COVINGTON

BEIJING BOSTON BRUSSELS DUBAI FRANKFURT
JOHANNESBURG LONDON LOS ANGELES NEW YORK
PALO ALTO SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

Covington & Burling LLP
Salesforce Tower
415 Mission Street, Suite 5400
San Francisco, CA 94105-2533
T +1 415 591 6000

February 18, 2025

By Electronic Mail

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Boulevard
Sacramento, California 95834
regulations@cppa.ca.gov

Re: CCPA Rulemaking

The California Chamber of Commerce ("CalChamber") submits these comments in response to the California Privacy Protection Agency's ("CPPA" or "the agency") request for public input on draft regulations regarding automated decisionmaking technologies ("ADMT"), cybersecurity audits, and privacy risk assessments (collectively, "Draft Regulations").[1] CalChamber's members reflect a diversity of small, medium, and large businesses across industries and sectors in the state and approximately a quarter of all California private sector jobs.[2]

CalChamber supports the stated goal of the Draft Regulations to protect consumer privacy and security while advancing innovation.[3] However, the Draft Regulations fall short of this goal and require significant revisions to avoid both overreaching the limits of the statute and detrimental consumer impacts. While in no way an exhaustive list, CalChamber urges the CPPA to implement revisions to address, for example, concerns that the Draft Regulations and the Standardized Regulatory Impact Assessment ("SRIA"):

- Overreach the CPPA's statutory authority and encroach on the California Legislature and Governor's ongoing efforts to strike a balance in ADMT regulation;
- Conflict with existing statutory rights and exemptions;

[1] *See* CPPA, *Proposed Text of Regulations (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations)* (Nov. 22, 2024), https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf [hereinafter Draft Regulations]; California Regulatory Notice Register, Volume 47-Z.

[2] *See* CalChamber, *CalChamber Membership*, https://www.calchamber.com/calchamber-membership#:~:text=CalChamber%20membership%20represents%20one%2Dquarter,thrive%20through%20challenges%20and%20adversity.

[3] *See* California Privacy Protection Agency, *Initial Statement of Reasons on Updates to existing CCPA regulations; Cybersecurity Audits; Risk Assessments; Automated Decisionmaking Technology; and Insurance Companies*, 3, 23, https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_isor.pdf [hereinafter Initial Statement of Reasons]; *see also* California Proposition 24 of 2020 (codified as Cal. Civ. Code § 1798.110 *et seq.*), § 3(C)(1), https://cppa.ca.gov/regulations/pdf/prop24_text.pdf [hereinafter CPRA Ballot Initiative] ("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.").

- Depart from established global privacy frameworks and standards;
- Undercut foundational constitutional protections; and
- Drastically underestimate the costs that the Draft Regulations will impose on businesses and the state.

Each of these concerns are discussed further in the sections below. Proposed edits to the Draft Regulations are reflected in the Appendix and provide reasonable alternatives that demonstrate how the CPPA can protect and advance consumer privacy and security interests without creating unnecessary and unreasonable burdens on businesses.

I. The Draft Regulations Overreach The CPPA's Statutory Authority.

The Draft Regulations require substantial revision in order to conform to the bounds of the statutory text. For example, the Draft Regulations on ADMT inappropriately transform the California Consumer Privacy Act's ("CCPA" or "the statute") limited privacy framework into broad AI regulation and attempt to legislate through rulemaking new opt-out rights that are absent from the statutory text. To be consistent with the existing statutory opt-out rights, the ADMT opt-out requirements must be limited to significant decisions made without human involvement that present a significant risk to consumer privacy. Moreover, the broader behavioral advertising and the ADMT training restrictions must be removed. In addition, requirements for explainability, cybersecurity audits, and privacy risk assessments must be revised for the agency to avoid exceeding the authority granted to it in the statute.

A. The Draft Regulations Expand Beyond Privacy Requirements Into Broader AI Regulation, In Contravention Of The Statute And Ongoing Efforts Of California's Elected Representatives.

The Draft Regulations go far beyond the narrow grant of authority for the agency to issue privacy rules clarifying how the CCPA's existing "access and opt-out rights" will be interpreted in the context of ADMT.[4] Instead, the Draft Regulations improperly enlarge the statutory scope by imposing over 45 pages of sweeping ADMT regulations covering bias, explainability, model training, and other risks addressed in broader AI frameworks.[5] For example, the Draft Regulations propose risk assessments that more closely resemble AI impact assessments than

[4] Cal. Civ. Code § 1798.185(a)(14),(15). To determine whether a regulation is "consistent and not in conflict" with the agency's authorizing statute, courts look to "whether the regulation is within the scope of the authority conferred." *California Chamber of Com. v. State Air Res. Bd.*, 10 Cal. App. 5th 604, 619 (2017); *see also* Cal. Gov't Code § 11342.2 (stating that "no regulation adopted is valid or effective unless consistent and not in conflict" with the agency's authorizing statute). The California voters provided clear direction in 2020 through Proposition 24 that the CPPA's mission is limited to protecting consumer privacy, and does not extend to broader AI regulation. *See* CPRA Ballot Initiative, § 2(L).

[5] *Compare, e.g.*, The EU AI Act, Regulation (EU) 2024/1689, arts. 11, 27 (requiring impact assessments and technical documentation for high-risk AI systems); Colorado AI Act, Colo. Rev. Stat. §§ 6-1-1703(2), (3); 6-1-1702(2) (requiring impact assessments, risk management programs, and technical documentation for high-risk AI systems), *with* Draft Regulations § 7222. Notably, Cal. Civ. Code § 1798.185(15) makes no mention of topics like self-testing, pre-use notices, or explainability. It is a court's "obligation to strike down such regulations" if they "alter or amend the statute or enlarge or impair its scope." *Naranjo v. Spectrum Sec. Servs., Inc.*, 88 Cal. App. 5th 937, 945 (2023), *aff'd* 15 Cal. 5th 1056, 547 P.3d 980 (2024).

