimal data use, have neutral or even positive effects on consumers. Applying the balancing test as proposed may lead to inconsistent outcomes across organizations, undermining the clarity and predictability essential for compliance. Lastly, we encourage more detailed guidance on the application of ADMT rules to deepfake technologies to ensure they target malicious uses without hindering legitimate AI innovation.

Excessive Liability for Vendors
The expanded definitions of "agent" and "employment agency" unfairly extend liability to third-party vendors, service providers, and platforms. These entities, even if merely implementing employer-set requirements, could be held responsible for discrimination risks beyond their control. This broad liability imposes unpredictable and undue legal risks on businesses across the supply chain, including those with minimal involvement in hiring decisions. Under this construct, vendors, service providers, and platforms may need to halt certain business operations in order to not face incalculable legal liability.

Cybersecurity

The proposed regulations expand cybersecurity audit obligations beyond industry standards and that of other jurisdictions, imposing an undue burden on all CCPA-covered businesses. Section 7120(b) incorrectly assumes that any business subject to CCPA presents a significant security risk, and with it, unnecessary annual audits. Section 7123(b)(2) mandates cybersecurity requirements beyond statutory authority, prescribing rigid controls rather than focusing on audits. Cybersecurity must evolve to address emerging threats, making a prescriptive checklist ineffective. Instead, audits should assess security programs holistically against recognized frameworks. These frameworks include: NIST CSF, ISO 27001 and SOC-2. We encourage the inclusion of *all* the recognized frameworks, not just NIST CSF or any other one in particular.

Mandating businesses to document security gaps (§ 7123(c)(3)) could expose them to undue scrutiny in the event of a breach. Similarly, requiring disclosure of incidents reported to out-of-state regulators (§ 7123(e)) exceeds CPPA's jurisdiction and lacks auditor expertise. These provisions should be struck. Finally, waiver criteria are overly prescriptive, thereby limiting flexibility. Waivers should allow audits to serve as substitutes without rigid proof of compliance with each element.

Economic Impact Underestimated and Uneven

The proposed regulations fail to account for the significant fiscal impact on businesses, particularly small medium-sized enterprises. Similar legislation, AB 2930, was estimated to cost tens of millions annually for compliance and CPPA's own regulatory impact assessment estimates compliance costs of up to an astounding $3.5 billion. Such a significant financial burden will disproportionately affect small and medium-sized businesses, potentially leading to widespread job losses as companies restructure and adapt to the new requirements. These costs risk stifling innovation, reducing competitiveness, and creating barriers to entry for smaller entities. We urge the CPPA to conduct a more detailed cost-benefit analysis and explore phased implementation or alternative approaches that achieve regulatory objectives without jeopardizing jobs and economic stability.

The focus on avoiding discriminatory outcomes demands regular audits and adjustments to AI systems, requiring technical expertise that many businesses may lack. Employers face liability risks even with good-faith efforts if unintended biases emerge, further complicating AI adoption. This will inevitably tip the competitive balance towards larger platforms with greater legal and engineering resources to absorb these obligations. The proposed penalties, coupled with the broad definition of ADMT, could result in disproportionate fines for inadvertent or low-risk violations. The CPPA should consider tiered penalties based on the severity and intent of noncompliance.

IW thanks you for the opportunity to provide our comments on this proposal. We would be happy to make ourselves available for a meeting to discuss these important issues with you further. We look forward to working with you and your staff and supporting California as a home to the technology industry.

Respectfully submitted,

[redacted]

Peter Chandler
Executive Director, Internet Works
https://www.theinternet.works/

Grenda, Rianna@CPPA

From: Hammer, Alyce A. <alyce.hammer@faegredrinker.com>
Sent: Wednesday, February 19, 2025 5:36 PM
To: Regulations@CPPA
Cc: Abrahamson, Reed
Subject: Comment on Proposed Regulations - International Pharmaceutical & Medical Device Privacy Consortium (IPMPC)
Attachments: International Pharmaceutical & Medical Device Privacy Consortium (IPMPC) - Comment on Proposed CPPA Regulations (February 2025).pdf

To: California Privacy Protection Agency Board

Dear all,

Please see the attached comments regarding the Agency's Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies. These comments are submitted on behalf of the International Pharmaceutical & Medical Device Privacy Consortium (IPMPC). If you have any questions, please do not hesitate to contact the IPMPC Secretariat at reed.abrahamson@faegredrinker.com.

With thanks,
IPMPC Secretariat

Alyce A. Hammer
Associate
Pronouns: she/her/hers
Admitted only in Maryland; supervision by principals of the firm admitted to the D.C. bar
alyce.hammer@faegredrinker.com
Connect: vCard

+1 202 230 5304 direct

Faegre Drinker Biddle & Reath LLP
1500 K Street, N.W., Ste. 1100
Washington, DC 20005, USA

IPMPC
International Pharmaceutical &
Medical Device Privacy Consortium

February 19, 2025

California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, California 95834

Subject: Public Comment on Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies

The International Pharmaceutical & Medical Device Privacy Consortium ("IPMPC") welcomes the opportunity to provide comments in response to the request from the California Privacy Protection Agency Board (the "Agency") for comment on the proposed draft California Consumer Privacy Act ("CCPA") updates, in addition to the proposed regulations on cybersecurity audits, risk assessments, automated decisionmaking technology ("ADMT"), and insurance companies.

The IPMPC is comprised of chief privacy officers and other data privacy and security professionals from a number of research-based, global pharmaceutical and medical-device manufacturers. The IPMPC is the leading voice in the global pharmaceutical and medical device industry to advance innovative privacy solutions to protect patients, enhance healthcare, and support business enablement.[1]

We thank the Agency for the opportunity to comment and for understanding the important role artificial intelligence takes in our modern society. We are grateful for the Agency's addition of several illustrative examples in the proposed regulations as this allows businesses to better understand their rights and obligations. We encourage the Agency to add further examples.

Our specific comments follow below.

§ 7001(f) – Definitions ("ADMT")

We ask the Agency to revise the definition of "ADMT" by tailoring the language in a way that specifically focuses on high-risk tools requiring human oversight. The proposed definition states that ADMT means "any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking." In its current state, the definition overbroadly encompasses, and thereby regulates, low-risk processing technologies. We suggest the Agency narrow the definition to "any **high-risk** technology **necessitating human oversight** that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking."

[1] More information about the IPMPC is available at https://www.ipmpc.org. These comments reflect the position of the IPMPC as an organization and should not be construed as the positions of any individual member.

§ 7150(b)(3)(B) – When a Business Must Conduct a Risk Assessment
§ 7001(g) – Definitions ("Behavioral advertising")

We ask the Agency to revise § 7150(b)(3)(B) by removing subsection (iii), which states that "extensive profiling" includes "[p]rofiling a consumer for behavioral advertising." Behavioral advertising should not be included as a category of "extensive profiling" because advertisements are incapable of making decisions; rather, advertisements are a method of communication used to promote products and services. By subjecting behavioral advertising to the regulations' extensive profiling requirements, businesses would be limited in their ability to reach individuals that may benefit from their products or services. This is particularly crucial in the life sciences industry, where pharmaceutical and medical device companies advertise to inform patients and caregivers about medications, devices, treatment options, and patient support programs.

Accordingly, we ask the Agency to narrow the definition of "behavioral advertising" to exempt first-party advertising. Currently, "behavioral advertising" is defined to mean "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." Businesses should have the ability to market directly to their own consumers, and the data collected is already subject to robust comprehensive data privacy law requirements under the California Consumer Privacy Act and its subsequent regulations. We ask the Agency to revise § 7001(g) as follows:

> "Business 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~~.
>
> (1) Behavioral advertising includes cross-context behavioral advertising.
>
> **(2) Behavioral advertising does not include the consumer's personal information obtained from the consumer's activity within the business's own distinctly-branded websites, applications, or services.**
>
> ~~(2)~~ **(3)** Behavioral advertising does not include nonpersonalized advertising, as defined by Civil Code section 1798.140, subdivision (t), provided that the consumer's personal information is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business, and is not disclosed to a third party.

§ 7155 – Timing and Retention Requirements for Risk Assessments
§ 7157 – Submission of Risk Assessments to the Agency

We ask the Agency to harmonize the proposed risk assessment submission requirements with other state comprehensive privacy law risk assessment requirements. In its current form, § 7157(a) requires businesses to both submit risk assessment materials twenty-four months after the effective date and then subsequently submit risk assessment materials annually to the Agency. Unlike these regulations' annual reporting requirement, other states have adopted an incident-based approach. An incident-based approach would require businesses to submit risk assessment materials to the Agency or the California Office of the Attorney General only upon request (*See, e.g.,* Colo. Rev. Stat. § 6-1-1309(4); *see also* Va. Code Ann. § 59.1-580(C)).

Additionally, § 7155(a)(3)'s requirement that "a business must *immediately* update a risk assessment whenever there is a material change relating to the processing activity" is unrealistic [emphasis added]. A standard requiring a business to update a risk assessment within a reasonable period of time, or within a period of business days, would be more realistic given the time and effort that goes into properly conducting a risk assessment.

§ 7121 – Timing Requirements for Cybersecurity Audits

We ask the Agency to adjust the timing of cybersecurity audits as these requirements are inconsistent with other, similar timing obligations. In its current form, § 7121 requires businesses to both submit cybersecurity audits twenty-four months after these proposed regulations' effective date and then subsequently submit cybersecurity audits annually to the Agency. However, other states have adopted an incident-based approach for their risk and impact assessments (*See, e.g.,* Colo. Rev. Stat. § 6-1-1309(4); *see also* Va. Code Ann. § 59.1-580(C)). We ask for alignment with these other U.S. state requirements.

§ 7122 – Thoroughness and Independence of Cybersecurity Audits

We ask the Agency to strike § 7122(i)'s requirements that cybersecurity audits be certified by a business's board of directors or governing body. Boards of directors are not well-situated to certify in-depth cybersecurity audits or approvals or cyber policies. Additionally, boards of directors are not well-situated to evaluate the performance of and set compensation for an internal auditor. Many businesses, specifically in the life sciences industry, maintain employees with better understandings of cybersecurity requirements and audit regulatory processes; these employees would be better positioned for certification. We ask that the Agency change § 7122(i) to the following:

> The cybersecurity audit must include a statement that is signed and dated by **~~a member of the board or governing body, or if no such board or equivalent body exists,~~** the business's highest-ranking executive with authority to certify on behalf of the business **~~and~~ or** who is responsible for the business's cybersecurity program. The statement must include the signer's name and title, and must certify that the business has not influenced or made any attempt to influence the auditor's decisions or assessments regarding the cybersecurity audit. The statement also must certify that the signer has reviewed, and understands the findings of, the cybersecurity audit.

§ 7123(b)(2)(C) – Scope of Cybersecurity Audit

We ask the Agency to alter § 7123's subsection (b)(2)(C) requirement to have zero trust architecture identified, assessed, and documented in annual cybersecurity audits. While this is an admirable concept, zero trust architecture is not currently a feasible option for many businesses, and this novel requirement may lead to confusion and accidental noncompliance. We ask the Agency, therefore, to either consider removing this requirement or making it optional until a future date (for instance, making this an optional requirement until four years after the effective date).

§ 7123(b)(2)(N) – Scope of Cybersecurity Audit

We ask the Agency to clarify the scope of its § 7123(b)(2)(N) requirements. § 7123(b)(2)(N) states that a cybersecurity audit must specifically identify, assess, and document components of that business's cybersecurity program, which includes "[s]ecure development and coding best practices, including code reviews and testing." In its current form, it is unclear which entities are subject to this requirement. Particularly, developers of artificial intelligence systems are the ones coding and developing such systems—not deployers or distributors. This provision would greatly benefit from clarification regarding whether this requirement applies only to developers, and if not, what specific type of work is subject to this requirement since only a select few are charged with developing and coding the system.

§ 7124(b) – Certification of Completion

We ask the Agency to clarify the certification requirements listed in § 7124(b). Currently, § 7124(b) states that the "written certification must be submitted to the Agency through the Agency's website at https://cppa.ca.gov/ and must identify the 12 months that the audit covers." We suggest the Agency provide more details regarding this submission process. For instance, can any person submit the certification on behalf of the business, or must it be submitted by an authorized representative? Additionally, is there a specific format in which the certification must be submitted, or may it be submitted in any format? More guidance would allow businesses to feel more comfortable when submitting certifications and would lessen the risk of accidental noncompliance.

Conclusion and Contact Information

Thank you for considering our comments and recommendations. If you have any questions, you may contact Reed Abrahamson at reed.abrahamson@faegredrinker.com.

Sincerely,

/s/ Reed Abrahamson

Reed Abrahamson
Secretariat
International Pharmaceutical & Medical
Device Privacy Consortium (IPMPC)

Grenda, Rianna@CPPA

From:	Jessica Lee <jblee@loeb.com>
Sent:	Wednesday, February 19, 2025 11:58 PM
To:	Regulations@CPPA
Subject:	JessicaBLee_Comments
Attachments:	JessicaBLee_Comments(240851909.1).pdf

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Please see the attached.

Jessica Lee

Chief Privacy & Security Partner; Chair, Privacy, Security & Data Innovations

LOEB & LOEB LLP

345 Park Avenue | New York, NY 10154
Direct Dial: 212.407.4073 | **Fax:** 212.407.4990 | **E-mail:** jblee@loeb.com
Los Angeles | New York | Chicago | Nashville | Washington, DC | San Francisco | Beijing | Hong Kong | www.loeb.com

LOEB & LOEB LLP

JESSICA B. LEE
Chief Privacy & Security
Partner; Chair, Privacy,
Security & Data Innovations

345 Park Avenue
New York, NY 10154

Direct 212.407.4073
Main 212.407.4000
Fax 212.407.4990
jblee@loeb.com

February 19, 2025

VIA ELECTRONIC SUBMISSION

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

Re: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations ("Proposed Regulations")

I respectfully submit the following comments in response to the California Privacy Protection Agency's ("Agency") November 22 Notice of Proposed Rulemaking. I am submitting these comments in my individual capacity and not on behalf of Loeb & Loeb LLP or any of its or my clients.

I. 70001(c): Artificial Intelligence

Historically, data protection laws have provided data subjects with a right not to be subject to "automated decisions" made based on personal data. For example, Art. 22 GDPR provides: "[t]he data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." While automated decisions may be made using artificial intelligence ("AI") systems, AI itself expands well beyond the bounds of ADMT as it is typically defined and regulated under data protection laws. As the Agency stated in its Fact Sheet on the Draft Automated Decisionmaking CPPA Technology (ADMT) Regulations, "Artificial intelligence (AI) can be ADMT, but not all AI is ADMT."

Throughout the Proposed Regulations, the Agency refers to "automated decisionmaking technologies or artificial intelligence" as if they were distinct and separate triggers for the relevant obligations. (See, e.g. § 7153(a)). By doing so, the Agency appears to be creating an AI regulation within what should be a set of regulations designed to address data protection concerns. The California Consumer Privacy Act (CCPA) directs the Agency to make rules about access and opt-out rights relating to businesses' use of ADMT. The CCPA does not refer to AI, nor does it give the CCPA the authority to regulate AI that is not an ADMT.

Injecting references to AI into the Proposed Regulations creates confusion for both businesses and consumers. This confusion was made apparent during the February 19, 2025 public comment hearing when an individual representing the arts community submitted comments in favor of the Proposed Regulations due to their perceived ability to protect artists' content from being misused in AI systems. California's state legislature passed a series of bills in 2024 designed to regulate AI and appears poised to pass additional regulation in 2025. I would encourage the Agency to work with the state legislature rather than jumping ahead of it. The Proposed Regulations should either remove the reference to AI or limit its inclusion to 70001(f)(1).

II. 70001(f): Automated decisionmaking technology or ADMT

As noted above, Art. 22 GDPR provides individuals the right not to be subject to certain decisions made solely by ADMT. This right is designed to prevent individuals from being subject to an ADMT that may process their personal data in a manner that has a legal or significant effect without the influence of a human review. The Information Commissioner's Office ("ICO") in the United Kingdom provides an illustrative example[1] based on the UK's similar definition in its implementation of the GDPR:

> An employee is issued with a warning about late attendance at work. The warning was issued because the employer's automated clocking-in system flagged the fact that the employee had been late on a defined number of occasions. However, although the warning was issued on the basis of the data collected by the automated system, the decision to issue it was taken by the employer's HR manager following a review of that data. In this example the decision was not taken solely by automated means.

This example illustrates that while the ADMT helped inform the HR manager's decision, the HR manager had an opportunity to consider other factors before making a decision.

The Proposed Regulations expand this commonly accepted approach to regulating ADMT to include technologies that "substantially facilitate human decisionmaking," but do not make the decision on their own. The term "substantially facilitate" is vague and will leave businesses unsure about where to draw the line to determine whether a tool is an ADMT. In the ICO's example above, the automated clocking-in system would arguably be a "substantial factor" in determining whether to issue a warning regarding lateness, even if the HR manager also considered her own observations about the employees' timeliness.

This language becomes even murkier considering the human appeal exception in Section 7221(2). Going back to the example - where the HR manager is notified of the employee's lateness via the automated clocking system, but the HR manager reviewed that data and used her own judgment prior to rendering the decision - what is the utility of the appeal? The human appeal exception only makes sense when the right to opt-out is limited to decisions based solely on ADMT, not those where a human has already had the opportunity to review the information and use her own judgment.

III. 70001(g), 7150(B)(3), 7221(c)(1): Behavioral Advertising

The Proposed Regulations introduce a new definition of "Behavioral Advertising," which goes beyond the existing definition of cross-contextual behavioral advertising ("CCBA") to include targeted advertising within the business's own distinctly-branded websites, applications, or

[1] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-does-the-uk-gdpr-say-about-automated-decision-making-and-profiling/#id2

services. In Section 7150(B)(3), behavioral advertising is listed as an example of "extensive profiling." Most first-party advertising should not be considered "extensive profiling." As the FTC noted in its Fact Sheet on the FTC's Commercial Surveillance and Data Security Rulemaking,[2] the concern with certain types of advertising arises in connection with the use of tools that "can track every aspect of consumers' engagement online." This type of tracking, which is typically conducted using third-party cookies, is covered under the current definition of CCBA in the CCPA.

For most websites and mobile apps, there isn't an opportunity to engage in "extensive profiling" solely based on the individual's activities on the business' own websites and apps. The information collected from a consumer's interactions with one website or app is generally limited. Third-party cookies, data brokers, and other tools are designed to help businesses deepen their understanding of their consumers beyond what can be learned based on that individual's interaction with their own websites. Imposing restrictions on a business's ability to use the information it collects from its own direct interactions with its customers threatens to harm small businesses and publishers engaging in activities that do not rise to the level of extensive profiling.

Furthermore, by including a newly defined term for behavioral advertising and expanding the definition of CCBA, the Agency will force businesses to create another confusing set of consumer interactions. Under the Proposed Regulations, consumers have the right to opt out of ADMT. Section 7221(c)(1) requires businesses to provide an opt-out of ADMT using a link titled "Opt-out of Automated Decisionmaking Technology." As currently drafted, the Proposed Regulations will require businesses whose sole use of ADMT is via behavioral advertising to have a Do Not Sell/Share Link and an Opt-out of automated Decisionmaking Technology link. This creates a new set of operational burdens with no discernible benefit to the consumer, who will not understand whether she needs to opt out of both ADMT and sale/share or whether opting out of one will have an equivalent effect. Requiring yet another link will not increase the privacy protection for consumers.