privacy risk assessments.[6] Moreover, while nothing in the statute requires businesses to create and share documentation with other enterprises, the Draft Regulations would require businesses to create technical documentation that is similar to, but also broader than, the technical documentation required of high-risk AI systems under laws that focus on regulating a type of technology, not the processing of personal information, like the EU AI Act and Colorado AI Act.[7] Businesses with certain ADMT applications or systems also would be required to conduct self-testing to confirm the technology works as intended and does not result in discrimination under state and federal civil rights laws, and would have to comply with broad governance requirements including policies, procedures, and training – requirements all untethered from the agency's limited privacy mandate.[8] Because the Draft Regulations exceed the scope of the statutory authority, they must be substantially revised to align with the statutory text and voter intent.[9]

This overreach is particularly concerning given that the Legislature and Governor Newsom continue to assess how best to regulate AI in a manner that preserves California's position as a world leader in AI innovation. For example, the California Legislature passed, and the Governor signed, a number of laws related to AI last year, including laws specifically addressing disclosures regarding the use of AI.[10] *None* of these laws provided the CPPA with rulemaking authority. The Legislature also abandoned, or the Governor vetoed, a variety of other ADMT proposals that the CPPA now attempts to unilaterally enact through the Draft

[6] Draft Regulations § 7152(a)(3)(G) (requiring risk assessments to take into account, for example, the technology used in processing, including any assumptions or limitations of the logic and the output of the ADMT).

[7] *See* The EU AI Act, Regulation (EU) 2024/1689, arts.11, 27 (requiring impact assessments and technical documentation for high-risk AI systems); Colorado AI Act, Colo. Rev. Stat. § 6-1-1702(2).

[8] Draft Regulations § 7201(a)(1); *see also* Draft Regulations §§ 7221(b)(3)(B); (b)(4)(B); (b)(5)(B). Not only do the Draft Regulations exceed the authority permitted in the statutory text, the Draft Regulations also exceed the CPPA's jurisdiction and set forth rules where other California agencies have authority and have issued requirements. Specifically, the California Civil Rights Department issued regulations to protect against employment discrimination with ADMT in May 2024. *See* Press Release, *Proposed Regulations to Protect Against Employment Discrimination in Automated Decision-Making Systems* (May 17, 2024), https://calcivilrights.ca.gov/2024/05/17/civil-rights-council-releases-proposed-regulations-to-protect-against-employment-discrimination-in-automated-decision-making-systems/.

[9] *See, e.g.*, November 8, 2024 Board Meeting Transcript, 102, https://cppa.ca.gov/meetings/materials/20241108_audio_transript.pdf [hereinafter November 8, 2024 Board Meeting Transcript] (reflecting Board Member Mactaggart's experience in drafting the text that the scope should focus on the nature of the activity, not the technology involved); *id.* (noting Mactaggart's statements that "ADM is just a tool. It does not inherently impact privacy. And it was specifically omitted from [risk assessments] when drafting the statute").

[10] *See* CA AB 2013 (requiring developers of generative AI systems to make disclosures about training data); CA SB 942 (mandating generative AI watermarks). The California Legislature also passed, and the Governor signed: CA AB 2602 (required contractual terms for digital replicas), CA SB 1120 (AI healthcare decisionmaking), CA SB 981 (AI-generated intimate imagery), CA AB 2355 and CA AB 2839 (AI-generated political ads), and CA SB 926 (AI-generated intimate imagery).

Regulations.[11] For example, efforts to require ADMT impact assessments,[12] audits and testing,[13] and policies to govern ADMT systems each failed to be enacted into law,[14] and some would have provided oversight authority to other California agencies.[15] Indeed, the Legislature specifically contemplated and eventually removed authority for the CPPA to oversee AB 2930 (Bauer-Kahan, 2024) during the committee process.[16] Nevertheless, the Draft Regulations would impose prescriptive disclosure requirements in the form of, for example, publicly available pre-use notices, disclosures of technical documentation, and certifications of risk assessments. Not only has the California Legislature clearly indicated that it intends to issue legislation on these exact matters, the Legislature also has clearly evidenced its intent to limit the agency's rulemaking authority with respect to ADMT disclosures to *reactive* responses to a consumer's specific request to access their own personal information. Because the Draft Regulations "alter or amend the statute or enlarge or impair its scope,"[17] each provision requiring proactive ADMT disclosures must be removed from the Draft Regulations.

Importantly, it would be one thing for elected representatives to revisit those public policies in the new legislative session; it is entirely another for the CPPA to adopt those rejected and/or abandoned policies via regulations, knowing they failed enactment. The CPPA, led by its five unelected board members, encroaches upon the role of California's elected representatives by proposing Draft Regulations that would impose broad bias, accuracy, transparency, and documentation requirements, even though its enabling statute focuses on consumer privacy. The potential for conflicting ADMT policy priorities is likely to increase because the California Legislature is preparing to focus on ADMT legislation in the current session.[18] Accordingly, the CPPA must limit the Draft Regulations to clarifying how the CCPA's existing "access and opt-out rights" will be interpreted in the context of ADMT and the CPPA's privacy mandate and defer to

[11] *See, e.g.*, CA AB 2930, 2023–2024 Leg. (Ca. 2024). (ADMT used for consequential decisions), CA SB 1047, 2023–2024 Leg. (Ca. 2024) (large AI models that pose risks to public safety), CA AB 3211 (generative AI content labeling), CA AB 3050, 2023–2024 Leg. (Ca. 2024) (synthetic content watermarking), CA AB 1791, 2023–2024 Leg. (Ca. 2024) (digital content provenance standards), and CA AB 1651 (workplace surveillance).

[12] CA AB 2930, 2023–2024 Leg. (Ca. 2024) (proposing impact assessments for ADMT consequential decisions).

[13] CA SB 1047, 2023–2024 Leg. (Ca. 2024) (requiring annual retention of a third-party auditor).

[14] *Id.* (requiring written policies and procedures for certain covered models).

[15] CA AB 2930, 2023–2024 Leg. (Ca. 2024) (providing the Civil Rights Department, rather than the CPPA, with enforcement authority).

[16] *See* CA AB 2930, 2023–2024 Leg. (Ca. 2024) (Jul. 3, 2024 Amended Version) (removing requirements that state government deployers provide reports to the CPPA).

[17] *Naranjo*, 88 Cal. App. 5th at 945.

[18] *See, e.g.,* Emily Hamann, *Lawmakers gear up for more debate on AI in the new session*, State Affairs (Dec. 10, 2024), https://pro.stateaffairs.com/ca/ai/artificial-intelligence-legislation-regulation; Julia Marsh, *Newsom's AI working group sets out timeline in wake of SB 1047 veto*, Politico Pro (Dec. 11, 2024), https://subscriber.politicopro.com/article/2024/12/newsoms-ai-working-group-sets-out-timeline-in-wake-of-sb-1047-veto-00193868; *Update from the Co-Leads of the Joint California Policy Working Group on AI Frontier Models* (Dec. 11, 2024), https://hai.stanford.edu/sites/default/files/2024-12/20241211_Joint_CA_AI_Update.pdf (describing the group's work to develop a report on responsible AI development in the state at the direction of Governor Newsom).

California's elected representatives in deliberations about the appropriate scope of and approach to broader ADMT regulation.

In narrowing the Draft Regulations to align with the statutory text, the agency also should be guided by Governor Newsom's directive to adopt a "measured approach" so that California "remain[s] the world's AI leader."[19] This requires, for example, that Draft Regulations interpreting how the statute's existing opt-out rights apply in the context of personal information used for ADMT impose the same standards as those enacted under other consumer privacy frameworks to avoid putting California businesses at a regulatory disadvantage.[20] Specifically, and as described further in the next section, the Draft Regulations should allow consumers to opt out only where their personal information is used by ADMT without human involvement that results in a significant decision being made about that particular consumer.

B. The Draft Regulations Cannot Independently Regulate AI And Must Be Limited To ADMT Used To Make Significant Decisions Without Human Involvement, Consistent With Existing Statutory Opt Outs.

The Draft Regulations propose to regulate ADMT and AI, both of which are defined in a manner unmoored from the CCPA's statutory text. As a result, the Draft Regulations require significant revision to align to the narrow scope of rulemaking authority granted to the agency.[21]

As a threshold matter, nothing in the statute authorizes the agency to enact regulations governing "artificial intelligence." In fact, the CPRA Ballot Initiative did not include the term "artificial intelligence." Instead, the plain text of the statute makes clear that the agency is only authorized to issue regulations that clarify how specific statutory provisions apply in the context of "businesses' use of automated decisionmaking technology"[22] that is relevant to consumer privacy.[23] Nevertheless, in multiple places throughout the Draft Regulations, the CPPA proposes to regulate "artificial intelligence" as a technology distinct from ADMT.[24] Because the inclusion of AI "alter[s] or amend[s] the statute or enlarge[s] or impair[s] its scope," all references to AI must be stricken from the Draft Regulations.[25]

[19] Press Release, *Governor Newsom Signs Executive Order to Prepare California for the Progress of Artificial Intelligence* (Sept. 9, 2023), https://www.gov.ca.gov/2023/09/06/governor-newsom-signs-executive-order-to-prepare-california-for-the-progress-of-artificial-intelligence/. Executive Order N-12-23 and accompanying press releases underscore the Governor's broader strategy for AI that is not limited to generative AI.

[20] *See* CPRA Ballot Initiative, § 3(C)(8) ("To the extent it advances consumer privacy and business compliance, the law should be compatible with privacy laws in other jurisdictions").

[21] *See California Chamber of Com.*, 10 Cal. App. 5th at 619 (underscoring that regulation is not valid if in conflict with the agency's authorizing statute); *Naranjo*, 88 Cal. App. 5th at 945 (stating that courts must strike down regulations that "alter or amend the statute or enlarge or impair" the scope of the statute).

[22] Cal. Civ. Code § 1798.185(15).

[23] CPRA Ballot Initiative, § 2(L) (underscoring the focus on consumer privacy and the CPPA's role as a regulator "whose mission is to protect consumer privacy").

[24] See Draft Regulations §§ 7150(b)(4); 7152(a)(2)(B); 7153.

[25] *Naranjo*, 88 Cal. App. 5th at 945. To the extent that a definition of AI is necessary for the limited purpose of giving meaning to how the agency defines ADMT for its ADMT regulations, the agency should use the definition adopted by California's lawmakers in AB 2885 (Chapter 843, Statutes of 2024) last year and applied throughout all AI legislation enacted last year.

Moreover, the plain text of the statute requires that the Draft Regulations be limited to the processing of personal information by technology that both (1) is *automated* and (2) makes a *decision*. The definition in the Draft Regulations is overbroad on both of these points.[26] First, the proposed definition is not limited to "automated" processing. Where a human has the capability to overturn a decision, that decision is – by definition – not automated.[27] The text of the Draft Regulations explicitly concedes this fact by recognizing the ability of a human to overturn an ADMT decision as part of the human appeal exception.[28] Second, the Draft Regulations inappropriately encompass technology that substantially facilitates human decisionmaking within the scope of ADMT, which exceeds the statute's explicit direction to issue rules on automated *decisionmaking*.[29] Technologies capable of only supporting a decision do not themselves make a decision. Similarly, ADMT training does not itself result in any decision about a particular consumer, and therefore is outside the clear bounds of the rulemaking authority. As another example, automated software to identify whether a benefits application omits components so that a case manager can efficiently request additional details does not itself make decisions. Incorporating technologies that merely inform human decisionmaking does not reflect the California electorate's limited scoping for ADMT regulations.

The overbreadth of the Draft Regulations results in vague, arbitrary, and capricious regulation susceptible to administrative challenge. Board Member Mactaggart appeared to recognize this concern, noting the confusing and extremely broad scope of the ADMT provisions in the Draft Regulations.[30] For example, the text of the Draft Regulations is circular and misleading, indicating that ADMT does not include certain technologies, like a calculator or spellchecking, but only if they are not used as ADMT.[31] Although the Draft Regulations disclaim an intent to regulate everyday technologies,[32] the breadth of the definition sweeps such tools into its scope. Similarly, the Initial Statement of Reasons emphasizes that the Draft Regulations provide only an "illustrative" and "non-exhaustive" list of what could qualify as ADMT, underscoring both the breadth of the term and the challenge in determining what would and would not be included.[33] To address this concern, the ADMT definition must be narrowly calibrated to address privacy harms that are the specific aim of the CCPA.