The Agency should strike the proposed definition of Behavioral Advertising. Instead, the Agency can rely on the existing definition of CCBA. Additionally, the Agency should clarify that a business who provides an opt-out of CCBA under the existing CCPA regulations, can rely on that existing opt-out mechanism to facilitate the opt-out of ADMT, solely with respect to the CCBA.

IV. 7022(f): Requests to Delete

The Agency should clarify that while a business may need to implement measures to prevent the recollection of data from third parties after a deletion request, this obligation does not extend to acts taken by consumers. For example, if a consumer visits a website after making a deletion request, makes a purchase, or otherwise provides information or engages with a business in a manner that would result in the collection of personal information, that should not impact the determination that the business complied with the deletion request.

V. 7026(f)(3): Requests to Opt-out of Sale/Sharing

[2] https://cppa.ca.gov/meetings/materials/adt_regulations.pdf

While a business that uses programmatic advertising technology on its website may be able to instantaneously opt a consumer out of a sale/share via the cookies on its website, that business may engage in other sales/shares for which an instant opt-out is not feasible. For example, other sales or shares may take place via the transfer of data using an API. The Agency should clarify the example in this section to make it clear that Business U is not expected to opt consumers out of all sales or shares instantaneously, but only the sales or shares where an instant opt-out is feasible.

I appreciate the time and opportunity to submit these comments.

Sincerely,

[redacted]

Jessica B. Lee
Chief Privacy & Security Partner; Chair, Privacy, Security & Data Innovations

From: Celeste Wilson
To: Regulations@CPPA
Subject: Long Beach Area Chamber of Commerce Written Comment
Date: Wednesday, February 19, 2025 5:13:54 PM
Attachments: 2_19_2025_Opposition_CPPA Rulemaking.docx

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Good afternoon,

My name is Celeste Wilson, I am the Long Beach Area Chamber of Commerce's (LBACC) new internal Government Affairs Manager. Attached is the formal written comment on behalf of the LBACC re: CPPA Public Hearing.

Thank you,

--

Celeste Wilson
Government Affairs Manager
Long Beach Area Chamber of Commerce
1 World Trade Center Ste 101
Long Beach, CA 90831
Direct: 562-435-9594
Cell: [redacted]
Email: cwilson@lbchamber.com

The Chamber
Long Beach Area Chamber of Commerce

The Long Beach Business Organization since 1891
Catalyst for business growth, Convener of leaders and influencers, and a Champion for a stronger community

February 19, 2025

California Privacy Protection Agency
2101 Arena Boulevard
Sacramento, CA 95834

Subject: Proposed Regulations on CPPA Updates Cybersecurity Audits, Risk Assessments, Automated Decision Making Technology (ADMT), and Insurance Companies

Dear California Privacy Protection Agency,

On behalf of the Long Beach Area Chamber of Commerce, representing nearly 900 businesses, I write to express strong opposition to the CPPA's decision to advance formal rulemaking on proposed privacy and security regulations, which present significant economic and legal challenges, and respectfully request that further modifications of the proposed regulations are conducted at a future Board Meeting. While consumer protection is an important priority, the proposed regulations present significant economic and legal challenges that must be addressed before moving forward.

In alignment with CalChamber's concerns, there are several issues regarding the CPPA's proposed privacy and security regulations. Firstly, the CPPA's Standardized Regulatory Impact Assessment (SRIA) underestimates the financial burden these regulations will impose on businesses, consumers, and governments. The proposed changes could lead to substantial economic losses, including reduced employment and diminished tax revenues. For example, the extension of opt-out rights to first-party behavioral advertising risks reducing online publishers' revenue while increasing advertising costs for businesses. This would particularly harm small businesses that rely on affordable digital advertising and e-commerce sales to compensate for limited brick-and-mortar presence.

Second, the CPPA appears to exceed its statutory authority by proposing regulations on topics not explicitly authorized by statute, such as artificial intelligence (AI) and Automated Decision-Making Technologies (ADMT). Voters did not grant the agency authority over AI, and any implied authority should be strictly limited to regulations that directly further the purposes of the California Consumer Privacy Act (CCPA). Expanding the CPPA's jurisdiction in this way risks creating uncertainty and overreach that could stifle innovation and place California businesses at a competitive disadvantage.

Finally, the proposed regulations fail to adhere to the voter-approved timeline, which requires a one-year gap between the adoption of final regulations and their enforcement. This timeline is critical for ensuring that businesses have adequate time to understand and implement new compliance requirements. Enforcing regulations without this buffer risks imposing unfair burdens, especially on small businesses with limited resources for legal and technical compliance.

While we recognize the importance of consumer privacy protections, it is essential that these rules do not come at the expense of economic prosperity and entrepreneurial encouragement. For instance, businesses that experience frustrated customers leaving their websites due to burdensome opt-out mechanisms or restricted ability to communicate critical information will face revenue losses. These impacts are particularly concerning for small businesses in Long Beach, many of which rely on internet sales and digital engagement to thrive.

California is already grappling with an affordability crisis for both consumers and business owners. The added compliance costs these regulations introduce could further discourage businesses from operating in the state, driving up costs for consumers and reducing opportunities for economic growth.

On behalf of the Long Beach Area Chamber of Commerce, I respectfully request that the CPPA defer adoption of the proposed regulations until further analysis of their economic impact can be conducted. Specifically, we urge the agency to:

1. Reassess the economic implications of the proposed regulations, particularly for small businesses.
2. Ensure that regulatory changes remain within the scope of statutory authority as outlined in the CCPA.
3. Provide a full 12-month compliance period after final regulations are adopted to give businesses sufficient time to adapt.
4. Work collaboratively with stakeholders to develop balanced rules that protect consumers while supporting economic growth.

Thank you for your attention to this important matter. We stand ready to work with the CPPA to find solutions that safeguard consumer privacy without undermining California's economic vitality.

Sincerely,

[redacted]

Jeremy Harris
President & CEO
Long Beach Area Chamber of Commerce

Grenda, Rianna@CPPA

From:	Jerick Sobie [redacted]
Sent:	Tuesday, February 18, 2025 9:02 AM
To:	Regulations@CPPA
Subject:	Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments:	JerickSobieCPPAPublicComment (1).pdf

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Dear CPPA,

My name is Jerick Sobie, and I'm a California-based small business owner (co-owner, Lucky Feet Shoes). I'd like to submit the following comment to the CPPA for consideration during the public hearing on Feb. 19th.

Public Comment on Proposed ADMT Rulemaking Actions

California Privacy Protection Agency Public Hearing
February 19, 2025

Jerick Sobie, owner, Lucky Feet Shoes
Temecula, CA

Good Afternoon, Chair Urban and Board Members.

Thank you for letting me speak today. My name is Jerick Sobie, and I'm co-owner of Lucky Feet Shoes. We have 13 shoe stores employing 62 people in southern California. Our website is vital to our business, and I'm worried that the CPPA's proposed pop-up screen requirements for cookie consent, promotional communications, information on automated decision-making technology, and opt-out offers will badly hurt us. We get over 100,000 website hits annually, so we'd be immediately affected by the requirements.

Lucky Feet Shoes sells footwear and arch supports that help people with foot, leg, and back pain. Our customers range from distance runners to diabetes patients. To fit people with the right shoes, we need them to come into our shops so our specialists can understand their specific health challenges, measure their feet, and analyze their gait.

To get people into our stores, we first need them to visit our website. Almost all our marketing directs people to our website, which we've spent years making as informative and easy-to-navigate as possible. People can buy shoes from our website, but its primary purpose is to guide them into our stores for a fitting.

If people have to navigate several pop-up screens to get to our site, we'll have a serious problem. According to *Forbes*, 61% of people will leave a website if they can't find what they’re looking for in 5 seconds, and 88% won’t return to a site where they had a bad experience. So the proposed pop-up screens will almost certainly mean fewer visitors to our website. That means fewer visitors to our stores, fewer sales — and fewer people getting help with their pain and mobility issues.

I have two additional concerns. First, the state estimates it will cost small businesses up to $92,000 to make their websites compliant with the new rules, and $20,000 a year for the next decade. That’s an enormous expense — and it doesn’t account for lost sales.

Second, new regulations often allow lawyers to prey on small businesses. They accuse us of noncompliance, then threaten to sue unless we pay a hefty settlement. It’s a nightmare, both financially and emotionally.

I appreciate your efforts to protect Californians’ privacy. But please consider revising these rules so they’re less punishing to small businesses like mine. Big businesses can afford to overhaul their marketing strategies, absorb reduced sales, and pay tech experts and lawyers, but those costs are devastating for small businesses like mine. Thank you again for allowing me to speak today.

Jerick Sobie
Lucky Feet Shoes
www.luckyfeetshoes.com

Public Comment on Proposed ADMT Rulemaking Actions

California Privacy Protection Agency Public Hearing
February 19, 2025

Jerick Sobie, owner, Lucky Feet Shoes
Temecula, CA

Good Afternoon, Chair Urban and Board Members.

Thank you for letting me speak today. My name is Jerick Sobie, and I'm co-owner of Lucky Feet Shoes. We have 13 shoe stores employing 62 people in southern California. Our website is vital to our business, and I'm worried that the CPPA's proposed pop-up screen requirements for cookie consent, promotional communications, information on automated decision-making technology, and opt-out offers will badly hurt us. We get over 100,000 website hits annually, so we'd be immediately affected by the requirements.

Lucky Feet Shoes sells footwear and arch supports that help people with foot, leg, and back pain. Our customers range from distance runners to diabetes patients. To fit people with the right shoes, we need them to come into our shops so our specialists can understand their specific health challenges, measure their feet, and analyze their gait.

To get people into our stores, we first need them to visit our website. Almost all our marketing directs people to our website, which we've spent years making as informative and easy-to-navigate as possible. People can buy shoes from our website, but its primary purpose is to guide them into our stores for a fitting.

If people have to navigate several pop-up screens to get to our site, we'll have a serious problem. According to *Forbes*, 61% of people will leave a website if they can't find what they're looking for in 5 seconds, and 88% won't return to a site where they had a bad experience. So the proposed pop-up screens will almost certainly mean fewer visitors to our website. That means fewer visitors to our stores, fewer sales — and fewer people getting help with their pain and mobility issues.

I have two additional concerns. First, the state estimates it will cost small businesses up to $92,000 to make their websites compliant with the new rules, and $20,000 a year for the next decade. That's an enormous expense — and it doesn't account for lost sales.

Second, new regulations often allow lawyers to prey on small businesses. They accuse us of noncompliance, then threaten to sue unless we pay a hefty settlement. It's a nightmare, both financially and emotionally.

I appreciate your efforts to protect Californians' privacy. But please consider revising these rules so they're less punishing to small businesses like mine. Big businesses can afford to overhaul their marketing strategies, absorb reduced sales, and pay tech experts and lawyers, but those costs are devastating for small businesses like mine. Thank you again for allowing me to speak today.

From:	Saunders, David P.
To:	Regulations@CPPA
Cc:	Mooney, Austin
Subject:	Public comment to CCPA UPDATES, CYBER, RISK, ADMT, AND INSURANCE REGULATIONS
Date:	Friday, February 14, 2025 2:42:58 PM
Attachments:	2-14-25 - CCPA Comment Letter from MWE on behalf of clients.pdf

This Message Is From an External Sender

WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

To Whom It May Concern:

Please see the attached comment letter.

Thank you for your consideration.

Best,
David

DAVID SAUNDERS (HE/HIM/HIS)
Partner
McDermott Will & Emery LLP 444 West Lake Street, Suite 4000, Chicago, IL 60606-0029
Tel +1 312 803 8305 Email dsaunders@mwe.com
Website | vCard | LinkedIn

Paul Cronin, Assistant to David Saunders
Email pcronin@mwe.com

CCPA UPDATES, CYBER, RISK, ADMT, AND INSURANCE
REGULATIONS

mwe.com
David Saunders
dsaunders@mwe.com
+1 312 803 8305

February 14, 2025

VIA EMAIL

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

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

Dear Board Members and Staff of the California Privacy Protection Agency:

McDermott Will & Emery appreciates the opportunity to submit these comments in response to the California Privacy Protection Agency's (CPPA) November 22, 2024 Notice of Proposed Rulemaking under the California Consumer Privacy Act (CCPA). These comments are not provided on behalf of McDermott Will & Emery. Rather, we submit these comments on behalf of certain of our clients who asked that we submit these comments on their behalf. These comments do not necessarily reflect the views of all of our clients. The clients for whom we submit these comments recognize the importance of individuals' privacy interests. These comments are meant to assist the CPPA in developing regulations that that are both clear and easily understood and that protect consumer privacy rights, while not imposing undue burden on businesses attempting in good faith to comply with the CCPA.

Section 7001(f) – Definition of Automated decisionmaking technology" or "ADMT"

We are aware that the definition of "automated decisionmaking" has been the subject of significant scrutiny. However, the definition as proposed continues to be overbroad, and inclusive of everyday technology use that is not fairly described as "automated decisionmaking."

In particular, our clients are concerned with the inclusion of technology processes that "substantially facilitate human decisionmaking." As defined in the proposed regulations, that phrase means any technology output that serves as a "key factor" in a human's decisionmaking. That definition is simply too broad and encompasses everyday use of technology from a calculator to a spreadsheet. It would be onerous – and practically impossible – for businesses to conduct risk assessments every time any employee uses a computer or machine to facilitate such decisionmaking. Take the following hypothetical as an example:

An HR manager is hiring for a new job. They are deciding between two candidates and decide to evaluate the aspects of the candidates based on the same set of criteria. The HR manager uses a spreadsheet and assigns scores to the importance of each factor (e.g., 1 through 5). The HR manager then indicates which candidate they think is best for each of the criteria. The manager uses a spreadsheet formula to add up the scores and decides to hire the candidate with the higher score.

Here, the only technology processing was the calculation of a score that was originated by a human and was derived of their own subjective views of the candidates. To say that this falls within the ambit of an "automated decisionmaking" activity is difficult to comprehend. Yet, under the plain language of the proposed regulations, that is arguably what this activity is. We encourage the CPPA to evaluate its proposed definition and focus its definition further to those activities where the technology "replace[s] human decisionmaking." *See* 7001(f). Where a human is the reason for a technology input and is the one rendering a decision based on the output, it is unreasonable to label a mere calculation, sorting, or similar process as "automated" decisionmaking.

Recommendation: Modify the definition of "automated decisionmaking" by removing the phrase "substantially facilitate human decisionmaking" and also remove the related definition in 7001(f)(2). That phrase, and its corresponding definition is so broad so as to not fairly give notice to businesses as to what activities might fall within it, and thus which activities might require assessments.

Section 7001(g), Section 7150(b)(3)(B)(iii), Section 7200(a)(1)(A)(ii) and Section 7221(b)(6) – "Behavioral Advertising"

The regulations would extend ADMT opt out rights and other requirements to "profiling for behavioral advertising," a proposed subcategory of automated decisionmaking technology. As the CPPA knows, the CCPA already requires that businesses provide an opt out right to consumers for "*cross context* behavioral advertising," defined as targeted advertising "based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services." *See* CCPA 1798.140(k). The proposed regulations would extend this opt out to advertising conducted entirely "within [a] business's own distinctly-branded websites, applications, or services." *See* 7001(g). In addition to the providing an opt out right, businesses that engage in these advertising practices would also be required to comply with the risk assessment, pre-use notice, and other ADMT-related requirements in the proposed regulations.

These novel requirements should be omitted from the final regulations. Due to the broad definitions of "profiling" and "behavioral advertising," the proposed regulations would impose onerous requirements on otherwise mundane – and consumer expected – advertising practices. Take two examples:

1. A touring band wants to categorize (or "profile") its past concertgoers based on city, so it can send targeted advertisements for concerts in its upcoming tour (e.g., "We're coming back to your city, get your tickets now!").

2. An online department store that sells clothes wants to use its customers' browsing and purchase history to recommend additional items of interest. Using solely "first party" data, it groups these customers based on interests, such as "streetwear" and "athleisure."

These practices are far removed from the "significant decisions" the ADMT rules are designed to protect, or for which the CCPA authorizes regulations in the first instance. Nonetheless, the proposed regulations would arguably impose the full scope of ADMT-related requirements on these practices, including that consumers first receive a pre-use notice informing them of their right to "Opt out of Automated Decisionmaking Technology." Requiring an opt out for such mundane advertising practices will only exacerbate consumer confusion—and many consumers who want to receive these advertisements may inadvertently "opt out" as a result of confusion over the meaning of "automated decisions" rather than making an informed choice to no longer receive first-party advertising.

The proposed regulations in this regard would also mark a major departure from existing US privacy law, which does not currently require opt outs for targeted advertisements based on "first party" data. Following the model set by the CCPA, other US state privacy laws impose targeted advertising opt outs that are limited to "cross context" advertisements: those where advertising is based on a consumer's activities across websites and over time. Through these opt outs, California and other states have embraced a model of consumer privacy that considers "third party" data to have different privacy implications from "first party" data—a model that is consistent with leading privacy scholarship that accepts privacy as context-driven norms. *See, e.g.,* Helen Nissenbaum, Symposium, *Privacy as Contextual Integrity*, 79 Wash. L. Rev. 119 (2004).

By abandoning this model and erasing the distinction between "third party" and "first party" advertising, the proposed regulations risk undermining the very privacy interests they aim to advance. Current "cross context" opt outs have created an incentive structure that rewards companies for finding ways to use data consumers have provided to them directly instead of relying on third party data. The proposed ADMT regulations would upend these incentives, stifling privacy-friendly innovation and competition.

Perhaps more concerning, the proposed regulations that arguably would reach first-party advertising overstep both the text and intent of the CCPA. The "cross context behavioral advertising" provisions in the CCPA were clearly intended to exclude "first party" advertising from the CCPA's opt out rights. The proposed regulations frustrate this purpose and are in direct conflict with the plain text of the CCPA.

<u>*Recommendation*</u>: Remove "behavioral advertising" provisions entirely, as they are mismatched with the concept of "automated decisionmaking" and likely to lead to increased consumer confusion over the exercise of privacy rights. At a minimum, the CPPA should remove "profiling for behavioral

advertising" from the proposed regulations' ADMT opt out requirements, due to the tension with the text of the CCPA and the potential to undermine rather than advance consumer privacy interests.

Section 7001(c) and Related Provisions Concerning Artificial Intelligence

The proposed regulations purport to extensively regulate the development and use of "artificial intelligence" systems. In particular, the proposed regulations would extend the risk assessments and related requirements to all "training" of "large language models." *See* 7150(b)(4). Additionally, the proposed regulations appear to apply all "automated decisionmaking" requirements to the practice of training any technology "capable of being used for" significant decisions or other ADMT purposes. *See* 7200(a)(3). In effect, the proposed regulations treat the development and training of artificial intelligence systems as a form of "automated decisionmaking technology."

The clients on whose behalf we provide these comments believe that these proposed regulations exceed the CPPA's rulemaking authority. Developing or "training" a technology is not the same as using technology to make a decision about an individual. And using data for product development is not "profiling" as defined in the CCPA. By using the CPPA's "automated decisionmaking technologies" authority to regulate such training and product development, the proposed regulations exceed the CPPA's rulemaking mandate.