[26] The definition of AI also introduces confusion by encompassing all systems that resemble or include AI (*e.g.*, generative AI, AI models, AI systems), and therefore fails to calibrate requirements to the risks presented by different versions of AI technologies.

[27] The Cambridge Dictionary defines "automated" as "carried out by machines or computers *without needing human control*." Cambridge Dictionary, https://dictionary.cambridge.org/us/dictionary/english/automated.

[28] Draft Regulations § 7221(b)(2).

[29] *See* Cal. Civ. Code § 1798.185(15) (directing the CPPA to issue regulations on automated decisionmaking technologies, as opposed to all automated technologies).

[30] *See, e.g.*, November 8, 2024 Board Meeting Transcript, 99-102.

[31] Draft Regulations § 7001(f)(4) (excluding these technologies only "provided that the technologies do not execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking").

[32] *Id.*

[33] Initial Statement of Reasons at 14-15.

Notably, nothing in the statutory text creates an independent ADMT opt-out right.[34] To the contrary, the statutory text limits the scope of the regulations to interpreting how the existing opt-out rights – the opt-out of sale, sharing for cross-context behavioral advertising, and use or disclosure of sensitive personal information – will apply where a business uses ADMT for such processing. Although the voters had the opportunity in the CPRA Ballot Initiative to create a separate ADMT opt-out right, they explicitly limited the agency's authority to establishing opt-out right regulations "*with respect to* a business's use of automated decisionmaking technology."[35] Because the most logical interaction of ADMT with existing opt-out rights exists in the context of processing sensitive personal information to make a significant decision about a particular consumer, the Draft Regulations should focus on the consumer's right to opt out of such processing. This approach is supported by the statutory text, which connects the ADMT opt-out right to "profiling."[36] There is also substantial overlap between the profiling and sensitive personal information concepts. Specifically, "profiling" is defined as the "automated processing" of personal information to, for example, evaluate or predict aspects of a person's "performance at work, economic situation, health," and similar aspects.[37] This shares meaningful similarities with the scope of sensitive personal data, as it includes, for example, health, financial information, and union membership.[38] Accordingly, to avoid overreaching the statute's authority, the Draft Regulations should be limited to the use of ADMT for significant decisions, such as those relating to employment, education, benefits, legal services, and healthcare.[39]

The agency's recent references to AB 1008 do not remedy the Draft Regulations' inappropriate overreach.[40] First, the Legislature's narrow amendment to the definition of personal information does not authorize the agency to broadly regulate the field of AI. AB 1008 clarifies that personal information can exist in many forms, including AI systems "capable of

[34] The only mention of the ADMT opt-out is in Section 1798.185(15).

[35] Cal. Civ. Code § 1798.185(15) (emphasis added).

[36] *Id.*

[37] Cal. Civ. Code § 1798.140(z).

[38] *Compare* Cal. Civ. Code § 1798.140(z) (defining profiling 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 *performance at work, economic situation, health*, personal preferences, interests, reliability, behavior, *location, or movements*") (emphasis added) *with* Cal. Civ. Code § 1798.140(ae) (defining sensitive personal information as (1) personal information that reveals a consumer's *social security, driver's license, state identification card, or passport number*; account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; *precise geolocation*; racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or *union membership*; contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication; genetic data; and neural data; and (2) *biometric information for the purpose of uniquely identifying a consumer*; personal information collected and analyzed *concerning a consumer's health*; and personal information collected and analyzed concerning a consumer's sex life or sexual orientation) (emphasis added).

[39] If the CPPA chooses to remain focused on the nature of the decision, CalChamber requests that the agency narrow the scope of "access to, or provision or denial of, . . . essential goods and services" to emergency situations.

[40] *See, e.g.*, Notice of Proposed Rulemaking (Nov. 22, 2024).

outputting personal information."[41] The amendment neither expands the scope of the statute to cover AI systems nor enlarges the agency's authority to create regulations touching on AI.[42] Accordingly, the Draft Regulations' obligations related to AI development, underlying technology, governance, and numerous other topics "alter[s] or amend[s] the statute or enlarge[s] or impair[s] its scope" and must be revised.[43] Additionally, only after the business community identified the Draft Regulations' overreach did the agency mention AB 1008. The agency cannot retroactively legitimatize the Draft Regulations, which were drafted before AB 1008 was passed. Therefore, AB 1008 does not provide a basis for the agency to regulate AI, and the Draft Regulations must be substantially revised.

In sum, the Draft Regulations should refrain from generally regulating AI and must focus the ADMT opt-out on the processing of personal information to make a significant decision without human involvement and where a significant risk to consumer privacy exists.[44]

C. The Behavioral Advertising Requirements Would Also Be Inconsistent With The Scope of the CPRA Amendments.

The Draft Regulations invent new obligations, including an opt-out right, for "behavioral advertising." These new obligations must be removed because both the creation of a new opt-out right and the new opt-out right obligations are inconsistent with the statute for the reasons stated above. The California electorate clearly defined the bounds of online advertising regulation under the state's landmark privacy legislation by specifying that consumers may opt out of the "sharing" of personal information for "cross-context behavioral advertising."[45] Both "sharing" and "cross-context behavioral advertising" are defined terms under the statute that are narrower than "behavioral advertising" in the Draft Regulations.[46] Moreover, the statute *expressly* provides that no opt-out right shall apply where the consumer intentionally interacts with the particular business that receives the personal information.[47] In direct conflict with this statutory text, the Draft Regulations would create an opt-out for behavioral advertising that would encompass targeted advertising based on a consumer's activity "*within* the business's own distinctly-branded" websites, apps, and services.[48] The CPPA in fact acknowledges that the

[41] CA AB 1008, 2023–2024 Leg. (Ca. 2024).

[42] The Legislature could have amended the grant of rulemaking authority in Section 1798.185(15) to include AI systems, but notably, chose not to do so.

[43] *Naranjo*, 88 Cal. App. 5th at 945. To the extent that a definition of AI is necessary for the limited purpose of giving meaning to how the agency defines ADMT for its ADMT regulations, the agency should use the definition adopted by California's lawmakers in AB 2885 (Chapter 843, Statutes of 2024) last year and applied throughout all AI legislation enacted last year.