Notably, to the extent artificial intelligence technologies are used in automated decisionmaking, they would already be covered by the proposed regulations. For example, if a company were to feed a large language model resumes of job applicants and ask the model to "decide which candidate to hire," and follow the model's recommendation, that (including within the definition of automated decisionmaking as proposed in this letter) would satisfy the definition (even as modified in the way we propose) of automated decisionmaking technology. The CPPA does not need a definition of "artificial intelligence" to ensure that these uses are within the scope of the proposed regulations. And the CPPA also does not need to regulate "training" or development of technologies in order to regulate later use cases. The introduction of proposed regulations related to "artificial intelligence" expands the CPPA's regulatory authority beyond its statutory mandate and effectively transforms the agency into California's artificial intelligence regulator, a role it has been neither authorized nor been budgeted to perform.

To be sure, recent advancements in artificial intelligence technologies have major policy implications. But these implications are already being addressed through the legislative process. The legislative process in California has resulted in rapid policymaking around artificial intelligence, with many new laws enacted in the last year—none of which gave the CPPA authority to regulate artificial intelligence development or training. *See* C. Kibby and R, Sentinella, IAPP, *New laws in California look to the future of privacy and AI* (November 27, 2024), https://iapp.org/news/a/new-laws-in-california-look-to-the-future-of-privacy-and-ai. The CPPA should respect the legislative process and not attempt to expand its already-broad jurisdiction into this nascent field.

Recommendation: The CPPA should remove the definition of "training automated decisionmaking technology or artificial intelligence" and all related provisions. The CPPA should also remove the definition of "artificial intelligence" entirely, as this technology would already be covered by the definition of "automated decisionmaking technology," to the extent employed for such purposes.

Article 9 Cybersecurity Audits and Section 7157 Submission of Risk Assessments to the Agency

Implicitly, Article 9 regarding Cybersecurity Audits and explicitly, Section 7157 regarding risk assessments, contemplate that a business may have to provide the CPPA with audits or assessments that ordinarily are privileged and/or protected by the work product doctrine. Yet, unlike other state consumer privacy laws, the proposed regulations offer no waiver protections to these materials.

It is common for businesses to consult with and seek the legal advice of counsel during the course of a risk or cyber assessment. As a result, some or all of the resulting assessment may be privileged and/or protected by the attorney work product doctrine. Indeed, it would be challenging for a business to conduct an evaluation of legal risks as required by the proposed regulations absent the input of counsel. Yet, nowhere in the proposed regulations is any acknowledgement of that fact. The clients on behalf of whom we submit this letter urge the CPPA to consider adopting safeguards like those in other states regarding the disclosure of privilege material to the CPPA.

For example, under the Colorado Privacy Act (CPA), when a business is required to provide a data protection assessment to the Colorado Attorney General, the CPA provides that the assessment is "confidential and exempt from public inspection and copying under the 'Colorado Open Records Act'" and that the production "does not constitute a waiver of any attorney-client privilege or work product protection that might otherwise exist with respect to the assessment and any information contained in the assessment." Colo. Rev. Stat. § 6-1-1309(4). Similar protections can be found in the laws of Connecticut (Conn. Gen. Stat. § 42-529(b)(f)); Delaware (Del. Code Title 6 § 12D-108), Indiana (Ind. Code Ann. § 5-14-3-4), Kentucky (Ky. Rev. Stat. § 367.3621(4)), Maryland (Md. Code Ann. 14-4610(D)(3), (G)), Montana (Mont. Code Ann. § 30-14-2814(3)(c), (d)), Nebraska (Neb. Rev. Stat. Ann. § 87-1116(4)), New Hampshire (N.H. Rev. Stat. Ann. § 507-H:8(III)), New Jersey (N.J. Stat. § 56:8-166.12(b)), Oregon (Or. Rev. Stat. Ann. § 8-646A-586(7)), Tennessee (Tenn. Code Ann. § 14-18-3206(c)), Texas (Tex. Bus. & Com. Code § 541.105(d)), and Virginia (Va. Code Ann. § 59.1-580(C)). These fourteen states recognize the importance of protecting the attorney-client privilege and work product nature of these assessments.[1]

The protections against public disclosure and against waiver of any privilege or work product protection is an essential part of any regime that requires businesses to produce to a government agency an otherwise internal assessment or audit performed with the assistance of legal counsel. *See Note, The*

[1] Additionally, in contrast to the risk assessment disclosure requirements in Section 7157, none of these states require proactive submissions of risk assessments without cause or request—another way in which the proposed regulations would mark a significant departure from existing U.S. privacy laws.

Privilege of Self-Critical Analysis, 96 Harv L Rev 1083, 1092 (1983) (concluding that, in the absence of privilege protections, compelled disclosures will create a "chilling effect on the institutional self-analyst's frankness or thoroughness, an effect that results from the threat of liability"). Absent protections like those in the statutes cited above, businesses would be presented with the Hobson's choice of (a) fully documenting their assessments and risking a waiver of privilege or work product protections or (b) not fully disclosing the full scope of their assessments in order to protect privilege, but not fully comply with the new regulations. This is an unfair choice that fourteen other states have recognized that businesses should not have to make.

Recommendation: Add into the proposed regulations protections for cybersecurity audits and risk assessments produced to the CPPA so that (a) there is no waiver of the attorney client privilege or work product doctrine and (b) the cybersecurity audits and risk assessments are exempt from open records laws disclosures.

Compliance Timeline

The proposed regulations introduce fifty pages of entirely new regulations, many of which have no corollary to any existing law in the United States. The CPPA appears to recognize the novelty of its proposals given the fact that it is proposing to give businesses 24 months to complete an initial cybersecurity audit and the same 24 month period to document any risk assessments for processing activities identified prior to the effective date of the proposed regulations. *See* §§ 7121, 7155(c). Our clients are appreciative of this period. However, our clients believe that there should be a compliance grace period for processing activities that are scheduled to begin within the first 6 months of the effective date of the new regulations as well.

Section 7155(a)(1) provides that "[a] business must conduct and document a risk assessment….***before*** initiating any processing activity" that is subject to a risk assessment. Because of the immediate effective date of the proposed regulations, that means if a business has been planning a product launch for months – or even years – but the launch happens to fall the day *after* the effective date of the proposed regulations, the business would have to *try* to complete a risk assessment against not-yet-effective regulations. Given the depth of analysis required for risk assessments, and the correlated time and resources required to complete those assessments, it would be reasonable for businesses in this position to have a grace period in which to complete a risk assessment for processing activities that were planned prior to the effective date of the proposed regulations, but that launched in the first 6 months after their effective date.

Recommendation: For processing activities that were (a) planned before the effective date of the proposed regulations and (b) that are initiated within the 6 months after the effective date of the proposed regulations, give businesses 12 months within which to complete the risk assessment required by the proposed regulations, calculated from the effective date of the proposed regulations.

* * *

We hope that the CPPA finds these comments helpful. On behalf of our clients, thank you for the opportunity to comment on the proposed regulations.

Sincerely,

[redacted]

David Saunders

[redacted]

Austin Mooney

Grenda, Rianna@CPPA

From:	Bjerke, Brandon <Brandon.Bjerke@asm.ca.gov>
Sent:	Wednesday, February 19, 2025 3:59 PM
To:	Regulations@CPPA
Subject:	Public Comment on ADMT
Attachments:	Legislative Letter to CPPA ADMT Regs 2192025.pdf

This Message Is From an External Sender

WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Hello,

Please find attached a public comment letter on Proposed Regulations on Automated Decisionmaking Technology from 18 Members of the Legislature.

Brandon Bjerke
Legislative Director
Office of Assemblywoman Jacqui Irwin
42nd District, California State Assembly
(916) 319-2042
Brandon.Bjerke@asm.ca.gov

Visit Assemblywoman Irwin's Website

California Legislature

February 19, 2025

California Privacy Protection Agency
2101 Arena Blvd
Sacramento, CA 95834

Subject: Public Comment on ADMT Regulations
Submitted via email: regulations@cppa.ca.gov

Chair Urban and Board Members Liebert, Mactaggart, Nonnecke, and Worthe:

We write as Members of the California Legislature to share our comments and concerns regarding the CPPA's Automated Decisionmaking Technology (ADMT), risk assessment, and cybersecurity audit rulemaking, and in particular on the proposed ADMT/AI related regulations.

As you are aware, the Legislature considered many bills related to artificial intelligence (AI) in 2024. We debated and passed bills dealing with the intersection of AI and copyright, public safety, education, discrimination, frontier model safety, security, transparency, privacy rights, labor issues, state procurement, and more. We grappled with complex public policy issues facing California and balanced protecting consumers and workers with championing innovation while maintaining our state's leadership as home to many of the world's leading AI companies. Needless to say, this is a significant public policy issue that the legislative branch will continue to weigh in on in the 2025-2026 session and beyond.

At the end of 2024, Governor Newsom signed almost 20 pieces of legislation on AI or generative AI, vetoing only a select few. The Governor shared a key component of his decisions was that "California is home to 32 of the world's 50 leading Al companies, pioneers in one of the most significant technological advances in modern history. We lead in this space because of our research and education institutions, our diverse and motivated workforce, and our free-spirited cultivation of intellectual freedom. As stewards and innovators of the future, [he takes] seriously the responsibility to regulate this industry." (Veto Message of SB 1047.)

In the end, Governor Newsom's unequivocal message to the Legislature and all Californians regarding AI regulation? "*We must get this right.*" The CPPA is not exempt from Governor Newsom's clear admonition that regulating AI must be done responsibly. Nor is it exempt from its inherent responsibility to Californians, as a responsible regulator, to do so. Particularly when there is so much on the line not just in terms of privacy rights but also other fundamental freedoms, as well as economic, societal, and moral impacts.

We disagree with Board Member Liebert's unfortunate suggestion that the Legislature is incapable of adequately legislating AI policy and the Board's incorrect interpretation that CPPA is somehow authorized to regulate AI. In truth, each of you must work with the Legislature and Governor Newsom to implement the specific statutory authority delegated to the Agency, rather than act alone.

Government Code Section 11349(b) states, "[a]uthority means the provision of law which permits or obligates the agency to adopt, amend, or repeal a regulation." The CPPA does not have authority to regulate any AI (generative or otherwise) under Proposition 24 or any other body of law. AI is not included in Proposition 24, and the Legislature has not granted the CPPA authority to regulate AI. The ADMT regulations currently being considered need to be scaled back to focus on the specific issue identified under Civil Code Section 1798.185 and avoid the general regulation of AI.

While we recognize CPPA's role in the regulatory setting, the CPPA must avoid operating in a vacuum when developing regulations. You voted to move these regulations forward with the knowledge they will cost Californians $3.5 billion in first year implementation, with ongoing costs of $1.0 billion annually for the next 10 years, and 98,000 initial job losses in California. That is nothing to say of the adverse impact on future investment and jobs noted by the analysis that will get moved to other states, or the startups that will get developed elsewhere. These are significant consequences which the Legislature and Governor Newsom have sought to avoid in our enacted legislation, and the CPPA should seek to avoid them as well.

It is also important to note that California could face a $2 billion deficit in 2025 as recently reported by the Legislative Analyst Office. Your votes to move these regulations forward are unlikely to help California's fiscal condition in 2025 and, in fact, stand to make the situation much worse. We urge you to take a broader view and redraft all of your regulations to minimize its costs to Californians. Moving forward, the CPPA must work responsibly with other branches of government to get these regulations right in order to avoid significant and irreversible consequences to California.

Sincerely,

[redacted]

Assemblymember Jacqui Irwin

[redacted]

Assemblymember David Alvarez

[redacted]

Assemblymember Lisa Calderon

[redacted]

Assemblymember Diane Dixon

[redacted]

Assemblymember Josh Hoover

[redacted]

Assemblymember Stephanie Nguyen

[redacted]

Assemblymember Blanca Pacheco

[redacted]

Assemblymember Darshana Patel

[redacted]

Assemblymember Joe Patterson

[redacted]

Assemblymember Gail Pellerin

[redacted]

Assemblymember Cottie Petrie-Norris

[redacted]

Assemblymember Sharon Quirk-Silva

[redacted]

Assemblymember Catherine Stefani

[redacted]

Assemblymember Avelino Valencia

[redacted]

Senator Anna Caballero

[redacted]

Senator Tim Grayson

[redacted]

Senator Brian Jones

[redacted]

Senator Akilah Weber Pierson, M.D.

Catbagan, Christian@cppa

From:	Michelle Calabro [redacted]
Sent:	Wednesday, February 19, 2025 9:58 AM
To:	Regulations@CPPA
Subject:	Response to California Consumer Privacy Act of 2018

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Hello,

I offer this feedback on the California Consumer Privacy Act of 2018, as a member of civil society.

Overall, the current draft of the CCPA is written to protect businesses and government entities by default, enabling them to collect, share and sell people's data without our knowledge or consent. "Consumer Privacy" is a misnomer, since our data is not protected by the California Consumer Privacy Act. The lack of transparency into data usage practices has led to an economy of exploitation and targeting that goes far beyond business use cases and also extends to government research which we are not made aware of, and which the CCPA itself acknowledges is problematic. People are not proactively informed in a meaningful manner, of the specific use cases of these trades, nor are we given an easy way to opt out, nor are we properly compensated for the use of our data.

The CCPA does a good job of addressing the themes related to privacy, and those should remain in its final iteration. But the current draft conceptualizes people as consumers, and consumers as passive entities. This is problematic given that people use the internet for reasons other than commerce, and that we live in a democracy, and democracies rely on active participation. If the CCPA's purpose is to protect people's privacy, it should take a human-centric approach, not a business-centric or government-centric approach. It must be written in plain language that's easy for people to understand so we can use it; it must not have any loopholes; and it must, above all, avoid negating itself.

Given the fact that most technology companies are headquartered in California yet the people who use the technologies live throughout the United States and far beyond our country's borders, I recommend that members of Congress work with their colleagues to make federal privacy protections. Many of the most extreme harms caused by data collection, use, sharing and selling are addressed in the EU AI Act, which was stress-tested in a policy sandbox before being ratified. I recommend US lawmakers review it before drafting federal law. Finally, the US should form an alliance for mutual defense.

Thank you for considering my perspective. I welcome the opportunity to provide feedback in greater detail.

Sincerely,
Michelle Calabro

Grenda, Rianna@CPPA

From:	Reem Suleiman <reems@mozillafoundation.org>
Sent:	Wednesday, February 19, 2025 2:32 PM
To:	Regulations@CPPA; Jennifer Hodges
Subject:	Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments:	Mozilla Comments CPPA Proposed Rulemaking_2.19.25.pdf

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Good afternoon,

Please find Mozilla's written comments (attached) on the CPPA's proposed rulemaking on "CCPA Updates, Cybersecurity, Risk, ADMT, and Insurance Regulations." Please reach out if you have any additional questions.

Thank you for the opportunity to provide input,
-Reem

--
Reem Suleiman (she/her)
US Advocacy Lead
Mozilla Foundation

MOZILLA'S RESPONSE TO THE CALIFORNIA PRIVACY PROTECTION AGENCY (CPPA) PROPOSED RULEMAKING ON "CYBERSECURITY AUDITS, RISK ASSESSMENTS, AND AUTOMATED DECISIONMAKING"

FEBRUARY 19, 2025

TABLE OF CONTENTS

I. MOZILLA'S VISION FOR THE INTERNET

Thank you for the opportunity to engage again[1] with the California Privacy Protection Agency on the rulemaking for "Cybersecurity, Risk Assessments, and Automated Decisionmaking Technologies". Mozilla is a global community working together to build a better internet. As a mission-driven organization, we are dedicated to promoting openness, innovation, security, and accessibility online. We are constantly investing in the security of our products, the internet, and its underlying infrastructure. We are also deeply vested in furthering our mission of trustworthy AI, which we lay out in our white paper "Creating Trustworthy AI",[2] to advance transparency and accountability in the use of automated systems. Owned by a not-for-profit foundation, a

[1] Mozilla Comments to CCPA Consultation https://blog.mozilla.org/netpolicy/files/2021/11/Mozillas-Comments-to-CCPA-Consultation-November-2021-6.pdf Mozilla Response to 2023 CPPA Request for Preliminary Comments on "Cybersecurity, Risk Assessments, and Automated Decisionmaking" https://cppa.ca.gov/regulations/pdf/rm2_pre_comments_1_26.pdf#page=487

[2] Ricks, B and Surman, M. "Creating Trustworthy AI." Mozilla. December 2020. https://assets.mofoprod.net/network/documents/Mozilla-Trustworthy_AI.pdf

foundational principle of Mozilla's guiding Manifesto[3] demands that individual privacy and security online must not be treated as optional.

II. MOZILLA ON CPPA RULEMAKING PROCESS

The CPPA's rulemaking procedure comes at a critical time. Last month, President Trump signed an Executive Order revoking the previous administration's Order on "Safe, Secure and Trustworthy Development and Use of Artificial Intelligence," and signalled significant policy changes and potential reversals[4] in the Office of Management and Budget guidelines around testing and transparency in AI systems[5]. Consequently, this lack of federal oversight over public sector procurement and uses of AI only heightens the necessity for state leadership, particularly in California, to institute sensible transparency measures, privacy protections, quality control, and guardrails against harmful AI use including for Automated Decision Making Technologies. Privacy is a critical component of AI policy, not just because AI has the potential to accelerate and exacerbate privacy related harms, but because at its heart, AI relies on the utilization of vast amounts of consumer data.

Mozilla supports the CPPA's effort to conduct rulemaking that examines cybersecurity audits, risk assessments, and automated decisionmaking as it further develops the proposed regulations that implement amendments to the California Consumer Privacy Act (CCPA). Overall we are encouraged to see new guardrails intended to offer consumers more agency in exercising privacy rights, and are open to having further discussion on several of the topics addressed in the proposed rulemaking in more detail, including the new proposed guardrails on ADMTs, cybersecurity audits, risk assessments, and curbing deceptive practices in detail. We believe real choice and transparency are the foundations of a healthy internet, and that these should be

[3] Mozilla Manifesto. https://www.mozilla.org/en-US/about/manifesto/

[4] See Civil Society letter to the White House on Untested AI https://consumerfed.org/wp-content/uploads/2025/01/Coalition-Letter_-Dont-Use-Untested-and-Opaque-AI-on-Seniors-Vets-and-Consumers_.pdf

[5] See Mozilla blog https://blog.mozilla.org/netpolicy/2024/03/28/us-government-use-of-ai/

afforded to all people – whether as consumers, public beneficiaries, workers, or otherwise.

III. MOZILLA'S FEEDBACK ON CYBERSECURITY AUDITS AND ADMT REGULATIONS

a. Cybersecurity audits:

Several of the proposed elements of the cybersecurity audit are widely accepted and socialized standards within the cybersecurity industry, such as multi-factor authentication, strong passwords, and encryption of personal information. In fact, these are reflected concepts in Mozilla's five basic minimum security standards we believe all products should meet. These require that the product must use encryption; the company must provide automatic security updates; if a product uses a password, it must require a strong password; the company must have a way to manage security vulnerabilities found in their products; and the company must have an accessible privacy notice.

However, there are aspects of the cybersecurity audit regulations that require further clarification or could be less prescriptive to allow for differing but rigorous approaches to cybersecurity management. In particular, the regulations in **§ 7123 Scope of Cybersecurity Audits (b) (2)(C)** require an audit of the "Zero trust architecture," which could encompass many different things. Unlike data-loss-prevention systems or antimalware protections, which are tools that can be audited, Zero Trust is a collection of principles, including least privileged access, continuous monitoring, and breach minimization. There are many ways an organization may implement a Zero Trust Architecture, including by focusing on identity governance, network segmentation, or deploying device agents. For example, Mozilla requires Endpoint Detection and Response (EDR) tools, Multi-factor Authentication (MFA), and Mobile Device Management (MDM). Mozilla is continually improving our Identity and Access Management practices, including by implementing Just-In-Time access. The CPPA's clarity on the intent and expectations for this particular section of the audit would be especially helpful.

b. Automated Decision Making Technology (ADMT)

Mozilla supports transparency measures – for consumers, workers, or public citizens alike – as an important step towards potentially identifying or mitigating harms, especially when coupled with guardrails on how an ADMT can be used. We are encouraged to see the CPPA outline the high-risk contexts in which an ADMT can be potentially deployed – either where sensitive data is concerned, when there is a consequential use case or decision to be made, or both. This risk-based approach is one that is likely to effectively protect consumers and those who might be negatively impacted by ADMT.

We support human intervention as an important way to validate decisions of high consequence for consumers, such as approval for a lower mortgage interest rate, rejection for an auto loan, or flagging someone as suspect in the criminal justice system. There may be a need, however, for guidance or further examples to show how businesses should implement this principle in practice. For example, it is not uncommon for companies to receive hundreds if not thousands of applicants for a particular job. If an employer uses an HR or recruitment management tool to sort applications, there is the challenge of offering a proper alternative at scale if applicants choose to exercise individual opt-outs on an ADMT processing their application. Applicants who choose to exercise opt-out rights may receive a disadvantage if the employer cannot offer a meaningful alternative. Similarly, it would be helpful to receive guidance from the Agency, wherever possible, on opportunities for companies to streamline various risk assessment obligations. For example, the CPPA can offer demonstrative examples of equivalently strong ADMT risk assessments.

IV. CONCLUSION

If we can provide any additional information that would be helpful, please do not hesitate to contact us. We look forward to continued engagement with the Agency, and would be happy to have discussions on the areas outlined above requiring further clarity. Thank you for the opportunity to provide feedback.

Contact for Additional Information

Reem Suleiman, US Advocacy Lead, Mozilla Foundation
reems@mozillafoundation.org

Jenn Taylor Hodges, Director of US Public Policy and Government Relations, Mozilla Corporation - jhodges@mozilla.com

Grenda, Rianna@CPPA

From:	Nick Meyer <nick@networkadvertising.org>
Sent:	Wednesday, February 19, 2025 11:42 AM
To:	Regulations@CPPA
Subject:	Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments:	NAI Comment on CCPA Updates 2.19.2025.pdf

Dear Ms. Sanders,

Attached are the NAI's comments on the CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations.

Please let us know if anything else is needed. Otherwise, have a wonderful day!

Best,
Nick

Nick Meyer
Counsel, Compliance & Policy
The NAI
409 7th Street, NW, Suite 250, Washington, DC 20004
P: 408.394.9612 | nick@networkadvertising.org

--

To help protect your privacy, Microsoft Office prevented automatic download of this picture from the Internet.

To help protect your privacy, Microsoft Office prevented automatic download of this picture from the Internet.

NAI
PRIVACY, TRUST & ACCOUNTABILITY

409 7th Street, NW; Suite 250
Washington, DC 20004

February 19, 2025

Submitted via electronic mail to regulations@cppa.ca.gov

California Privacy Protection Agency
Attn: Legal Division - Regulations Public Comment
2101 Arena Boulevard
Sacramento, CA 95834

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

To the California Privacy Protection Agency:

On behalf of the Network Advertising Initiative ("NAI"), thank you for the opportunity to comment on the proposed regulations regarding CCPA Updates, Insurance, Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking Technology under the California Consumer Privacy Act (the "Proposed Regulations").[1] The NAI shares the concerns the California Privacy Protection Agency (the "Agency") has expressed regarding the proliferation of Automated Decisionmaking Technology ("ADMT") in the everyday lives of consumers and, as such, we support the Agency's efforts to introduce much-needed regulations to protect consumers and provide them with additional rights regarding businesses' use of ADMT. The NAI also applauds the ongoing commitment to public involvement and transparency the Agency is demonstrating through this important rulemaking process.

In addition to providing information about the NAI, we offer the following comments and recommendations related to the Proposed Regulations, which we hope will assist the Agency in meeting its objectives for the rulemaking while preserving a free, open, and secure internet for all California consumers:

- Remove Cross-Context Behavioral Advertising ("CCBA") from the definition of "Behavioral Advertising" to avoid presenting consumers with duplicative and potentially confusing choices.
- Consolidate the additional disclosures proposed for the ADMT Pre-Use Notice with the existing Notice at Collection requirements.
- Remove the proposed "remains deleted" language in section 7022 of the CCPA regulations to avoid inconsistencies with existing requirements to *permanently and completely* erase data.
- Clarify that, when conducting risk assessments, businesses must ensure that their use of ADMT does not *unlawfully* discriminate based upon protected classes.
- Clarify that the proposed right to access ADMT does not require a business to reveal any trade secrets when responding to a verifiable consumer access request.

[1] California Privacy Protection Agency Proposed Text, Cal. Code Regs. tit. 11 (proposed Nov. 22, 2024) (hereinafter "Proposed Regulations").

- Harmonize the attestation requirements for ADMT risk assessments with the grace period that relieves businesses from immediately conducting risk assessments of ADMT processing initiated prior to the effective date of the Proposed Regulations..

These comments are set forth in more detail below.

I. About the NAI

The NAI is a non-profit, self-regulatory association dedicated to responsible data collection and use for digital advertising. The NAI has been a leader in this space since its inception in 2000,[2] promoting the highest voluntary industry standards for member companies, which range from small startups to some of the largest companies in digital advertising. NAI's members are providers of advertising technology solutions and include ad exchanges, demand and supply side platforms, and other companies that power the digital media industry by helping digital publishers generate essential ad revenue, helping advertisers reach audiences interested in their products and services, and helping to ensure consumers are provided with ads relevant to their interests.

The NAI was founded on a mission of responsible data collection and use for digital advertising to promote economic and societal benefits to consumers. In further accordance with this mission, the NAI recently brought together member companies and leading industry privacy experts to develop and launch our new NAI Accountability and Self-Regulatory Framework ("Framework").[3] The new Framework consists of five fundamental principles for privacy in digital advertising which our member companies must adhere to. The new Framework not only prepares NAI member companies for the ever-evolving legal and regulatory environment in which they are operating in, it reinforces the NAI as a leader in this new era of self-regulation and privacy. We offer the following detailed comments on the Proposed Regulations, which we are hopeful will assist the Agency in meeting its objectives for the rulemaking while preserving an open, global, and secure internet for all consumers.

II. The Agency should remove "Cross-Context Behavioral Advertising" from the proposed definition of "Behavioral Advertising" to avoid confusing consumers without sacrificing privacy protections.

Notice about and consumer control over certain uses of personal information are important and fundamental privacy protections. However, in order for those protections to be effective, they must be presented in simple, clear, and unambiguous terms. Otherwise, choices presented to consumers risk creating confusion about what choices are being offered and how they may be exercised – an issue the Agency has been appropriately attentive to through its focus on dark patterns.[4] However, by including CCBA – a term already clearly defined and regulated by the CCPA – within the umbrella term "behavioral advertising," the Agency risks creating unnecessary confusion among consumers seeking to exercise different opt-out rights without any corresponding privacy benefit. As explained in more detail below, we therefore recommend that the Agency remove CCBA from the definition of "behavioral advertising" in the Proposed Regulations.

[2] *See History of the NAI*, The Network Advertising Initiative, https://thenai.org/about-the-nai-2/history-of-the-nai/.
[3] The NAI Self-Regulatory Framework, https://thenai.org/self-regulatory-framework/.
[4] *See* Enforcement Advisory No. 2024-02, *Avoiding Dark Patterns: Clear and Understandable Language, Symmetry in Choice*, https://cppa.ca.gov/pdf/enfadvisory202402.pdf.

A. Background on how the California Consumer Privacy Act of 2018 (“CCPA”) regulates Cross-Context Behavioral Advertising (“CCBA”).

The CCPA clearly defines CCBA and unequivocally requires businesses to provide transparency into how they conduct CCBA and to offer consumers methods to opt out of that activity.[5] However, the CCPA also distinguishes between CCBA – which inherently involves transfers of personal information such as “selling” or “sharing” personal information – from advertising that relies solely on personal information collected in a first-party context (“first-party advertising”).[6]

The fact that CCBA is treated explicitly by the CCPA (and is distinguished from other types of advertising and marketing purposes like first-party advertising)[7] empowering the Agency to develop regulations and define requirements pertaining specifically to CCBA. Since its creation, the Agency has exercised this power by setting specific, detailed regulatory requirements for CCBA , including, amongst other things, that consumers be notified as to what personal information is sold or shared and to whom, and be enabled to opt out of the sale or sharing of their personal information.[8] Indeed, consumers have been given broad rights and, most importantly, the tools necessary to exercise those rights, with respect to CCBA.

While it may not meet the definition of CCBA, first-party advertising may still involve the collection of consumer personal information and its processing using ADMT to provide interest-based advertising to consumers. As neither the CCPA nor the Agency’s regulations had previously defined *first-party* behavioral advertising, these advertising practices were not covered by the same notice and choice

[5] The CCPA defines CCBA as the “targeting of advertising to a consumer based on the consumer’s personal information obtained from the consumer’s activity across businesses, distinctly branded internet websites, applications, or services, other than the business, distinctly branded internet website, application, or service with which the consumer intentionally interacts.” California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.140(k) (2018) (hereinafter “CCPA”) (emphasis added). The CCPA requires businesses to provide consumers with prominent disclosures about their selling and/or sharing of personal information, including in the notice at collection. *See, e.g., id.* § 1798.100(a). It also grants consumers the direct right to opt out of sharing for CCBA, *see id.* § 1798.120, and requires businesses to provide a clear and conspicuous link enabling them to opt out of selling or sharing their personal information for CCBA, *see id.* § 1798.135(a)(1), (c)(2). *See also generally* Arsen Kourinian, *How Expansion of Privacy Laws, Adtech Standards Limits Third-Party Data Use for Retargeting*, IAPP (Apr. 27, 2021), https://iapp.org/news/a/how-the-expansion-of-data-privacy-laws-and-adtech-standards-limits-companies-ability-to-use-third-party-data-for-retargeting.

[6] The CCPA Regulations define “first party” as a consumer facing business with which the consumer intends and expects to interact. *See* Cal. Code Regs. tit. 11 § 7001(m). Conversely, the CCPA defines “sharing” as sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to a third party for cross-context behavioral advertising. *See* CCPA at § 1798.140(ah)(1). As such, data collected by a social media platform from consumers browsing the platform for behavioral advertising would be considered first-party data under the CCPA. *See generally* Allison Schiff, *Here’s How Facebook, Google and Amazon Are Tackling CCPA Compliance*, AdExchanger (Jul 9, 2020) (“Facebook isn’t making major changes to its web and mobile-tracking services on the grounds that the way it collects and shares data through its tracking pixel doesn’t constitute selling data.”).

[7] *See* CCPA at § 1798.140(e)(6) (defininig“business purpose” to include “[p]roviding advertising and marketing services, *except for cross-context behavioral advertising*[.]” (emphasis added).

[8] *See, e.g.,* Cal. Code Regs. tit. 11 §§ 7013 & 7026.

requirements as CCBA. By defining “Behavioral Advertising”[9] in the Proposed Regulations, we believe the Agency’s primary goals are to extend the rights consumers already possess relating to CCBA to first-party advertising, as well as other forms of ADMT that may not involve transfers of information like “selling” or “sharing.” However, by proposing to include CCBA within the umbrella definition of “Behavioral Advertising,” the Proposed Regulations introduce an unnecessarily confusing and duplicative set of requirements for CCBA *as a subset of behavioral advertising* when those same requirements already apply to CCBA directly through the CCPA and the existing regulations.

B. Including “Cross-Context Behavioral Advertising” in the definition of “Behavioral Advertising” is <u>duplicative and potentially confusing for consumers and businesses</u>.

Transparency and *choice* are most effective when business activities involving personal information processing are described clearly, simply, and unambiguously, and accompanied by simple, easy-to-use choice mechanisms. However, by including CCBA in the definition of “Behavioral Advertising,” the Proposed Regulations would subject CCBA to a new set of notice and choice requirements that are entirely duplicative of those that already exist under the CCPA. As they are duplicative, the notice and opt-out rights associated with ADMT, as applied to CCBA, would present <u>no benefit to consumers</u>; but instead may cause confusion about the scope and meaning of an opt out when a consumer is presented with different options to opt out of “sales,” “sharing,” and “ADMT.”

More specifically, and as discussed above,[10] the CCPA already grants consumers robust transparency and control into a business’s processing of personal information for CCBA. However, if the Proposed Regulations also define CCBA as a form of behavioral advertising, it would also be subject to redundant notice and choice requirements.[11] This additional and duplicative information does not further inform consumers about how businesses process their personal information for CCBA beyond what is already required by the CCPA. Even worse, the additional information is likely to confuse or overwhelm consumers with redundant information about CCBA, running counter to the requirement that disclosures must be “easy to read and understandable[.]”[12]

In addition to duplicative transparency, the Proposed Regulations, as written, would also present consumers with duplicative and overlapping choices to opt out of CCBA. The CCPA already requires businesses to provide multiple methods for consumers to opt out of for CCBA,[13] including by honoring

[9] The Proposed Regulations define “Behavioral Advertising” as “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.” Proposed Regulations at § 7001(g). As noted, this definition “includes cross-context behavioral advertising.” *Id.* at § 7001(g)(1)

[10] *See supra* section II.A.

[11] *See, e.g.,* Proposed Regulations at § 7220 (requiring separate disclosures for ADMT).

[12] Cal. Code Regs. tit. 11 § 7003(a).

[13] A business conducting CCBA must (1) provide a clear and conspicuous link on the business’ internet homepages, titled “Do Not Sell or Share My Personal Information,” to an Internet web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale or sharing of the consumer’s personal information; and (2) provide a clear and conspicuous link on the business’ internet homepages, titled “Limit the Use of My Sensitive Personal Information,” that enables a consumer, or a person authorized by the consumer, to limit the use or disclosure of the consumer’s sensitive personal information. *See* CCPA at § 1798.135(a). The current regulations enshrine these statutory requirements in section 7013. *See* Cal. Code Regs. tit. 11 § 7003(a).

opt-out preference signals.[14] However, if the Proposed Regulations continue to include CCBA as a form of "Behavioral Advertising", then businesses conducting CCBA would be subject to a separate and duplicative opt-out right.[15] This would risk confusing consumers about the meaning and scope of their opt-out rights while providing them no additional benefits, and would also run counter to the Agency's existing requirements to provide information to consumers in a way that is straightforward, easy to read, and avoids technical and legal jargon.[16] By way of example, a consumer might interact with a business that provides opt-out mechanisms for sales, sharing for CCBA, and for certain forms of "profiling" as required by the Proposed Regulations. A consumer interacting with that business may wish to opt out of profiling by the business due to specific concerns about how the business might use a profile for employment purposes; but may also have made a conscious decision *not* to opt out of CCBA, given the separate choice mechanisms and the explanation given by the business of how advertising supports their operations . Under the proposed regulations, this consumer's expectations would be frustrated because an opt-out of "profiling" would by definition also include an opt-out of CCBA, even though these are presented separately by the business in compliance with CCPA.

The Agency can prevent this potential for consumer confusion and upset expectations – without sacrificing any privacy benefits for consumers – simply by removing CCBA from the definition of behavioral advertising and allowing the existing provisions of the CCPA regarding CCBA to do their intended work directly.

C. Treatment of CCBA in other parts of the Proposed Regulations

The NAI recognizes that the Proposed Regulations create business obligations on their use of ADMT beyond consumer notice and choice (already discussed above). For example, the Proposed Regulations include a requirement for businesses to conduct a risk assessment for high-risk processing activities, including certain forms of ADMT.[17] Our recommendation to remove CCBA from the definition of behavioral advertising is not intended to excuse CCBA from risk assessments. Indeed, the Agency appears to have independently determined that selling and/or sharing personal information for CCBA is a high-risk processing activity in its own right.[18] Again, this is an example where removing CCBA from the definition of behavioral advertising will not prevent the Agency from meeting its goals for the treatment of CCBA.[19]

There may be other areas of the Proposed Regulations where similarly direct treatment for CCBA can meet the Agency's goals without causing the confusion we anticipate if CCBA is left within the definition of behavioral advertising.

[14] *See* CCPA at § 1798.135(e).

[15] *See* Proposed Regulations at § 7221(c).

[16] *See* Cal. Code Regs. tit. 11 § 7003(a) ("Disclosures and communications to consumers shall be easy to read and understandable to consumers. For example, they shall use plain, straightforward language and avoid technical or legal jargon."); *See also* Enforcement Advisory No. 2024-02, *Avoiding Dark Patterns: Clear and Understandable Language, Symmetry in Choice*, https://cppa.ca.gov/pdf/enfadvisory202402.pdf.

[17] *See* Proposed Regulations at § 7150.

[18] *See id.* § 7150(b)(1).

[19] Other states have made similar determinations. For example, the Colorado Privacy Act requires businesses that are selling or sharing personal information for behavioral advertising to conduct *Data Protection Assessments* to ensure its processing does not present a heightened risk of harm to consumers. *See* Colo. Rev. Stat. § 6-1-1309(2)(b).

NAI Recommendation: For these reasons, we recommend modifying the definition of "Behavioral Advertising" to remove CCBA, as follows:

> (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.
>
> (1) Behavioral advertising does not include~~s~~ cross-context behavioral advertising, as defined by Civil Code section 1798.140, subdivision (k).
>
> (2) Behavioral advertising does not include nonpersonalized advertising, as defined by Civil Code section 1798.140, subdivision (t), provided that the consumer's personal information is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business, and is not disclosed to a third party.

II. The Agency should consolidate the additional disclosures proposed for the Pre-Use Notice with the existing Notice at Collection requirements.

As noted above, the CCPA regulations require disclosures to consumers to be straightforward and avoid technical and legal jargon. Indeed, consumers must be provided language that is easy to understand when faced with privacy choices. To promote simplicity and ease of understanding, consumers interacting with a service that collects personal information and employees ADMT to process that information will be best served by a single, easy-to-read notice that explains the data processing taking place. For this reason, we recommend the Agency consolidate the additional disclosures proposed for the *Pre-Use Notice* with the existing disclosures required for the *Notice at Collection.*

The Proposed Regulations would require any business using ADMT to provide consumers with an *additional* pre-use notice informing consumers about the business's use of ADMT and the consumers' rights to opt-out of ADMT and to access ADMT. The Proposed Regulations would require the pre-use notice to include (1) an explanation of the specific purpose for using ADMT; (2) a description of the consumer's right to opt-out of ADMT; (3) a description of the consumer's right to access ADMT; (4) a statement that the business is prohibited from retaliating against consumers for exercising their CCPA rights; and (5) additional information about how ADMT works including the logic used in ADMT and the intended output of the ADMT.[20]

However, the CCPA and existing regulations already require a *Notice at Collection* for consumers, to ensure they have transparency into how a business may collect, use, and share their personal information at or before the point of collection. This notice must include (1) a list of categories of personal information about consumers; (2) the purpose of collecting and using the personal information; (3) whether personal information is sold or shared; (4) the length of time the business intends to retain the personal information; (5) a link to the right to opt-out of sale/sharing of data; and (6) a link to the business's privacy policy.[21]

[20] *See* Proposed Regulations at § 7220(c).