[44] Because the statute's opt-out rights are forward-looking (*e.g.*, ceasing the sale of personal information), Section 7221(n) should be removed, as it appears to relate to personal information that has already been ingested into ADMT.

[45] Cal. Civ. Code § 1798.140(k). *See also* CPRA Ballot Initiative, § 2(I) (noting the statute's focus on advertising tools that "trade vast amounts of personal information" to track and create profiles "across the internet").

[46] *Compare* Cal. Civ. Code §§ 1798.140(k); 1798.140(ah)(1) *with* Draft Regulations § 7001(g).

[47] *Id* § 1798.140(ah)(2)(A).

[48] Draft Regulations § 7001(g) (emphasis added).

term “behavioral advertising” is neither defined nor referenced in the statute.[49] The specificity in the statute leaves no doubt, and no room for the agency to unilaterally expand, the advertising requirements to an entirely new class of advertising activities and protected speech.

In response to concerns raised by some Board Members regarding the overbreadth of the behavioral advertising definition, CPPA staff responded that the ADMT behavioral advertising opt-out right would be analogous to opt-out choices for email and text marketing under other laws, such as the Controlling the Assault of Non-Solicited Pornography and Marketing Act (“CAN-SPAM Act”) and the Telephone Consumer Protection Act (“TCPA”).[50] This analogy is misplaced. Importantly, and unlike the CCPA, those other statutes expressly address consumer choice with respect to the specific manner in which businesses can communicate with the consumer. This is not the case under the Draft Regulations, which do not regulate the communication method, but rather, regulate what information can be used to tailor the content of marketing or advertising materials. Moreover, and as described above, the CCPA does not regulate “behavioral advertising” and instead specifically limits the scope of the advertising opt-out right to “sharing” personal information for “cross-context behavioral advertising.”[51] The comparison to the CAN-SPAM Act and the TCPA raises particular concerns given that the federal CAN-SPAM statute expressly pre-empts state laws attempting to govern the sending of commercial email.[52] Rather than expand the scope of the CCPA (which the agency lacks the authority to do), the CPPA must narrow the scope of its Draft Regulations to eliminate all obligations related to behavioral advertising.

[49] *See* Initial Statement of Reasons at 15 (“The term behavioral advertising by itself is not defined in the CCPA. This definition draws from the CCPA’s definition of ‘cross-context behavioral advertising’ for consistency and clarifies that behavioral advertising means any targeting of advertising to a consumer based on their personal information obtained from the consumer’s activity. Subsection (g)(1) is necessary to clarify that cross-context behavioral advertising is one type of behavioral advertising.”). The Initial Statement of Reasons also provides no reasonable basis demonstrating any significant privacy risk or cognizable harm resulting from consumers’ personal information being processed for behavioral advertising.

[50] *See, e.g.*, November 8, 2024 Board Meeting Transcript, 97-98 (reflecting an analogy comparing the Draft Regulations to other contexts in advertising via email lists and text messages).

[51] Cal. Civ. Code § 1798.120.

[52] *See* 15 U.S.C. § 7707(b). Congress designed this preemption “to ensure that legitimate businesses would not have to guess at the meaning of various state laws when their advertising campaigns ventured into cyberspace.” *Gordon v. Virtumundo, Inc.*, 575 F.3d 1040, 1063 (9th Cir. 2009) (internal quotes and citations omitted).

This narrower scope is not only legally required, but also reflects better public policy. The use of personal information for first-party advertising is consistent with consumer expectations, and consumers benefit from such advertising and marketing. For example, a consumer would not be surprised to receive offers for pet food from the grocery store at which he or she regularly purchases pet products and would benefit from such promotions. Likewise, it would be consistent with a consumer's expectation to receive a discount on a meal from his or her favorite local restaurant or a recommendation for content to watch next based on his or her viewing history. The practical effect of the Draft Regulations would be to treat first-party marketing within the context of the consumer's relationship with the business the same as, for example, the sale of personal information to a data broker. Multiple regulators have recognized that behavioral advertising within the business's own sites, apps, and services does not raise meaningful privacy concerns because such processing is within the context of the consumer's relationship with the business.[53] Moreover, restrictions on first-party marketing raise questions regarding protected speech,[54] and would impose significant practical and operational challenges on businesses subject to the CCPA. Privacy legislation,[55] regulatory guidance,[56] and self-

[53] *See, e.g.*, November 8, 2024 Board Meeting Transcript, 94 (reflecting Board Member Worthe stating that the Draft Regulations reflect "restrictions on advertising to your own customers," which "as presented, . . . seem[] like a pretty strange restriction"); *id.* at 104 (reflecting Board Member Mactaggart stating that stopping first-party ads "was never, and is not the intention of the bill" and that doing so will "at some meaningful level, . . . break the internet," and underscoring that "[p]rivacy laws encourage contextual ads, yet these regulations would undermine that ship").

[54] A business's right to speak is implicated when information it possesses is subject to restraints on the way in which the information might be used or disseminated. *Sorrell v. IMS Health, Inc.*, 564 U.S. 552, 568 (2011). Even assuming, arguendo, that the Draft Regulations' specific targeting of behavioral advertising is not subject to strict scrutiny, courts apply the four-part legal standard articulated in *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n* to determine if government regulation of commercial speech is permissible under the First Amendment. *See* 447 U.S. 557, 566 (1980); *see also Zauderer v. Off. of Disciplinary Council*, 471 U.S., 626, 637 (1985) (holding that "advertising pure and simple . . . falls within th[e] bounds" of commercial speech). The test requires that the regulation is not more extensive than necessary to serve a substantial government interest. A broad opt-out right for ADMT behavioral advertising is more extensive than necessary to achieve that interest. CalChamber questions what substantial government interest could purportedly be found to support the Draft Regulations' restrictions on behavioral advertising when there is no cognizable harm to a consumer (or device) recognized by a U.S. court that arises from using information already and lawfully collected to place an advertisement intended to be seen by that consumer or device.

[55] *See, e.g.*, Colo. Rev. Stat. § 6-1-1303(25) (defining targeted advertising as the display of an ad selected from activities "across nonaffiliated" websites, apps, and services).