[21] *See* Cal. Code Regs. tit. 11 § 7012(e).

Because consumers are already entitled to clear, timely notice about how businesses will process their personal information, we recommend that the Agency consolidate the additional disclosures proposed for the ADMT pre-use notice with the existing notice at collection. This would continue to promote the Agency's objective of ensuring consumers are provided with meaningful information and an opportunity to exercise their rights regarding ADMT while avoiding unnecessarily complex and confusing disclosures for consumers.

NAI Recommendation: The Agency should consolidate the additional disclosures proposed in section 7220 with the existing *Notice at Collection* requirements in section 7012.

III. The Agency should remove the proposed "remains deleted" language in section 7022 to avoid inconsistencies with existing requirements to *permanently* and *completely* erase data.

The Proposed Regulations change how businesses comply with deletion requests by adding a requirement not only that the business delete the consumer's personal information consistent with the CCPA's requirements, but also "implement measures to ensure that the information remains deleted, deidentified, or aggregated" upon receiving a valid deletion request from a consumer.[22] While the NAI appreciates the Agency's efforts to ensure that valid deletion requests are fully effectuated by businesses, the practicalities of ensuring that a consumer's personal information "remain deleted" are inconsistent with other clear requirements in the CCPA and the existing implementing regulations.

Specifically, any measures that a business may implement to ensure that a consumer's personal information "remain deleted" would appear to require that the business actually retain personal information about the consumer — *i.e.*, for suppression purposes – instead of fully and completely deleting the consumer's personal information. However the CCPA and its existing regulations require that a business respond to a verifiable consumer request to delete by ***permanently and completely eras[ing] the consumer's personal information from their systems*** (emphasis added).[23] A business cannot, therefore, retain some of a consumer's personal information to ensure that other elements of it "remain deleted" without violating the requirement to "permanently and completely" delete the consumer's information.

Additionally, taking steps to ensure that a consumer's personal information remains deleted appears to change the plain meaning of a single request to delete into two distinct requests – one to delete personal information associated with the requestor, and a second one to stop collecting personal information about the requestor. In its *Initial Statement of Reasons*, the Agency explains that this language has been added to "ensure that a consumer's right to delete is meaningful" and that

[22] Proposed Regulations at § 7022(b)(1); *see also* § 7022(c)(1).

[23] *See* Cal. Code Regs. tit. 11 § 7022(b) ("A business shall comply with a consumer's request to delete their personal information by: (1) Permanently and completely erasing the personal information from its existing systems except archived or backup systems, deidentifying the personal information, or aggregating the consumer information; (2) Notifying the business's service providers or contractors of the need to delete from their records the consumer's personal information that they collected pursuant to their written contract with the business…; and (3) Notifying all third parties to whom the business has sold or shared the personal information of the need to delete the consumer's personal information unless this proves impossible or involves disproportionate effort."); *id.* at § 7022(c) ("A service provider or contractor shall… cooperate with the business in responding to a request to delete by doing all of the following: (1) Permanently and completely erasing the personal information from its existing systems except archived or backup systems, deidentifying the personal information, aggregating the consumer information, or enabling the business to do so.").

consumers should not be required to "make repetitive requests to delete with the business, rendering the right to delete pointless."[24] However, the additional *remains deleted* language does not match the plain meaning of the word "delete" or the way it is treated under the CCPA and existing regulations . In some cases, it may also run afoul of consumer expectations. A consumer may wish to delete excessive or historical personal information a business has collected about them; but also wish to continue interacting with the business in a more limited or current manner. Requiring businesses to stop collecting information about the consumer in those circumstances is likely to be frustrating and confusing to consumers, as well as putting businesses at risk of violating the other dictates of the CCPA to completely delete the consumer's information instead of retaining some elements of personal information for suppression purposes.

Further, the California legislature has explicitly considered and provided a mechanism for an analog of the "remains deleted" requirement in the Delete Act. In effect, a consumer who in the future uses the Delete Request and Opt-Out Platform under development at CPPA to request deletion by registered data brokers will "remain deleted" by those brokers because data brokers must continue to delete all subsequently collected personal information of that consumer once every forty five days.[25] Data brokers are expected to achieve this result by integrating with a deletion mechanism maintained by the Agency at regular intervals.[26] This solution achieves the objective of ensuring a consumer's data *remains deleted* upon submitting a deletion request while avoiding the pitfall of a business needing to retain some personal information about the consumer – which is currently prohibited under the CCPA and its implementing regulations. The Proposed Regulations do not include – and the CCPA's drafters did not provide for – a comparable mechanism that would allow businesses to ensure a consumer remains deleted without violating the requirement to fully comply with a deletion request. For these reasons, we recommend removing the "remains deleted" language from the Proposed Regulations.

NAI Recommendation: The Agency should remove the proposed "remains deleted" language in section 7022 of the CCPA regulations to avoid inconsistencies with existing requirements to *permanently and completely* erase data.

IV. The Agency should clarify that businesses must evaluate whether their use of ADMT does not ***unlawfully*** discriminate based upon protected classes in § 7152(a)(6)(B)(i).[27]

Identifying and mitigating risks to consumers posed by discrimination based upon protected classes is an important objective of the Proposed Regulations, particularly where those classes of individuals have vulnerabilities or have been historically subject to harmful discrimination. However, because the Agency has not adequately defined or specified the type of discrimination it is seeking to address, the Proposed Regulations risk creating a prohibition on all distinctions made among consumers, even when those distinctions are otherwise lawful and beneficial to consumers.

[24] CALIFORNIA PRIVACY PROTECTION AGENCY – INITIAL STATEMENT OF REASONS (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations) at 30, (Nov. 22, 2024), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_isor.pdf.

[25] *See* California Delete Act, Cal. Civ. Code § 1798.99.86(c) (2023) (hereinafter "Delete Act").

[26] *See id.* at § 1798.99.86(a).

[27] There are seven instances in the Proposed Regulations where "does not discriminate based upon protected classes" is mentioned. *See* Proposed Regulations at § 7152(a)(6)(B)(i); § 7152(a)(6)(B)(ii); § 7201(a)(1); § 7201(a)(2); § 7221(b)(3)(B).

For businesses using ADMT to conduct “extensive profiling,” the Proposed Regulation require the business to evaluate whether the ADMT technology works as intended for the business’s proposed use and “does not discriminate based upon protected classes[.]”[28] Protected classes are extensively defined in the State of California to include, amongst many other things, race, religion, gender, sexual orientation, medical condition, disability, and age if over forty years old.[29]

There are many scenarios where discriminating based on a protected class can cause consumer harm. For example, in its *Initial Statement of Reasons*, the Agency describes a scenario where ADMT is used to serve advertisements for high-paying job opportunities disproportionately to men. In this case, women may be deprived of the opportunity to learn about and apply for higher-paying jobs that they have historically been excluded from. In this scenario, the discrimination at issue would also be unlawful.[30] In a second example, the Agency describes a scenario where advertisers use social media to target housing advertisements based on protected classes, such as race, gender, and age.[31] In this scenario as well, the discrimination based on protected classes is unlawful.[32] As such, it appears that the type of discrimination based upon protected classes that the Agency is primarily concerned with is unlawful discrimination. The NAI therefore recommends that the Agency modify the sub-section to clarify that a business’s evaluation must ensure the ADMT technology does not *unlawfully* discriminate based upon protected classes.

Further, In a recent Legal Advisory, the California Attorney General, Rob Bonta, provided specific guidance on the application of existing California laws to various uses of artificial intelligence (AI), which encompasses many of the same uses the Agency seeks to cover for ADMT in the Proposed Regulations. In his advisory, the Attorney General cited the Unruh Civil Rights Act, the California Fair Employment and Housing Act, and the California Consumer Credit Reporting Agencies Act as examples of laws that apply equally to AI systems as they do to systems without the involvement of any AI.[33]

[28] *Id.* at § 7152(a)(6)(B)(i).

[29] *See* Protected Classes in California, https://www.senate.ca.gov/protected-classes (last visited Feb. 1, 2025).

[30] For example, serving advertisements for high-paying job opportunities disproportionately to men is already unlawful under the California Fair Employment and Housing Act (FEHA). *See* Cal. Gov’t Code § 12940(c); *e.g. Facebook EEOC Complaints*, ACLU (Sep. 25, 2019) https://www.aclu.org/cases/facebook-eeoc-complaints, (Facebook settles case where ACLU alleges Facebook delivered job ads selectively based on age and gender categories and agrees to require all advertisers to certify compliance with Facebook’s policies prohibiting discrimination and with applicable federal, state, and local anti-discrimination laws).

[31] *See* CALIFORNIA PRIVACY PROTECTION AGENCY – INITIAL STATEMENT OF REASONS (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations) at 62, (Nov. 22, 2024), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_isor.pdf.

[32] *E.g. Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising*, Department of Justice Office of Public Affairs (Jun. 21, 2022), https://www.justice.gov/archives/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known, (Facebook settles case where the Department of Justice alleges that Facebook’s algorithms relied, in part, on consumer characteristics to serve housing ads in violation of the Fair Housing Act).

[33] *See* California Attorney General’s Legal Advisory on the Application of Existing California Laws to Artificial Intelligence, https://oag.ca.gov/system/files/attachments/press-docs/Legal%20Advisory%20-%20Application%20of%20Existing%20CA%20Laws%20to%20Artificial%20Intelligence.pdf.

If the Agency does not specify that businesses must evaluate for *unlawful* discrimination, the current language would put legitimate, beneficial, and otherwise lawful distinctions between individuals in protected classes at risk. For example, and keeping to the advertising context, an advertiser may wish to reach an audience of individuals over 40 years old – a protected class under California law – to share information about financial products for retirement. Similarly, an advertiser may wish to reach a specifically male or female audience with advertising for men's or women's fashion; but doing so requires making a distinction based on gender, another protected class under California law. Failing to specify that the Agency intends to address *unlawful* discrimination is likely to cause confusion among advertisers seeking to reach relevant audiences without harmful or illegal discrimination and prevent consumers in protected classes – even simply based on age group or gender – from learning about products that are designed for them. Making this clarification would still require advertisers and the platforms they use to evaluate whether their methods for advertising for particular things – like housing, credit, or employment – could involve *unlawful* discrimination.

The NAI believes this recommendation is consistent with the agency's goals with the proposed requirement as well as consistent with the decades of carefully-crafted statutes and case law in the State of California that extensively define what unlawful discrimination is. This clarifying amendment would not only ensure the CCPA regulations are harmonized with other state laws[34] and regulations,[35] but it would also ensure that harmless uses of ADMT in advertising are not unnecessarily restricted by the Proposed Regulations. For these reasons, we recommend modifying the sub-section to clarify that a business's evaluation must ensure the ADMT technology does not "unlawfully discriminate" based upon protected classes.

NAI Recommendation: The Agency should clarify that businesses must evaluate whether their use of ADMT does not unlawfully discriminate based upon protected classes in § 7152(a)(6)(B)(i). For example:

> (A) For uses of automated decisionmaking technology set forth in section 7150, subsection (b)(3), the business must identify the following:
>
> (i) Whether it evaluated the automated decisionmaking technology to ensure it works as intended for the business's proposed use and does not unlawfully discriminate based upon protected classes ("evaluation of the automated decisionmaking technology");

[34] *See* Colo. Rev. Stat. § 6-1-1308(6) ("A controller shall not process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers."); Conn. Gen. Stat. Ann. § 42-520(a)(5) ("A controller shall… not process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers[.]"); Md. Code Ann., Com. Law § 14-4607(A)(3) ("A controller may not… [p]rocess personal data in violation of State or federal laws that prohibit unlawful discrimination[.]") (going into effect on Oct. 1, 2025); N.H. Rev. Stat. Ann. § 507-H:6(e) ("A controller shall… [n]ot process personal data in violation of the laws of this state and federal laws that prohibit unlawful discrimination against consumers[.]"); N.J. Stat. Ann. § 56:8-166.12(a)(5) ("A controller shall… not process personal data in violation of the laws of this State and federal laws that prohibit unlawful discrimination against consumers[.]").

[35] Similar to what the Agency is proposing in this rulemaking concerning *Risk Assessments*, the Colorado Privacy Act Rules require businesses that are processing personal data for profiling to conduct a *Data Protection Assessment* to ensure its processing does not risk causing an *Unlawful Disparate Impact* on consumers. *See* Colorado Privacy Act Rules 4CCR 904-3, Rule 9.06(A). The Colorado Privacy Act Rules define *Unlawful Disparate Impact* as "conduct or activity which violates state or federal laws that prohibit unlawful discrimination against Consumers." *Id.* at Rule 9.06(D).

V. **The Agency should add language to section 7222 clarifying that nothing in the section may be construed to require a business to reveal any trade secrets when responding to a verifiable consumer access request.**

Providing consumers with the right to access information about an ADMT - be it the ADMT's purpose, data outputs, and how those outputs are then used with respect to the consumer - is an important objective of the Proposed Regulations.[36] However, the CCPA recognizes the importance of transparency to consumers with business interests in proprietary or trade secret information by requiring any adoption of regulations to include exceptions to ensure trade secrets are not disclosed in response to a verifiable consumer request.[37] As such, the NAI recommends adding language to section 7222 clarifying that nothing in the section may be construed to require a business to reveal any trade secrets when responding to a verifiable consumer access request.

NAI Recommendation: The Agency should add language to section 7222 clarifying that nothing in the section may be construed to require a business to reveal any trade secrets when responding to a verifiable consumer access request.

VI. **As businesses will have 24 months from the effective date to identify processing activities and conduct risk assessments, the Agency should add an exception to the attestation requirement.**

The Agency rightfully included a grace period for businesses to conduct risk assessments of ADMT processing initiated prior to the effective data of the Proposed Regulations. However, in doing so, the Agency inadvertently included language in the Proposed Regulations that risk requiring businesses to falsely attest that they abstained from their ADMT processing. As such, we recommend the Agency add an exception to the attestation requirement.

Under the Proposed Regulations, businesses will need to conduct risk assessments to determine whether the "risks to consumers' privacy from the processing of personal information outweigh the benefits to the consumer, the business, other stakeholders, and the public from that same processing."[38] These assessments must be conducted and documented prior to initiating the use of ADMT, and be submitted to the Agency with an attestation stating "that the business initiated any of the processing set forth in section 7150, subsection (b), only after the business conducted and documented a risk assessment as set forth in this Article."[39] However, in consideration of ADMT processing initiated prior to the effective date of the Proposed Regulations, the Agency gives businesses a 24 month grace period to "conduct and document a risk assessment in accordance with the requirements of this Article[.]"[40]

[36] *See* Proposed Regulations at § 7222.

[37] *See* CCPA at § 1798.185(a)(3) ("On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to… [e]stablishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter, with the intention that trade secrets should not be disclosed in response to a verifiable consumer request.").

[38] Proposed Regulations at § 7152(a).

[39] *Id.* at § 7157(b)(1)(B)(iii).

[40] *Id.* at § 7155(c).

NAI Recommendation: Consistent with the grace period already included in the Proposed Regulations, the NAI recommends that the Agency clarify that it also applies to the attestation requirement. For example, section 7157(b)(1)(B)(iii) could be supplemented with the following redlined text:

> An attestation that the business initiated any of the processing set forth in section 7150, subsection (b), only after the business conducted and documented a risk assessment as set forth in this Article unless the processing activity identified in section 7150, subsection (b), was initiated prior to the effective data of these regulations;

This recommendation will ensure businesses that currently use ADMT for processing will not be required to falsely attest that they abstained from ADMT processing.

VII. Conclusion

Thank you for your continued commitment to public involvement and transparency in this important rulemaking process concerning automated decisionmaking technology. If we can provide any additional information, or otherwise assist your office as it continues to engage in the rulemaking process, please do not hesitate to contact me at leigh@networkadvertising.org, or David LeDuc, Vice President, Public Policy, at david@networkadvertising.org.

Respectfully Submitted,

Leigh Freund
President and CEO
Network Advertising Initiative (NAI)

Grenda, Rianna@CPPA

From: Ebbink, Benjamin <bebbink@fisherphillips.com>
Sent: Wednesday, February 19, 2025 7:00 AM
To: Regulations@CPPA
Subject: Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments: NAPEO Comments to CPPA ADMT Regulations (2.19.2025).pdf

This Message Is From an External Sender

WARNING:This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Attached please find public comments on behalf of the National Association of Professional Employer Organizations.

Benjamin M. Ebbink
Partner
Fisher & Phillips LLP
621 Capitol Mall | Suite 2400 | Sacramento, CA 95814
bebbink@fisherphillips.com | O: (916) 210-0407 | F: (916) 210-0401

vCard | Bio | Website *On the Front Lines of Workplace Law*SM

This message may contain confidential and privileged information. If it has been sent to you in error, please reply to advise the sender of the error, then immediately delete this message.

NAPEO® National Association
of Professional Employer Organizations

707 North St. Asaph Street
Alexandria, Virginia 22314

T 703 836.0466
F 703 836.0976
www.napeo.org

February 19, 2025

Submitted via email to regulations@cppa.ca.gov

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

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

Dear California Privacy Protection Agency:

On behalf of the National Association of Professional Employer Organizations (NAPEO), thank you for the opportunity to submit comments on the proposed regulations related to CCPA updates, cyber risk, automated-decisionmaking technology (ADMT) and insurance regulations.

We appreciate the focus and attention devoted to these issues, but we have concerns with provisions of the proposed regulations related to artificial intelligence (AI) and ADMT, as discussed in further detail below.

NAPEO is the voice of the PEO industry. Professional employer organizations (PEOs) provide human resource services to small and mid-size businesses—paying wages and taxes under the PEO's EIN, offering workers' compensation and risk management services, and providing compliance assistance with employment-related rules and regulations. In addition, many PEOs provide HR technology systems and access to 401(k) plans, health, dental, and life insurance, dependent care, and other benefits. In doing so, PEOs help businesses take care of employees by enabling them to offer Fortune 500-level benefits at an affordable cost and providing access to experienced HR professionals. PEOs also help business owners and executives save time by taking administrative and HR related tasks off their plates, allowing them to focus on the success of their businesses.

Across the U.S., PEOs provide services to 200,000 small and mid-sized businesses, employing 4.5 million people. More than 21,000 California businesses – employing more than 470,000 people partner with a PEO.

<u>Concerns Regarding Competing, Inconsistent and Conflicting Regulation of AI and ADMT</u>

AI and the use of ADMT is an active area of focus by legislators and regulators in California. While we appreciate the attention brought to this important area (particularly in the employment context), we remain concerned that uncoordinated approaches to regulation of the same issue will result in competing, inconsistent and conflicting provisions that are difficult for businesses to implement.