[56] *See, e.g.*, Fed. Trade Comm'n, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, 26 (2009) ("[FTC] staff agrees that 'first party' behavioral 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."); *id.* at 27 ("In addition, [FTC] staff agrees that 'first party' collection and use of consumer data may be necessary for a variety of consumer benefits and services."); Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change*, 15-16 (2012) ("The Commission agrees that the first-party collection and use of non-sensitive data . . . creates fewer privacy concerns than practices that involve sensitive data or sharing with third parties.").

regulatory frameworks[57] have thus focused obligations instead on third-party advertising, and the Draft Regulations should be revised to similarly remove behavioral advertising from scope.[58]

D. ADMT Training Requirements Exceed The Scope Of Statutory Authority.

The Draft Regulations exceed the scope of the statute by imposing requirements on ADMT training.[59] Importantly, the statute makes clear that rules should be limited to clarifying existing "access and opt-out rights with respect to a business's _use of_ automated _decision_making technology."[60] Processing to train underlying technologies does not involve making a decision about any particular consumer; instead, it creates or improves the technology more generally. Accordingly, and as explained further in Section I.B above, the Draft Regulations exceed the scope of the statute by extending obligations to ADMT training. ADMT training requirements likewise lack foundation in the statute's direction to establish rules for risk assessments. Although the statute permits the Draft Regulations to require risk assessments in limited circumstances that present a significant privacy risk, insufficient evidence exists to demonstrate that training ADMT meets that criteria.[61] Further, requirements related to ADMT training ignore existing exemptions and other rights in the statutory text (as discussed in more detail in Section II.B) and raise concerns about unconstitutional vagueness by imposing requirements on theoretical or possible uses of technology (expanded further in Section V.C). The Draft Regulations therefore should be revised to focus on concrete and actual uses of ADMT within the statute's direction – the use of ADMT to reach a significant decision without human involvement that results in a significant privacy risk to consumers.

Additionally, as a policy matter, permitting consumers to opt out of the use of their personal information for purposes of ADMT training undermines the development of fair, accurate, and safe ADMT. Regulators and technical experts recommend that companies develop and fine-tune ADMT systems based on training data that resemble the population within which the system will be deployed.[62] Notably, the CPPA acknowledges this point in the Initial

[57] *See, e.g.*, OneTrust, *What is Do Not Track?* (Sept. 10, 2024), https://my.onetrust.com/s/article/UUID-ddce2f5c-d01c-add4-26eb-c105b086217d?language=en_US; *see also* Dig. Advertising All., *Your Ad Choices Gives You Control*, https://youradchoices.com/.

[58] The Draft Regulations' focus on first-party advertising restricts consumer benefits and imposes significant costs on businesses, including through reduced income for online publishers and increased costs for businesses that advertise to new customers. These provisions could have substantial impacts on small businesses seeking to grow through targeted advertising campaigns. *See* Letter from Michael Genest & Brad Williams, Capitol Matrix Consulting, to CalChamber (Nov. 1, 2024), https://advocacy.calchamber.com/wp-content/uploads/2024/11/CMC_comments_on_CCPA_SRIA_11-1.pdf [hereinafter CalChamber SRIA Comment].

[59] *See* November 8, 2024 Board Meeting Transcript, 99 (reflecting Board Member Mactaggart's view that the "scope of these regulations effectively mandates risk assessments for almost any business using software," which will "overwhelm our agency"); *id.* at 100 (providing examples of how the ADMT definition is so broad that it encompasses all software).

[60] Cal. Civ. Code § 1798.185(15).

[61] *See* Cal. Civ. Code § 1798.185(14) (permitting the creation of regulations requiring businesses whose processing of "consumers' personal information presents significant risk to consumers' privacy or security" to submit risk assessments)

[62] *See, e.g.*, Complaint, *In the Matter of DoNotPay*, para. 20 (FTC 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/DoNotPayInc-Complaint.pdf (alleging, among other (continued…)

Statement of Reasons, which identifies concerns with "risks of using skewed data to train AI and ADMT" that contribute to "discrimination and inaccuracies in decisionmaking."[63] In addition to the concerns about statutory overreach outlined above, the practical impact of extending ADMT opt-out rights to training activities compromises efforts to develop valid, accurate, and safe ADMT to the detriment of California consumers. Additionally, any risks to consumers with respect to specific pieces of personal information used by ADMT are adequately addressed through the existing correction right.

E. By Requiring Detailed Explainability, The Draft Regulations Exceed The Statute's Limited Privacy Mandate.[64]

The Draft Regulations impose broad explainability requirements that go far beyond the statute's privacy right of access.[65] Specifically, the Draft Regulations would require detailed disclosures of how the business used an output and how the technology operated, which must include, for example, "key parameters" that affected the output.[66] Indeed, the text of the Draft Regulations go far beyond the scope of the statute to require a "plain language *explanation*" of the technology.[67]

Prescriptive explainability requirements also ignore ongoing discussions of what is possible regarding explainability. Technologists continue to research and do not agree on whether and to what extent ADMT decisions can be provided in a way that offers "meaningful

things that the DoNotPay AI-based product had not been "trained on a comprehensive and current corpus" of representative data); NATIONAL INST. STANDARDS AND TECH., AI RISK MANAGEMENT FRAMEWORK PLAYBOOK, 76, https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook (suggesting that entities ask over time whether the training data set remains representative of the operational environment); NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, FOSTERING RESPONSIBLE COMPUTING RESEARCH: FOUNDATIONS AND PRACTICES, 69 (National Academies Press, 2022) (noting that developers must engage in "purposeful sampling" to ensure "the representativeness of the population that generated the [training] data[set]" and that, "[f]or data sets to . . . provide a foundation for . . . deployed systems, they need to be intentionally designed and their sample population understood"); The EU AI Act, Regulation (EU) 2024/1689, recital 67 ("high-quality data and access to high-quality data plays a vital role in providing structure and in ensuring the performance of many AI systems . . . Data sets for training, validation and testing, including the labels should be relevant, *sufficiently representative*, and to the best extent possible free of errors and complete in view of the intended purpose of the system") (emphasis added). UK Dept. for Science, Innovation, & Technology, *Report: Enabling responsible access to demographic data to make AI systems fairer* (Jun. 14, 2023) ("[i]naccurate or misrepresentative data can be ineffective in identifying bias or even exacerbate bias").