For example, the California Civil Rights Department (CRD) is currently finalizing regulations that seek to incorporate provisions specific to AI and ADMT into California's regulations regarding employment discrimination – as their charge is to implement and enforce laws and regulations dealing with discrimination in employment. NAPEO is actively engaged in provided public comments to help improve and fine-tune CRD's proposed regulations.

Moreover, many of the same provisions of the CPPA's proposed ADMT regulations (advance notice, impact assessments, opt-out rights) were considered by the legislature last year in AB 2930 (Bauer-Kahan). While AB 2930 did not advance to the Governor, it will likely be reintroduced in 2025 and addresses many of the same issues contemplated by the CPPA's proposed regulations.

Contributing to potential confusion for the employer community is the inclusion of employees and applicants for employment in a consumer protection scheme such as the CCPA/CPRA. Attempting to graft employment concepts into what at its core is a consumer protection law creates confusion and uncertainty for both employees and the regulated employer community. It also potentially doubles enforcement costs and burdens for employers as they attempt to comply with multiple regulatory schemes that all seek to address the same issue. For these reasons, we strongly supported the previous exemption in the CCPA/CPRA for employment and employees.

For these reasons, we believe that any proper regulation of AI and ADMT in the employment context is the purview of the legislature or the CRD. To the extent that CPPA's proposed regulation will apply to the employment context, the result will be competing, inconsistent and conflicting regulation of AI that will be nearly impossible for the business community to reconcile.

Overbroad Definition of ADMT (Section 7001(f))

While we appreciate efforts during the pre-rulemaking process to narrow the definition of ADMT, we remain concerned that this definition is far too overbroad and includes in the definition of "automated" functions that by their nature are not (human decisionmaking).

This stems from the fact that the proposed definition of ADMT includes anything that "substantially facilitates" human decisionmaking. This would include virtually any "technology" that a business uses in order to help human decisionmaking. In the employment context, suppose an employer uses a calculator or an Excel spreadsheet to calculate sales results to help it decide who gets a bonus, or a promotion, or who is terminated for failing to meet sales quotas? Under this proposed definition, the use of the calculator or the Excel spreadsheet would be covered as ADMT because it "substantially facilitates" decisions made by a human.

Use of vague terms like "substantially facilitate" and "key factor" will only lead to litigation against businesses to determine the scope and meaning of these broad terms.

Moreover, while we appreciate the "carve out" contained in Section 7001(f)(4), circular language in the "carve out" gives it little or no effect. Specifically, the language says ADMT does not include specified technologies "provided that the technologies do not…substantially facilitate human decisionmaking," which essentially gets us back to square one with the exceedingly broad inclusion of technology that merely facilitates human decisionmaking.

Therefore, we strongly recommend that the definition of ADMT (and other key terms) be limited, narrow in scope, and developed with industry experts.

Concerns Regarding "Opt-Out" Provisions (Section 7221)

The proposed regulations provide that a business must provide a consumer (employee/applicant) with the right to opt-out of the uses of ADMT. In the employment and hiring context, this could result in dynamics that are completely unworkable and costly and would compel businesses to forgo the use of ADMT altogether. For example, a business may use a resume screening tool to provide a first analysis of applications to determine which candidates meet the minimum job requirements and which do not, before hiring managers begin the process of human decisionmaking. Enabling an applicant to "opt-out" of this technology and require a human to perform this initial review of resumes would defeat any efficiencies provided by such ADMT in the first place.

The purported exception set forth in Section 7221(b)(2) to the "opt-out" requirement if the business provides a consumer with a method to appeal the decision to a "qualified human reviewer." However, this is really no exception an all. Requiring a business to allow an applicant/employee to appeal to a "qualified human reviewer" is the same as requiring them to opt-out completely from the use of ADMT in the first place.

We appreciate the exception set forth in Section 7221(b)(3), which allows certain decisions to be exempt from the opt-out provisions where the business demonstrates that the ADMT is necessary to achieve the specified assessment and the business has performed an impact assessment. However, we feel that this exemption is too narrow and will be a source of protracted litigation. The exemption only applies where the use of ADMT is "necessary" and "used solely for" specified purposes which are undefined and will be litigated at great expense. In the employment context, the exemption also only applies for decisions related to the applicant's ability to perform at work and whether to hire them. In order for such an exemption to be useful in the employment context, it needs apply to all employment-related decisions and not be limited by terms that will result in needless litigation.

Miscellaneous Concerns

We also have concerns with some of the non-ADMT specific provisions of the proposed regulations and therefore bring the following issues to your attention:

- **Definition of "Behavioral Advertising" (Section 7001(g))** – We are concerned that adding the activity of a user within a business' own websites/services as part of the behavioral advertising definition would make it so that contracting with an entity to provide behavioral advertising based on a user's activity across internal platforms/websites would make the entity a "third party" and not a "service provider," under CCPA. We suggest that this definition be deleted. Instead, the definition of "cross-context behavioral advertising" of the CCPA should be used.

- **Privacy Policies (Section 7011(e)(E))** – The added language should be removed because identifying the categories of third parties to whom information has been shared should be sufficient. Requiring more information to provide a "meaningful understanding" of the parties to whom information is sold or shared could be akin to having to actually name the third party in privacy policies.

- **Methods for Submitting Requests (Section 7020(e))** – Language should be added to clarify that a consumer may request information collected beyond the 12-month period only if the business has collected personal information on or after 1/1/2022.

- **Requests to Delete (Section 7022(f)0** – This language is overly burdensome for businesses as the additional language imposes a responsibility on the business that would normally belong to the service provider or contractor. Businesses can ensure that they have contractual obligations in place with their service providers or contractors, but beyond that the regulations should not make a business responsible for whether the contractual measurers are in fact implemented by the third party when it is not in the business's control.

- **Notices Regarding Complaints to CPPA or OAG (Sections 7022(g)(5), 7023(f)(6), 7024(e)(3), 7026(e) and 7027(f))** – The proposed notice language should be modified so as not to presume that there has been a violation of the law nor make legal conclusions. For example, rather than stating "If you believe your privacy rights have been violated…," the notices should say something like, "If you believe your request has been denied without a valid reason…"

- **Timing Requirements for Cybersecurity Audits (Section 7121(b))** – The proposed regulations should be clarified as to whether businesses will have the ability to determine the scope of the subsequent audits or whether the audits must conform to the requirements set forth in Sections 7122(e) and 7123.

- **Scanning of Employee Emails for Security Purposes (Section 7027(m)(2)(B))** – We are concerned that the second sentence of this subdivision implies that a business must do more than provide a notice to employees that their systems and technologies are monitored for information security purposes in order to satisfy this requirement.

- **Risk Assessments for ADMT, AI, and Sensitive Personal Information (Section 7150, *et seq.*)** – We are concerned this is an overly burdensome. Content requirements such as "specifically identifying business purposes for consumer process; specifically identifying benefits to the business; number of consumers whose personal information is processed; and contributors to the risk assessment" is essentially asking businesses to reveal company and client confidential information and/or business-trade secrets. There is also significant risk of downstream impact on smaller businesses through partnerships with larger companies that could be subject to compliance. There are no exemptions for non-ADMT developers or service providers.

- **Cybersecurity Audits (Section 7120, *et. seq.*)** – We are concerned this requirement is also overly burdensome (e.g., revealing and describing data breaches including sample regulatory letters). This may also be seen as duplicative. Businesses that already have to complete similar audits for other business purposes, would now have to meet all the requirements of the draft regulations which would drive up costs and resources to change auditing practices.

- **Economic Impacts** - The CPPAA proposed regulatory impact assessment estimates costs of approximately $3.5 billion to implement the proposed regulations, which may also lead to job losses.

Conclusion

Once more, we appreciate your consideration of our comments on the proposed regulations related to ADMT and other issues. Should you have any questions with respect to the issues discussed herein, please do not hesitate to contact me at hwalker@napeo.org.

Respectfully,

[redacted]

Hannah Walker
Senior Director, State Government Affairs
NAPEO
hwalker@napeo.org

Grenda, Rianna@CPPA

From:	Elliott Long <elliott@publicprivatestrategies.com>
Sent:	Wednesday, February 19, 2025 2:06 PM
To:	Regulations@CPPA
Cc:	Katie Vlietstra Wonnenberg; Baylee Anderson
Subject:	National ACE - Public Comment on CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations
Attachments:	National ACE CCPA Comment Letter.pdf

Hello,

We wanted to share the attached comments on behalf of the National Asian/Pacific Islander American Chamber of Commerce and Entrepreneurship (National ACE).

Please let us know if you have any questions or need anything else.

Thanks!
Elliott

--
Elliott Long
PUBLIC PRIVATE
STRATEGIES
www.publicprivatestrategies.com

National Asian/Pacific Islander American Chamber of Commerce and Entrepreneurship (National ACE)
California Privacy Protection Agency: Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies

National ACE
1300 Pennsylvania Avenue NW
Washington, DC 20004

February 19, 2025

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

Re: Comment on the Proposed Regulations Under the California Consumer Privacy Act (CCPA) – Concerns Regarding the Automated Decisionmaking Technology (ADMT) Provisions

Dear California Privacy Protection Agency,

The National Asian Pacific Islander American Chamber of Commerce and Entrepreneurship (National ACE) respectfully submits the following comment letter in response to the California Privacy Protection Agency's Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies.

National ACE serves as a strong advocate for the interests of 2.91 million Asian American and Pacific Islander (AAPI) small business owners and all entrepreneurs across the United States. We effect positive change on all issues that enhance and advance the goals and aspirations of AAPI business owners, all entrepreneurs, and community leaders. In California alone, there are more than 1.3 million AAPI-owned businesses that stand to be impacted by the implementation of these regulations.

We write specifically to express concerns regarding the proposed provisions governing ADMT and the undue compliance burden they will place on small businesses, particularly AAPI-owned enterprises. While we recognize the importance of consumer privacy protections, the current framework disproportionately affects small businesses with limited resources, imposing excessive costs and operational challenges that could hinder their ability to compete and grow.

The Burdensome and Costly Impact of ADMT Regulations on Small Businesses

The proposed regulations define ADMT broadly, encompassing any technology that processes personal information and uses computation to execute decisions, replace human decision-making, or substantially facilitate human decision-making. This expansive definition captures a wide range of standard business tools that small businesses rely on, including customer relationship management (CRM) software, marketing automation, fraud detection, and online hiring platforms.

Under the current draft, businesses deploying ADMT will be required to:

- Conduct risk assessments to evaluate the impact of ADMT on consumers;
- Submit detailed reports on their use of ADMT to the CPPA;
- Provide consumers with pre-use notices regarding ADMT's role in decision-making processes;
- Enable consumer opt-outs from the use of ADMT in many cases, including behavioral advertising.

These requirements impose substantial compliance costs, including legal, administrative, and technical expenses. According to the CPPA's Economic and Fiscal Impact Statement, compliance costs for small businesses are estimated to range from $7,045 to $92,896 in initial costs, with ongoing annual costs of approximately $19,317. These figures are prohibitive for many AAPI-owned businesses, which often operate with minimal margins and limited access to capital. These requirements will also have downstream implications for small businesses that rely on the digital advertising ecosystem for cost-effective tools to grow their businesses.

Impact on AAPI Small Businesses

AAPI small businesses contribute significantly to California's economy, spanning industries such as retail, hospitality, healthcare, and professional services. Many of these businesses operate with lean staffing models and lack in-house legal or IT teams, making compliance with complex data governance requirements exceedingly difficult.

Moreover, language and cultural barriers already pose challenges for AAPI business owners in navigating regulatory changes. The CPPA's proposed ADMT regulations add yet another layer of compliance complexity, requiring detailed documentation and technical audits that many small businesses are ill-equipped to handle. These requirements may push some businesses to forgo helpful technologies altogether, reducing efficiency and competitiveness in an increasingly digital economy.

Conclusion

National ACE strongly supports privacy protections that enhance consumer trust, but we urge the CPPA to reconsider its proposed framework, taking into consideration the operational realities of AAPI and all small businesses. Without tailored exemptions or modifications, the ADMT provisions risk placing excessive financial and administrative burdens on businesses that lack the resources to comply, potentially stifling innovation and economic opportunity.

We appreciate your consideration of these concerns and look forward to continued dialogue on ensuring that California's privacy regulations are both effective and equitable. Please feel free to contact us for further discussion.

Sincerely,

Chiling Tong
President and CEO
National ACE

Grenda, Rianna@CPPA

From:	dan.lewis@nprc-inc.org
Sent:	Tuesday, February 18, 2025 7:25 PM
To:	Regulations@CPPA
Subject:	NPRC Comment Letter - Cybersecurity Audits, Risk Assessments and Automated Decisionmaking Proposed Regulations
Attachments:	NPRC Final Letter on CA CPPA Proposed Rules

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

The National Payroll Reporting Consortium (NPRC) appreciates the opportunity to submit the attached comments on the cybersecurity audits, risk assessments and automated decisionmaking proposed regulations. Thank you in advance for your consideration, If you have any questions or I can provide any additional information that would be helpful, please contact me at 973-974-5273.

Best regards,

Dan Lewis

NPRC

National Payroll Reporting Consortium

PO Box 850 ★ Henrietta, NY 14467-0850 ★ www.NPRC-Inc.org

February 19, 2025

California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834

Re: COMMENTS ON CYBERSECURITY AUDITS, RISK ASSESSMENTS AND AUTOMATED DECISIONMAKING PROPOSED REGULATIONS

Dear Board Members,

On behalf of the National Payroll Reporting Consortium (NPRC), we appreciate the opportunity to comment on the proposed draft regulations updating the California Consumer Privacy Act (CCPA) and addressing cybersecurity audits, risk assessments and automated decisionmaking systems.

NPRC is a non-profit trade association which represents payroll processing service providers that serve roughly 48% of the U.S. workforce. NPRC members provide human capital management (HCM) solutions, including payroll services and software systems that enable clients to manage their workforces. HCM software/platforms typically offer a wide range of functions, allowing clients to manage payroll, approve time-off requests, facilitate recruitment and hiring, conduct performance reviews, administer benefits, and offboard employees when they resign or are terminated. As HCM providers, our companies provide services involving the processing of personal data that would be impacted by the proposed regulations.

NPRC has concerns with the provisions addressing automated decisionmaking systems and cybersecurity audits. More specifically, we are concerned as follows:

1. The definition of Automated Decisionmaking Technology is overbroad and would include basic HCM software functions that are neither designed nor intended to make hiring or employment decisions.
2. The proposed mandatory Cybersecurity Audit Requirement would impose an unnecessary burden on service providers without providing demonstrable benefit to California businesses.

Automated Decisionmaking Technology (ADMT)

The proposed regulations define “automated decisionmaking technology” (ADMT) as “any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking.” The definition extends to technologies “derived from machine learning, statistics, and artificial intelligence.” However, the regulations lack specificity about what qualifies as “substantially facilitate,” creating potential overreach into tools that merely assist decisionmaking without playing a predominant or significant role.

HCM providers offer essential tools that support human workforce management decisions. These services include payroll processing, benefits administration, tracking of time and attendance, recruitment platforms, and performance evaluation systems. Notably, these systems do not independently determine outcomes; instead, they organize and streamline processes, enabling employers (the clients) to make decisions more easily. For example, payroll systems calculate and distribute wages based on employer-provided inputs, such as hours worked and agreed-upon compensation. The system does not decide employee pay or deductions—it simply executes calculations and payments in accordance with the employer's instructions. Benefits platforms apply employer-defined parameters to manage employee benefits, ensuring compliance with regulatory requirements. Recruitment and hiring tools may help employers manage candidate applications by sorting resumes or ranking candidates based on employer-defined criteria; however, the employer solely makes decisions. These HCM tools facilitate organization and efficiency, but they do not make or play a predominant role in decisions.

Labeling these tools as ADMT under the proposed regulations would mischaracterize their purpose and impose unnecessary compliance burdens on service providers who merely supply employer technologies that provide organization and efficiency. This overreach could lead to significant compliance costs and deter innovation. Without clarification, service providers may also be unfairly exposed to liability for decisions their systems did not make.

We recommend that the agency limit the definition to technologies that play a predominant or significant role, like New York City's ordinance that regulates ADMT tools only if they play a predominant or significant role in decision making. Additionally, we suggest the agency define "substantially facilitate" to specifically exclude tools that do not play such a role. If an ADMT merely provides supplemental information to human decision-makers without automating or determining outcomes, it should not be subject to the same regulatory scrutiny as systems that directly automate or determine final decisions.

1. **The proposed regulations state that "automated decision-making technology includes profiling," but the definitions of key terms, particularly "profiling" and "performance of work," leave room for potential confusion.**

   The proposed regulations include "profiling" as part of an ADMT and defines it as *"any form of automated processing of personal information to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's intelligence, ability, aptitude,* ***performance at work****, economic situation; health, including mental health; personal preferences, interests, reliability, predispositions, behavior, location, or movements."*

   Additionally, "performance at work" is defined as "the performance of job duties for which the consumer has been hired or has applied to be hired." The regulations specify that the following do not fall under that definition: a consumer's union membership or interest in unionizing; a consumer's interest in seeking other employment opportunities; a consumer's location when off-duty or on breaks; or a consumer's use of a personal account (e.g., email, text messages, or social media) unless solely to prevent or limit the use of these accounts on the business's information system or to prevent the disclosure of confidential information.

While these exclusions help clarify that specific activities are not considered part of profiling, the list raises questions about how broadly these exclusions apply, and whether activities not explicitly listed are subject to regulation's provisions regarding profiling or automated decisionmaking. It could also create ambiguity about whether the exclusion of those listed from profiling means they are automatically excluded from consideration in automated decisionmaking or could still be considered automated decisionmaking under certain circumstances.

Over the past few years, technologies that support employers' efforts to assess employee performance/productivity (e.g. performance management platforms) have evolved. Without narrowing the definition, any of these technologies can be labeled as "profiling." This broad definition could lead to business interruptions and increased costs to both the businesses that sell and those that purchase said software or applications.

2. **The proposed regulations risk unintentionally subjecting common technologies, like spreadsheets and databases, to regulation, creating compliance challenges.**

§ 7001(f)(4) reads: *"Automated decision-making technology does* ***not*** *include the following technologies, provided that the technologies do not execute a decision, replace human decision-making, or substantially facilitate human decision-making: web hosting, domain registration, networking, caching, website-loading, data storage, firewalls, anti-virus, anti-malware, spam- and robocall-filtering, spellchecking, calculators, databases, spreadsheets, or similar technologies. A business must not use these technologies to circumvent the requirements for automated decision-making technology set forth in these regulations. For example, a business's use of a spreadsheet to run regression analyses on its top-performing managers' personal information to determine their common characteristics, and then to find co-occurrences of those characteristics among its more junior employees to identify which of them it will promote is a use of automated decision-making technology, because this use is replacing human decision-making. By contrast, a manager's use of a spreadsheet to input junior employees' performance evaluation scores from their managers and colleagues and then calculate each employee's final score that the manager will use to determine which of them will be promoted is not a use of automated decision-making technology, because the manager is using the spreadsheet merely to organize human decisionmakers' evaluations."*

The provision excludes many commonly used technologies (e.g., spreadsheets, databases, and statistical analysis tools). However, the examples provided suggest that certain uses of these technologies (e.g., using spreadsheets to find patterns in employees' data for promotions) could still be considered ADMT. These technologies are widely used for legitimate purposes in HCM processes, such as employee performance assessments, succession planning, and talent analytics.

The proposed regulations distinguish between "automated decision-making" and tools that facilitate it, such as spreadsheets and databases, but the criteria for what constitutes automation are unclear. The provision states that a business should not use certain technologies to "circumvent" automated decision-making requirements, yet it does not fully define what constitutes "circumvention." The examples provided create confusion around what is permissible. For example, using a spreadsheet to analyze employee data could be classified as ADMT in one scenario (pattern recognition for promotions) but not in another (calculating performance scores). This inconsistency risks creating compliance challenges for businesses trying to adhere to the regulations. NPRC recommends further clarification and revision to exclude technology that is commonly used for traditional business purposes.

Proposed CCPA Mandatory Audit Requirement

The regulations would require certain companies doing business in California ("California Business(es)") to perform a mandatory annual cybersecurity audit on their service providers (hereafter, "Proposed CCPA Mandatory Audit Requirement"). This requirement applies to service providers, such as NPRC members, if they process personal information of California consumers (including employees) and if such processing presents a "significant risk to consumers' security."

Under the Proposed CCPA Mandatory Audit Requirement, an annual audit of NPRC members would be mandatory so long as the auditor seeks relevant information. If adopted, NPRC members and other service providers should expect annual audit requests from either the California Businesses internal auditors or an engaged external audit firm which may lack the time or scope limit incentive of typical of in-house auditors. The Proposed CCPA Mandatory Audit Requirement poses issues for NPRC members, or indeed any significant service provider that operates at scale, for the following reasons.

1. **Volume of Audit Responses Unsustainable**. NPRC members are "one-to-many" providers of Human Capital Management (HCM) services with large numbers of customers. Companies with large client bases commonly provide standardized offerings. As part of this one-to-many model, NPRC members create, update, and provide cybersecurity collateral prepared in advance to customers to inform them of their cybersecurity programs. This collateral also includes information about the cybersecurity frameworks under which they operate; these may include, for example, SOC-2, ISO27001 and ISO27701.

   The process of making this collateral available to clients helps substantially minimize the volume, time, and expense that NPRC members would otherwise face responding to individual client cybersecurity audits. Also, it avoids any risk related to breach of confidentiality. An auditor coming in to audit on behalf of one client might see data of another, depending upon how systems are structured. That obviously creates a privacy risk; one that is avoided by provided vetted security-related collateral.

   The Proposed CCPA Mandatory Audit Requirement will impose substantial cost, effort, and expense on NPRC members without benefit to California Businesses or cybersecurity protection. What California Businesses need is information sufficient for them to have confidence in the cybersecurity practices of their service providers. As noted above, this can be provided via a standard set of written materials. Rather than require service providers to respond to specific bespoke audit requests from each customer's auditors, the CPPA should define a set of required information that service providers much provide to California Businesses regarding their cybersecurity practices. This would avoid imposing a substantial and unnecessary burden on service providers while providing the same level of information that would be obtained from specific audit requests.

2. **Resource Burden; Diverts Resources Away from Other Cybersecurity Work.** In addition to the cost and volume discussed in Point 1, the predictable large volume of mandatory audits from California Businesses will unnecessarily shift the focus of valuable security resources at service providers away from their day-to-day work and turn them into document production experts. As noted above, NPRC members already provide customers with substantial cybersecurity collateral, consistent with our one-to-many approach in providing services. Requiring service providers to respond to individualized audit requests from clients would entail a shift in focus from day-to-day cybersecurity work to document production, without any corresponding benefit in transparency or protection.

3. **No Exceptions for Confidential/Proprietary Information.** The Proposed CCPA Mandatory Audit Requirement lacks an exception which allows a service provider to object to the disclosure of confidential, proprietary, or similar information in the audit. This could compromise the cybersecurity posture of companies such as NPRC members or disclose materials are confidential or proprietary to them, and which provide them with a competitive advantage, including even trade secrets. At best, as drafted, the proposal will not encourage openness and cooperation. At worst, an unbridled disclosure requirement without guardrails for confidential and proprietary information could have a paradoxical effect on companies which continue to drive toward best-in-class security practices. If mandatory to disclose all cybersecurity methods, they may be less inclined to invest in competitive technologies if they must disclose their innovations without any carve-outs to every California Business which asks in a mandatory annual audit.

Costs and Tiered Compliance

The CPPA's assessment estimated a $3.5 billion cost to comply in the first year with an average of $1 billion each subsequent year for the first ten years. These stunning numbers likely translate to negative business impacts including job losses. The proposed regulations would require transforming business operations and budgets. We recommend working with stakeholders to find ways to reduce these costs and create tiered compliance dates.

Conclusion

Again, NPRC appreciates the opportunity to provide input on the proposed regulations and acknowledges the agency's thoughtful work in addressing these important issues. We respectfully urge the CPPA to refine the definition of ADMT to exclude tools like HCM systems that do not predominantly or independently determine outcomes and that leave ultimate decision-making authority entirely with human operators. Narrowing the scope of the ADMT definition, consistent with precedents like New York City's ADMT ordinance, will help focus regulatory oversight on systems that truly warrant scrutiny while ensuring HCM tools remain accessible and cost-effective for businesses.

In addition, we request that the CPPA reconsider the Proposed CCPA Mandatory Audit Requirement. Instead of requiring individualized annual audits, we recommend defining a standardized set of cybersecurity information that service providers must supply to California Businesses. This approach would balance the need for transparency and cybersecurity confidence with the practical realities faced by service providers. By reducing duplicative compliance burdens, this framework would allow service providers to focus resources on enhancing security practices rather than excessive administrative tasks.

By adopting these recommendations, the CPPA can create a regulatory framework that advances its objectives of consumer protection and cybersecurity while avoiding unnecessary burdens on service providers. This balanced approach will support the continued innovation and availability of workforce management tools that benefit California businesses and their employees.

If we can provide any additional information, please do not hesitate to contact me at 973.974.5273.

Sincerely,

[redacted]

Daniel Lewis
President
National Payroll Reporting Consortium

Grenda, Rianna@CPPA

From:	Jessica Early <jearly@nuhw.org>
Sent:	Tuesday, February 18, 2025 7:32 AM
To:	Regulations@CPPA
Cc:	Benjamin Eichert
Subject:	NUHW's Public Comment on Risk Assessments and ADMT
Attachments:	NUHW Public Comment on Proposed Risk Assessment and ADMT Regulations 2.18.25.pdf

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

To the California Privacy Protection Agency:

Please find attached a letter from the National Union of Healthcare Workers in response to the request for comments on proposed regulations for the California Consumer Privacy Act.

If someone could please reply to confirm receipt, that would be much appreciated.

Thank you,
Jessica

Sent using voice dictation software. Please excuse typos.
JESSICA EARLY
Patient Advocacy Coordinator
National Union of Healthcare Workers
jearly@nuhw.org
(781)- 507-4035
Pronouns: she/her/hers

NUHW NATIONAL UNION OF HEALTHCARE WORKERS

866-968-NUHW • nuhw.org • info@nuhw.org

February 18, 2025

California Privacy Protection Agency
2101 Arena Boulevard
Sacramento, CA 95834

Dear Board Members, Executive Director Soltani, and Agency Staff,

The National Union of Healthcare Workers (NUHW) appreciates the opportunity to provide recommendations in response to the California Privacy Protection Agency's request for comments on proposed regulations for the California Consumer Privacy Act (CCPA). We commend Executive Director Soltani, Agency staff, and members of the Board for their commitment and dedication to giving guidance to California businesses, consumers, and now workers on the most important and consequential data privacy policy in the U.S.

NUHW represents over 19,000 healthcare workers across California who serve in diverse roles including mental health providers, certified nursing assistants, pharmacists, radiology, lab, and phlebotomy technicians, environmental and dietary service workers, respiratory therapists, nurses, nurse practitioners, and physicians. Our members work in a variety of settings including acute care hospitals, skilled nursing facilities, outpatient psychiatric clinics, home health, hospice, and correctional facilities.

The emergence of AI and other data-driven technologies represents one of the most important issues that will shape the work of our members–and workers across California–for decades to come. These emerging technologies potentially affect workers' privacy, race and gender equity, wages and working conditions, job security, health and safety, right to organize, and autonomy and dignity.

By covering worker data in the CCPA and in the promulgation of regulations, California has a historic opportunity to lead the U.S. in establishing workers as key stakeholders in decisions about how best to govern artificial intelligence and related technological innovations. It is also an opportunity to ensure that workers have the ability to control the collection and use of their personal data.

As a member of the California Federation of Labor Unions, we fully support the detailed recommendations that have been submitted under separate cover from the Federation, multiple other unions, and consumer protection groups. We would also like to underscore that the working conditions of our members are already being impacted by the rapid introduction of emerging technologies including AI. Our members' employers are increasingly engaging in electronic monitoring, data collection, and algorithmic management of workflow, scheduling, and even decisions about patient care. Employers typically deploy these technologies with no consultation with our members even though it's frontline healthcare workers who have the deepest understanding of what changes and improvements are needed to most effectively care for patients and foster a healthy, safe, and sustainable work environment.

Strong regulations under the CCPA could combat this type of healthcare industry failure to draw upon the knowledge, experience, and insights of frontline healthcare workers, who historically have served as watchdogs for the interests of patients and public health.

Some points of particular importance to our members include:

- These regulations must apply to the full range of employment-related decisions and uses of algorithmic systems–not just those uses the employer can claim "substantially facilitate" an employer's decision.
- We need strong notice and risk assessment provisions so workers have information and agency when technologies are being deployed in hiring and in the workplace. Our members' employers already must comply with a variety of regulations requiring assessments and notifications; employers have the capacity and responsibility to do so in this key area as well. Moreover, only through risk assessments will workers be protected in a proactive and preventative way–before they are subjected to potentially irreversible harms.
- Workers need to be empowered in the face of technology that has the potential to track, evaluate, and discriminate against or otherwise harm them. But broad exceptions to workers' ability to opt out of potentially significant algorithmic systems in the revised draft regulations undercut an important and essential right.

The U.S. workplace is rapidly becoming a major site for the deployment of AI and other digital technologies, a trend that will only escalate going forward. Full coverage and protection by the CCPA is a critical first step to ensure that California workers have the tools necessary to advocate for their rights–and the rights of the consumers they serve–in the 21st century data-driven workplace.

Thank you for the opportunity to provide feedback during this important rulemaking process.

Sincerely,

[redacted]

Sophia Mendoza
President, National Union of Healthcare Workers

Grenda, Rianna@CPPA

From:	Emily Emery <emily@newsmediaalliance.org>
Sent:	Wednesday, February 19, 2025 12:39 PM
To:	Regulations@CPPA
Subject:	News / Media Alliance Comment on ADMT Rulemakings
Attachments:	News Media Alliance Comment on ADMT Rulemakings 02.19.2025.docx.pdf

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Please see the attached comment on behalf of the News/Media Alliance.

Best regards,
Emily Emery

NEWS MEDIA ALLIANCE

Emily Emery
VP – Government Affairs
News/Media Alliance
Cell: [redacted]
emily@newsmediaalliance.org
www.newsmediaalliance.org
Follow Us!

NEWS MEDIA ALLIANCE

February 19, 2025

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

Re: Public Comment on ADMT Regulations

A thriving, free, and independent press is an essential part of any healthy democracy and plays a vital role in supporting California's economy and local communities. The News/Media Alliance ("The Alliance") is a nonprofit organization representing the newspaper, magazine, and digital media industries and empowers members to succeed in today's fast-moving media environment. The Alliance represents over 2,200 diverse publishers in the United States and internationally, ranging from the largest news and magazine publishers to hyperlocal newspapers and from digital-only outlets to papers that have printed news since before the Constitutional Convention. Alliance members are trusted and respected providers of quality journalism, and the Alliance diligently advocates on a broad range of current issues affecting news media entities, including consumer privacy laws and regulations that relate directly to Alliance members' trusted relationships with their readers.

The Alliance appreciates the support the California Privacy Protection Agency ("CPPA" or "Agency") has shown for an independent and free press. The Alliance respectfully submits the following comments and urges the Agency to carefully consider the potentially devastating impact of the proposed regulations in their current form[1] on the wide availability and affordability of high-quality journalism for California consumers.

[1] California Privacy Protection Agency, Proposed Text of Regulations (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations) (November 2024), available at: https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf.

Specifically, as set forth in greater detail below, the Alliance requests that the Agency better align its rulemaking with the underlying California Consumer Privacy Act of 2018:

1. modify the definition of "automated decisionmaking technology" ("ADMT") to exclude ADMT used by digital businesses in a manner beneficial to and expected by the consumer, such as content personalization and supporting increased access to free or low-cost journalism; and

2. strike the new definition of "behavioral advertising," and instead substitute in the CCPA's existing definition of "cross-context behavioral advertising," and remove "behavioral advertising" from the definition of "extensive profiling" in section 7150 (b)(3)(B)(iii).

The Proposed Regulations in Their Current Form Would Have Devastating Effects on Consumers by Restricting Access to Free or Affordable High-Quality Journalism.

Like all online businesses, newspapers, magazines, and digital publishers leverage automated technologies. These technologies enable publishers to provide California consumers with easy access to free and affordable high-quality, curated, and responsibly-presented journalism. Automated technologies also allow publishers to efficiently and at low cost, process information collected in highly transparent ways to make content more relevant, serve reasonably expected advertising, and offer consumer-friendly subscription deals.

The Proposed Rules Would Deny Consumers Certain Benefits, Such as Content Personalization and Subscription Deals, Without Mitigating any Risk of Harm and Without Adding Any Meaningful Consumer Privacy Benefits.

The proposed regulations would stifle long-appreciated and expected consumer benefits offered by publishers. Readers could lose access to services they expect and appreciate, including content personalization, subscription offers, and advertising tailored to their interests, including advertising informed by their activity on publishers' sites. This is not the intent of the CCPA and is inconsistent with the law. Millions of Californians rely on newspapers, magazines, and digital media to stay up to date on the latest local, domestic, and international news of greatest personal interest to them, including weather events and natural disasters, political developments, sports and entertainment, recipes, technology, product reviews and other topics related to their hobbies and activities. The definition of ADMT in the proposed rules would restrict publishers' ability to leverage machine learning to provide the personalized content that many consumers prefer, which is often supported by advertising. The proposed regulations would also restrict the ability of publishers to use ADMT to identify the right price point for consumers seeking affordable access to high-quality journalism.

This is contrary to the language and intent of the CCPA, as well as other robust privacy and data protection laws. The proposed regulations should not – and since they exceed the scope of the CCPA, legally ***cannot*** – give consumers unfettered rights to object to the processing of their information by any kind of automated technology. Particularly when this technology improves the consumer experience, reduces costs that are passed on to the consumer, and is used in ways that are consistent with the CCPA. Unfortunately, ADMT, as defined in the draft regulations, would include ***any kind of technology*** that "facilitates" a human decision. This definition distinguishes these proposed rules from the CCPA itself, as well as existing robust privacy rights under European Union and other U.S. state privacy laws that allow consumers to opt out of decisions made ***solely*** by automated technology, and only where the decisionmaking presents a significant or meaningful legal risk to the consumer (e.g., denial of employment, lending or housing).

Rather than create an unwarranted new precedent without a legislative directive, these regulations must instead remain consistent with the CCPA and should align with existing strong data protection laws by tethering those rights to decisions of legal significance or those that create a materially and demonstrative detrimental consequence for the consumer. Indeed, the Federal Trade Commission ("FTC") staff itself has recognized the consumer benefits of content personalization based on automated processing of personal information:

> [S]taff agrees that "first party" collection and use of consumer data may be necessary for a variety of consumer benefits and services. These

> include not only personalized content and other elements of the interactive online experience that consumers may value, but also important internal functions such as security measures, fraud prevention, and legal compliance.[2]

In addition to eliminating revenue-sustaining activities and extending beyond the scope of the CCPA, the proposed regulations also impact publishers' ability to use technology (whether "AI" or other "automated decisionmaking systems") to perform legally protected First Amendment activities. Additional AI regulations will inhibit publishers' ability to responsibly use and develop AI to help expand access to innovative journalism for consumers. Publishers already rely on various "automated decisionmaking systems" to run their businesses, by, among other things, helping publishers to serve and suggest content to readers, filtering feedback and leads, or analyzing primary source materials or large data sets for reporting purposes. These "automated" activities have no impact on consumers' privacy or data subject rights, putting these activities outside of the scope of the Agency and, therefore, outside of the scope of the Agency's rulemaking authority. Indeed, concern about such overreach in this rulemaking has been raised repeatedly by Agency Board Members without subsequent modification to the proposed rulemaking language.[3]

The proposed regulations should not prevent or otherwise restrict publishers from responsibly leveraging data using automated technology to make their personalized, edited content more readily available to readers at a reasonable cost, particularly in an environment otherwise rife with disinformation. The Alliance respectfully requests that the Agency modify the definition of "automated decision-making technology" to exclude ADMT used by digital businesses in a manner beneficial to, and expected by the consumer, such as content personalization and responsible advertising, which supports increased access to free or low-cost journalism and which is consistent with the CCPA.

[2] See Federal Trade Commission Staff Report: Self-Regulatory Principles for Online Behavioral Advertising: Tracking, Targeting, and Technology, February 2009 ("FTC Staff Report") at 27.

[3] See CPPA Board Meeting on December 8, 2023, starting at 00:18:37, and available at: https://youtu.be/KOmvtyffenY.

The Proposed Rules Would Require Support for Opt-Out Mechanisms in Ways Not Supported by the CCPA, FTC Guidance or Other State Laws and Would Needlessly Suppress Consumers' Access to High-Quality Journalism Content Supported by Consumer-Friendly First Party Advertising.

In their current form, the proposed regulations would effectively outlaw standard consumer-friendly *first party* advertising by news publishers, by giving consumers the ability to opt out of algorithmically targeted advertising. The overbroad proposal to include first party advertising within the proposed definition of "behavioral advertising" far exceeds the scope of opt-out rights in the CCPA, far exceeds the scope of the agency's authority, and contradicts longstanding principles set forth by the FTC and the laws of every other state. To restate the problem in the most straightforward terms – even where the publisher is responsibly collecting and using its own first party data to personalize content and ads through algorithmic models (as expected by and to the benefit of the consumer), the consumer would be able to have their data removed from such models under the proposed rules.

Readers are aware and expect that advertising and subscription pricing will be based on their behavior on publisher sites. This is also vital to publishers because it helps keep much quality content free or low-cost to access. Without this value exchange, some publishers may go out of business, impose more paywalls, or be forced to charge considerably higher subscription fees for access to their content. Without advertising designed to engage readers whose behavior reflects their interest in particular content or topics on publisher sites, it may be cost-prohibitive for most news media outlets to provide content to large swathes of readers – in California and across the country. Indeed, thousands of communities are already news deserts with no local daily newspapers (either in print or online). At the same time, many magazine publishers have reduced frequency or cut print and digital editions altogether.[4]

[4] See generally University of Northwestern, University, Local News Initiative, The State of Local News 2024 (last visited Jan. 31, 2025); Beth Braverman, How Magazine Publishers Are Cutting Print Costs to Improve Profits (Aug. 2, 2021), Folio Magazine (last visited Jan. 6, 2025).