[63] Initial Statement of Reasons at 8 ("Adhering to these proposed requirements will help businesses to identify and mitigate the risks of using skewed data to train AI and ADMT and will thus help businesses identify and mitigate the risks of discrimination and inaccuracies in decisionmaking. Taken together, these proposed regulations will reduce incidences of discrimination and, in turn, inequality.")

[64] Additionally, the Draft Regulations propose that businesses should report metrics on how many specific ADMT access requests they receive, but access request metrics are already separately covered in Section 7012.

[65] Cal. Civ. Code § 1798.185(15).

[66] Draft Regulations § 7222(b).

[67] *Id.* (emphasis added).

information" to individual consumers.[68] The CPPA should wait for this research to be further developed before imposing legal obligations that may be impractical based on the current state of science.

The new requirement for adverse significant decision notices exceeds the CPPA's rulemaking authority. Importantly, the Draft Regulations require a business to provide an adverse significant decision notice, even where a consumer did not request details from the business.[69] The Draft Regulations acknowledge this by referring to the "[a]dditional notice" required in addition to ADMT access right responses. This bears no relationship to the statute's "right to request" access to personal information.[70] Additionally, the content of the adverse significant decision notices focuses on notifying the consumer that the business reached an adverse significant decision,[71] instead of access to the consumer's personal information. Because the CPPA is constrained to issuing regulations implementing only the specific access right authorized in the statute, the CPPA cannot attempt to create an entirely new CCPA right.

Moreover, the CPPA must remove references to and requirements for the pre-use notice to bring the Draft Regulations in line with the statute. The CCPA's authorization for the agency to issue rules on how businesses must respond to access requests does not permit the agency to go beyond such reactive responses to require proactive public disclosures detailing the use of ADMT. If the California electorate intended to permit the CPPA to issue rules on pre-use notices for ADMT, it would have been clear on this point. Notably, the statute expressly states when prior notice is required at or before collection, but the statute does not authorize the CPPA to amend the notice-at-collection rules to specifically address ADMT or authorize other ADMT pre-use notices. Consequently, to avoid requirements that "alter or amend the statute or enlarge or impair its scope,"[72] all references to the pre-use notice should be removed from the Draft Regulations.

F. The Draft Regulations Exceed The Authority Granted In the Statute For Cybersecurity Audits.

The Draft Regulations do not limit cybersecurity audits to "significant risks" to consumer security, as required by the statute.[73] Accordingly, the CPPA must significantly revise the Draft Regulations.

[68] Cal. Civ. Code § 1798.185(15) (requiring regulations on access that "include meaningful information about the logic involved" in ADMT); *see* Cynthia Rudin et al., *Interpretable Machine Learning: Fundamental Principles and 10 Grand Challenges*, ARXIV (July 10, 2021) https://arxiv.org/abs/2103.11251 (describing technical challenges for interpreting machine learning-based systems); Hofit Wasserman-Rozen, Ran Gilad-Bachrach, & Niva Elkin-Koren, *Lost in Translation: The Limits of Explainability in AI*, 42 CARDOZO ARTS & ENT. 391, 432 (2024) (noting that "sometimes models are so complex that they simply cannot be explained in a meaningful way"); Gabriel Nicholas, *Explaining Algorithmic Decisions*, 4 GEO. L. TECH. REV. 711, 727 (2020) (noting that there are no "intrinsic explanations" for certain machine learning algorithms).

[69] *See* Draft Regulations § 7222(k).

[70] Cal. Civ. Code § 1798.110(a).

[71] Draft Regulations § 7222(k).

[72] *Naranjo*, 88 Cal. App. 5th at 945.

[73] Cal. Civ. Code § 1798.185(a)(14) (empowering the CPPA to issue regulations requiring businesses to conduct cybersecurity audits when "processing of consumers' personal information *presents significant risk* to consumers' privacy or security") (emphasis added).

- The Draft Regulations should be revised to require cybersecurity audits where a business processes a significant amount of sensitive personal information in a way that presents a risk of harm to consumers. The Draft Regulations incorrectly require cybersecurity audits if the business meets certain revenue and processing thresholds. This focus on the size of the business and volume of data[74] ignores the statute's express directive that factors to be considered when determining if audits are required "shall include" the "size and complexity of the business *and* the nature and scope of processing activities."[75] The Initial Statement of Reasons states that revenue may "logically be a proxy for the complexity of a business," and revenue is a "proxy" for the business's size.[76] The CPPA cannot substitute the language approved by California voters with its own preferred language through the use of proxies. If the drafters intended for the CPPA to consider revenue and processing thresholds, it would have incorporated these standards in the statutory text, as it did in the definition of "business."[77] Amendments to the Draft Regulations should instead require cybersecurity audits where a business processes a significant volume of sensitive personal information and the nature of the business's processing presents a significant risk of harm to consumers if the business were to be impacted by a cybersecurity incident.[78]

- The CPPA does not have authority to rewrite California law, which is clear about the scope of security incidents. Thus, the Draft Regulations should incorporate the definition of security incident that already exists in the state's data breach notification statute and require the provision of prior security incident notifications only when the business was required to notify a California regulator. Relatedly, the Draft Regulations would require businesses to include in the audit all notifications provided to any domestic or global regulator regarding a security incident, regardless of whether it affected the personal information of California consumers.[79] CalChamber urges the CPPA to bring the Draft Regulations in line with its interests as a California regulator.

- In its granular list of activities that must be considered for cybersecurity audits, the Draft Regulations exceed the authority granted in the statute for cybersecurity audits by creating broad cybersecurity governance requirements, such as password protocols, cybersecurity training, and penetration testing, many of which will grow stale as best practices evolve.

[74] The Initial Statement of Reasons demonstrates that alternatives took a similar approach by tying cybersecurity audits to various revenue thresholds. *See* Initial Statement of Reasons, 121.

[75] Cal. Civ. Code § 1798.185(14)(a) (emphasis added).

[76] Initial Statement of Reasons, 42.

[77] Cal. Civ. Code § 1798.140(d) (defining business according to revenue and processing thresholds).