As it stands today, and as intended by its authors, the CCPA allows a California consumer to opt out of "selling" or "sharing" their personal information, which is restricted to cross-site tracking. "Sharing" has a very specific definition – it means "sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party **for cross-context behavioral advertising**." "Cross-context behavioral advertising" means "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity **across businesses, distinctly branded internet websites, applications, or services, _other than the business_, distinctly branded internet website, application, or service with which the consumer intentionally interacts**."[5]

This "cross-context" opt-out right is also consistent with longstanding FTC guidance on the kind of cross-site "behavioral advertising" that should be subject to a consumer opt-out right. In its February 2009 Staff Report, FTC staff *rejected* the recommendations of some stakeholders that the Self-Regulatory Principles should apply to "first party" or "intra site" behavioral advertising because such advertising is more likely to be consistent with consumer expectations, first party processing is necessary to consumer benefits like personalized content, and first party handling limits the risk the data will be subject to unauthorized access:

> "Staff agrees that 'first party' advertising practices are more likely to be consistent with consumer expectations, and less likely to lead to consumer harm, than practices involving the sharing of data with third parties or across multiple websites. … Staff believes that, given the direct relationship between the consumer and the website, the consumer is likely to understand why he has received the targeted recommendation or advertisement and indeed may expect it. The direct relationship also puts the consumer in a better position to raise any concerns he has about the collection and use of his data, exercise any choices offered by the website, or avoid the practice altogether by taking his business elsewhere."[6]

[5] California Consumer Privacy Act, Cal. Civ. Code § 1798.140 (k).

[6] FTC Staff Report at 26-27.

This direct relationship is precisely what the CCPA provides for. As noted by the definition, the “opt-out” of “sales” or ”sharing” is limited to uses that relate to personal information collected and used on websites ***<u>other than</u>*** the first-party publisher. In ignoring the plain language of the CCPA and well-established precedent, the proposed regulations seek to newly define “behavioral advertising” as “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**.” The proposed rule, in addition to its novel and expansive definition (which goes far beyond the Agency’s authority), also equates such first party behavioral advertising with “extensive profiling,” which gives rise to a consumer opt-out right even in the absence of any risk of harm.

Such a broad opt-out right also ignores the trajectory across the country towards a consolidated, single, universal opt-out (commonly referred to as the “Global Privacy Control,” the “Universal Opt-Out Mechanism” or other broadly recognized “Opt-Out Preference Signals”) that only applies to cross-context behavioral advertising across ***unaffiliated*** websites. Issuing regulations that are out of step with the current nationwide landscape only increases compliance costs. In particular, it imposes a meaningful level of uncertainty on newspaper, digital, and magazine publishers, posing a devastating risk to access to journalism without adding any meaningful consumer privacy benefits.

Conclusion

The Alliance urges the Agency to preserve the essential role that news and media publishers play in disseminating reliable information to consumers through a trusted one-to-one relationship with readers and the role publishers play in the California economy.

The Alliance respectfully requests that the Agency strike the new definition of “behavioral advertising,” substitute in the CCPA’s existing definition of “cross-context behavioral advertising”, and remove “behavioral advertising” from the definition of “extensive profiling” in section 7150 (b)(3)(B)(iii).

Grenda, Rianna@CPPA

From: Tracy Rosenberg <tracy@media-alliance.org>
Sent: Wednesday, February 19, 2025 11:46 AM
To: Regulations@CPPA
Subject: ADMTS/Risk Assessments Rule-Making - Comments
Attachments: CPPA ADMTS - Risk Assessment - Comments of Oakland Privacy and Media Alliance.pdf

This Message Is From an Untrusted Sender

Warning: This email originated from outside of the organization! Do not click links, open attachments, or reply, unless you recognize the sender's email.

Report Suspicious

Please find enclosed joint comments from Oakland Privacy and Media Alliance on the Agency's Automated Decision Making Systems, Risk Assessments and CyberSecurity Audit Rule Making in progress.

--
Tracy Rosenberg
Executive Director
Media Alliance
2830 20th Street Suite 201
San Francisco, CA 94110
https://media-alliance.org
Email: tracy@media-alliance.org
415-746-9475 (office)
[redacted] (cell)
Encrypted email at [redacted]
Text via Signal
Pronouns: She/Her/Hers

-

OAKLAND PRIVACY

MEDIA ALLIANCE

February 19, 2025

California Privacy Protection Agency
2011 Arena Boulevard
Sacramento CA 94834
Email: Regulations@cppa.ca.gov

Comments of Oakland Privacy and Media Alliance on Risk Assessments and Automated Decision Making Technology Proposed Regulations - 2025

Thank you for the opportunity to provide comments on the proposed regulations. As civil society groups who have worked long and hard in the privacy and equity spaces, we welcome the CPPA's comprehensive look at the societal impacts of automated decision making technology.

Oakland Privacy is a citizen's coalition that works statewide to defend the right to privacy, enhance public transparency, and increase oversight of law enforcement, particularly regarding the use of surveillance techniques and equipment. We were instrumental in the creation of the first standing municipal citizens' privacy advisory commission in the City of Oakland, and we have engaged in privacy enhancing legislative efforts with several Northern California cities and regional entities. As experts on municipal privacy reform, we have written use policies and impact reports for a variety of surveillance technologies, conducted research and investigations, and developed frameworks for occasionally weigh in on proposals that have significant impacts on human and civil rights in California.

Media Alliance is a Bay Area democratic communications advocate. Our members include professional and citizen journalists and community-based media and communications professionals who work with the media. Our members are concerned with communications rights and digital platforms, especially at the intersections of class, race and marginalized communities.

JURISDICTION

We would like to begin these comments with a brief statement regarding the Agency's jurisdiction, which it seems is being contested by some stakeholders. In Section 1798.185 of the California Privacy Rights Act, which we should all remember was a ballot initiative passed by the voters of this state, the Attorney General and the CPPA as the designee and inheritor of the AG's rulemaking capacity, was explicitly authorized and in fact, instructed, to develop the rules proposed here. Bullet points 15 and 16 in that rather lengthy section very specifically charge the agency with restricting or prohibiting processing if it poses unacceptable risks or the risk to benefit ratio does not lean in favor of allowing the processing to continue. Moreover, the Agency is charged by the voters with governing access and opt-out rights and providing consumers with meaningful information. Nothing, and we emphasize *nothing* in the proposed regulations exceeds or infringes on the jurisdictional authority provided in the Act.

The various proposed regulations should be evaluated on their policy merits alone, i.e. whether or not they are effective at protecting against harms, and not subjected to specious arguments about whether or not the Agency has standing to promulgate them.

We have been disappointed to see some business groups resorting to alarmist language and attempting to pit one branch of government against each other. In all frankness, at the time the CA Privacy Rights Act was put to California voters, we had some concerns about it and did not endorse a yes vote. But California's voters didn't listen to us, and it is the law of this state that the CPPA is to promulgate these regulations. At this particular time, it is especially important that we all, whatever our set of interests, uniformly uphold the rule of law and the plain text of the ballot initiative Californians chose to support at the ballot box. That includes the Governor and the Legislature.

DEFINITIONS - 7001

"SUBSTANTIALLY FACILITATE"

The term substantially facilitate is used in the draft regulations to mean using the output of the technology as a key factor in human's decision making. The word substantially was added after the rewrite following the December 2023 release of draft regulations. The December 2023 draft language defined ADMT as "*a system to make or execute a decision or facilitate human decision making*". The current proposal changes the definition to "*a system that executes a decision, replaces human decision making, or substantially facilitates human decision making".*

We want to make clear that we believe that the common understanding of substantially facilitate and key factor do attempt to correctly demarcate the line between a ministerial use of machine learning to perform menial administrative tasks like alphabetizing or sorting or summarizing and an automated decision making process.

However, we have concerns that relying on adjectives like substantial and key to have a commonly understood meaning in what is basically a self-attestment process, may allow business interests to adopt a distorted meaning or at a minimum, let some bad actors slip through. Your substantial may not be my substantial.

We like the suggestion from the labor group and ACLU that the Agency consider adopting the State Administrative Manual (SAM) definition of an ADMT:

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.

It is certainly appropriate for a state administrative body to adopt a definition from the State Administrative Manual, and in this case we think the “*assist to human discretionary decision making*” is a clearer definition that is less subject to potential gamesmanship from bad actors.

“BEHAVIORAL ADVERTISING”

We want to strongly endorse the definition of behavioral advertising included in Section 7001(g). By expanding beyond “*cross-contex*t” advertising to include all targeted advertising based on profiles of consumers online and off-line behavior, the CPPA generally improves opt-out rights to target the surveillance advertising behavior that most disturbs users and consumers. Targeted ads based on behavioral profiling have consistently been linked to predatory advertising that seeks to take advantage of people’s vulnerabilities and to scams.

“**PERFORMANCE AT WORK**”

The definition of performance at work in Section 7001(ee) includes the performance of job duties for which the consumer has been hired or has applied to be hired. To our eye, the work-related activities not included in that definition range from a consumer’s union membership or interest in unionizing; a consumer’s interest in seeking other employment opportunities; a consumer’s location when off-duty or on breaks; or a consumer’s use of a personal account (e.g., email, text messages, or social media).

In an era when both union organizing and employer clampdowns on that organizing have increased exponentially, it is foolhardy to exempt these activities from workplace rules. Moreover, some workplaces have started to embrace such overbearing surveillance that it spreads from a narrow definition of work duties into any and all aspects of an employee’s life during their work day, including associations, expressions and personal and familial relationships.

In the December 2023 draft, the Agency included language that strove to describe these work-related harms that seem to be excluded from the narrower definition later adopted.

Constitutional harms, such as chilling or deterring consumers’ free speech or expression, political participation, religious activity, free association, freedom of belief, freedom to explore ideas, or reproductive freedom; and harms to consumers’ ability to engage in collective action or that impede the right to unionize.

We recommend that the December 2023 language be put back into the regulations.

“**ZERO TRUST ARCHITECTURE**”

The definition of “zero trust architecture” provided in the draft regulations, appears to us to be misleading and somewhat inaccurate. The current draft characterizes zero trust architecture in the following way:

Zero trust architecture is based upon the acknowledgment that threats exist both inside and outside of a business's information system, and it avoids granting access based upon any one attribute. For example, on an information system using zero trust architecture, neither the use of valid credentials nor presence on the network would, on its own, be sufficient to obtain access to information.

The fundamental premise of zero trust architecture is that systems do not require the provision of credentials or sensitive information for system processing and therefore a user does not need to “trust” that the system will not mishandle or leak their information because the system does not have it and cannot do so - and therefore they can interact with the system even if they have zero trust in it. The classic example is the messaging system Signal, originally created by Whisper Systems, which cannot hand over information about your texts because the system simply doesn’t have it.

We aren’t sure where this definition came from, but we encourage you to revisit it and seek a definition that provides more clarity to California businesses and consumers. Or if you wish to continue using the definition you have, supplement it with examples that make it easier for people to understand the intended meaning.

“SENSITIVE PERSONAL INFORMATION”

The current definition of sensitive personal information includes information about a consumer’s health, sex life and sexual orientation, as well as their geneticr data.

We would like to see this include information about a consumer’s gender identity. While we understand that perceived gender is important for advertisers who often target messages to men and women differently, in the context of algorithmic decision making systems and how to protect the sensitive personal information they process, it seems important to us in the current era to prioritize trans individuals as a vulnerable and sensitive group often subjected to intense discrimination, if not outright erasure. When we discuss how machines decide who gets jobs, housing, business loans, health care, or pre-trial release, status as a transsexual person can be interpreted as a liability by both machines and the people who program the machines, and this bias need to be explicitly labeled and addressed.

SYMMETRY IN CHOICE – 7004

We wanted to take a second to thank the Agency for the strong language regarding symmetry in choice, namely that opting out needs to be exactly as easy in opting in. There is also strong language in this section regarding consent and that a consumer’s silence or failure to act affirmatively does not constitute consent. This is desirable language that shows that regulators have learned from the weaknesses of earlier privacy laws. It should stay in the final version.

NOTICE OF RIGHT TO LIMIT – 7027

This section grants an employer a right to scan employee emails for the purpose of checking if employees are leaking sensitive business information. However, if in the process of scanning emails for this purpose, it isn’t clear if ancillary uses/information uncovered in the scanning for the allowed purpose are prohibited or not. We think this section would be improved by the addition of “*sole purpose*” to the language allowing email scanning.

PURPOSE OF ADMTS – 7152

The current draft states that “*the business must specifically identify its purpose for processing consumers’ personal information*”. We believe this language provides too much room for overly generic, bland and pro forma statements about the purpose of the processing, like “security reasons” or “to improve business efficiency”. These catchall descriptions are pretty much the equivalent of saying nothing at all and do not provide the necessary transparency for either the consumer or for regulators.

Language removed from the December 2023 draft provided a more meaningful purpose description and we suggest that it be restored.

The business must specifically identify its purpose for processing consumers’ personal information, how the processing achieves that purpose, and the purpose’s compatibility with the context in which the personal information was collected.

HUMAN APPEAL – SECTION 7200

The ability of a consumer to appeal the verdict of an ADMT to a human reviewer is a crucial fairness doctrine. Accordingly, this portion of the regulations must be structured to maximize fairness to the consumer. We think some improvements can be made here in a few areas.

a) What does the adjective “qualified” mean in this regard? Who is qualified and what makes them qualified? We would like to see some more clarity - perhaps some required training or certification - or it seems like the qualification required is little more than a self-attestation of being qualified.

b) Basic conflict of interest provisions must be addressed. The person performing the human appeal cannot have financial interests that are impacted by the decision made, directly or indirectly, nor can they have been involved in any way in the initial selection process and thus incentivized to determine that the process worked well or was fair. As labor groups have pointed out, some regulatory language can be derived from Title IX processes that may be helpful.

c) As with literally any similar process, a reviewer needs to be inoculated against negative consequences or retaliation from the business for choosing to overturn an ADMT-assisted decision. This is a basic measure of fairness to prevent businesses from being able to place their foot upon the scale to determine how the appeal ends up.

d) Companies should be required to allocate ample resources to fund a robust human appeal process. Starving such a process of funds so that quality personnel cannot be retained, for example, should not be tolerated.

RETALIATION AGAINST CONSUMERS – 7221

We agree with the labor groups who ask for an explicit statement regarding the prohibitions against businesses retaliating against consumers for exercising their rights regarding an ADMTS.

Suggested: A business must not retaliate against a consumer because the consumer exercised their opt-out right, including, but not limited to, their right to opt-out of the use of an ADMT, their right to access details about an ADMT-assisted decision, or their right to appeal an ADMT-assisted decision, as set forth in Civil Code Section 1798.125 and Article 7 of these regulations.

DEFINITION OF ADVERSE SIGNIFICANT DECISION - 7222

We strongly suggest that employee discipline issues, including not being promoted or being involuntarily transferred, be included in adverse significant decisions that trigger additional access and notice requirements.

For some workplaces, machine-driven promotion or demotions and transfers between work sites can be of great import to employees and when delivered without clear explanations - and/or with seeming bias - can be extremely harmful. The definition of an adverse significant decision should be broadened to reflect the significance to consumer’s lives, especially low-wage workers, of disciplinary and locational decisions in employment.

AUTHORIZED AGENT – 7222

We strongly recommend that consumers be allowed to seek the help of an authorized agent to assist them to exercise the rights granted to them regarding ADMTS. While one obvious example of that is a worker being able to request the help of their bargaining unit, that is far from the only example.

In health care, patients and families often seek the help of patient advocates, who may be friends or other contacts to assist them in navigating the unwieldy health and hospital system and elderly and/or individuals lacking English fluency may designate a younger relative to speak for them with the bank or financial institution. All of these assistance needs should be explicitly authorized in the regulations as they are necessary to assure the usability of provided rights by all California residents, including those less well-equipped to exercise them independently.

We are sure that some stakeholder groups will raise the specter of paid businesses forming to assist consumers, as were raised during the "DROP" rulemaking. While that may be possible, we don't see the actual problem. If enough consumers want, and are willing and able to pay for, assistance in exercising their notice and opt-out rights with regards to ADMS, then the free market may provide such assistance and should. Business groups concerned about such a development can prioritize making it easy to exercise such rights and thus lower the likelihood of such an industry developing in response to consumer demand.

Suggestion: A consumer may use an authorized agent to submit a request to access information about a business's use of an automated decisionmaking technology on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf.

ENFORCEMENT – RISK ASSESSMENTS

The current draft of the regulations has a bit of donut hole in the middle when it comes to what happens to risk assessments after they are completed. While the clear intention of the regulations is to create a culture of businesses assessing their own systems and reacting appropriately to assessments and taking corrective action on their own, and many will, regulatory systems have to account for potential bad actors.

We can certainly envision a scenario where despite an assessment that finds many flaws and discrimination risks in an ADMT, a business may conclude that the personnel savings make the costs outweigh the risks to consumers and the system to be an overall benefit to the business.

However, a public interest entity may not make the cost/benefit analysis in quite the same fashion when the risks constitute significant adverse and unfair decisions affecting consumer's lives in ways that can cause irreparable damage.

We believe that there has to be an explicit mechanism present for the Agency to review risk assessments, and in the event of a clear deficiency, for the CPPA or perhaps another agency, to be able to take corrective action to protect consumers from harm.

We endorse the following suggestion from the ACLU to add such an explicit mechanism to the regulations – and caution that regulations without enforcement teeth rarely achieve their goals, even if the enforcement teeth are used sparingly.

Upon review of a business's Risk Assessment, if the Agency has a 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.

Finally, we would just like to briefly address the common complaint from business stakeholders, and occasionally some members of the Agency itself, that these proposed regulations are "onerous". No business in California is required to use an automated decision making system (ADMTS) and those that choose not to do so are entirely unaffected by these proposed regulations. That probably includes the vast majority of California's small businesses which will continue to sell flowers, dish up coffee and sandwiches and sell potpurri without the aid of machine learning.

Those that choose to use these systems are choosing to do so because they believe they will save money by automating certain functions. It is not too much to ask that some of the money and resources created by this automation be reinvested in the safety of consumers who are being subjected to automation in order to enhance the profits of others. We should not seek to enhance business revnue at the expense of harm to customers and consumers.

As in the Industrial Revolution long ago, the benefits of technology innovation also need to manifest in benefits to the workers and consumers, like (at that time) weekends and overtime. Those things did not happen without a fight, and new benefits probably won't happen without a fight this time, but in the end, we all came to the societal conclusion that weekends were good and that increased productivity caused by technological innovation needed to be accompanied by benefits for non-business owners.

The same is true in the here and now. Increases in productivity require additional measures to ensure there are not harms and are fungible benefits for all. These regulations are a step in that direction and should be seen as such.

America would not have been a better place in the 20th century with 7 days a week, 10 hour a day wor week and America will not be a better place in the 21st century with unfettered machine decision making.

Thank you for the opportunity to submit these comments and thank you for your work on behalf of Californians.

Sincerely,

[redacted]

Tracy Rosenberg
Executive Director
Media Alliance
2830 20th Street
San Francisco CA 94110
https://media-alliance.org

and

Advocacy Director
Oakland Privacy
P.O. Box 3003
Oakland CA 94609
https://oaklandprivacy.org