[78] The CPPA should take note that California law already establishes clearly when personal information rises to a level of sensitivity such that a cybersecurity incident could present harm to consumers. *Id.* § 1798.82 (defining cybersecurity incidents that should be reported to impacted consumers). In short, the Draft Regulations' apparent and unspoken assumption that all personal information processing presents harm to consumers is directly at odds with the statute's own recognition that the nature and scope "shall" be taken into account – some processing will, and some won't, rise to this level of potential harm worthy of auditing.

[79] Cal. Civ. Code § 7123(e).

- The Draft Regulations' sweeping prescriptive list of "components" contradicts applicable California law.[80] The Draft Regulations, contrary to any other cybersecurity regulation or framework and the basic foundations of cybersecurity best practices, offer no flexibility to focus on components that are appropriate for the processing activity, underlying data, or business's environment. Instead, the Draft Regulations only offer that compensating controls "provide at least equivalent security."[81] In contrast, California law and industry best practices incorporate a risk-based approach based on reasonableness – a business "shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[82] Additionally, and as recognized in the Initial Statement of Reasons,[83] existing security standards and frameworks already exist, so the Draft Regulations need not create a new set of components to be evaluated. Indeed, although the Initial Statement of Reasons references other security standards and frameworks, it does not provide a rationale to support why these expert-driven, multi-stakeholder, and regularly updated standards and frameworks are not sufficient to address significant risks to consumer security. Consequently, the Draft Regulations should permit the business flexibility to address topics most appropriate for the processing activity, including by reference to existing standards and frameworks.

- The Draft Regulations should be revised to align with the statute's direction to consider the "size and complexity of the business" and the "nature and scope of processing activities"[84] by requiring that a business, after completing its first cybersecurity audit, conduct an intervening risk-based audit annually and perform a full audit every three years. The statute permits the agency to take such an approach, as it directs the agency to "defin[e] the scope of the audit."[85] In operation, this cadence would promote security and further the goals of the statute, as it would avoid diverting cybersecurity resources away from security operations towards compliance operations.[86] In addition, it would align with other widely-accepted and used security frameworks, such as, for example, the National Institute of Standards and Technology's ("NIST") Cybersecurity Framework and ISO 27000.

[80] *See, e.g.*, Draft Regulations § 7123(b) (requiring that the business examine "each of" the following components of its cybersecurity program, and if the component is not implemented, the audit must explain why). Furthermore, the Draft Regulations' proposed content for the cybersecurity audit is inconsistent in many sections. For example, the business must evaluate password authentication, but must also conduct an evaluation of Zero Trust Architecture, which reflects a passwordless authentication protocol. *See id.* at §§ 7123(b)(2)(A)(ii); 7123(b)(2)(C).

[81] Draft Regulations § 7123(b)(2).

[82] Cal. Civ. Code § 1798.81.5(b).

[83] Initial Statement of Reasons at 51-52. Although the CPPA states in the Initial Statement of Reasons that the list of criteria for cybersecurity audits was developed using the Center for Internet Security Critical Security Controls, it does not explain why the 18 best practices from this group are more instructive than the analogous provisions in the NIST Cybersecurity Framework 2.0, ISO, and related frameworks or standards.

[84] Cal. Civ. Code § 1798.185(14)(A).

[85] *Id.*

[86] *Id.*

G. The Prescriptive Risk Assessment Requirements In The Draft Regulations Are Inconsistent With The Statute.

The Draft Regulations should be revised to conform the risk assessment content and procedures to the underlying statute. For example:

- The Draft Regulations take a one-size-fits-all approach to risk assessments by requiring a number of granular topics to be addressed, regardless of the processing activity, whether those elements are relevant, or even if the topic bears a relationship to the agency's authority as a privacy regulator. For example, every risk assessment must include the retention period for personal information and the criteria used to determine the retention period, as well as the technology used for the processing.[87] The Draft Regulations also suggest that risk assessments should consider, for example, "economic harms" that ADMT may cause, such as higher prices or lower wages, which are unrelated to the agency's mandate as a privacy regulator.[88] Consequently, the Draft Regulations depart from the purposes of risk assessments – to identify and address identified significant privacy risks – in favor of a paperwork exercise. CalChamber urges the CPPA to revise the Draft Regulations to permit businesses the flexibility to determine and address those topics that are relevant for the processing activity in completing risk assessments.[89]

- CalChamber appreciates the value in updating risk assessments following a material change, provided that the scope of "material change" is amended to align with the longstanding definition of the term. However, as proposed, the Draft Regulations would require "immediate[]" updates to risk assessments.[90] Therefore, good faith efforts to comply could result in hurried updates that do not address significant risks to privacy intended by the statute. Furthermore, the Draft Regulations define "material" as any change that diminishes the benefits, creates new negative impacts, or diminishes the effectiveness of safeguards, regardless of how minor those changes are in practice.[91] As drafted, the Draft Regulations define "material" in a way that would include an update beneficial to the consumer, which, in practice, would delay benefits to the consumer until documentation could be finalized. Rather, the Draft Regulations should adopt the FTC's

[87] Draft Regulations §§ 7152(a)(3)(B), (G).

[88] Draft Regulations § 7152(a)(5)(F).

[89] This approach would promote interoperability with other privacy frameworks. For example, the Colorado Privacy Act Rules permits controllers to consider the factors that are relevant to the processing activity. The Rules 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. Colorado Privacy Act Rule 8.02(C).

[90] Draft Regulations § 7155(a)(3).

[91] *Id.*

definition of materiality – *i.e.,* whether it would affect a consumer's decision to interact with the product or service.[92]

- The Draft Regulations should be revised to require submission upon request from the CPPA to align the requirement to the statute's focus on "significant risk" to privacy. Furthermore, the Draft Regulations should recognize that a business can withhold from submission trade secret and privileged or business sensitive information in a risk assessment or otherwise set forth protections to prevent the public disclosure of such information and the waiver of related privileges.[93]

II. The Draft Regulations Inappropriately Ignore Existing Rights And Statutory Exceptions.

The CPPA must amend the Draft Regulations to clarify the existing rights and exemptions in the statutory text, including with respect to opt-out rights, the ADMT access right, ADMT training, and extensive profiling.

A. The Draft Regulations Create Overlapping, Confusing Opt-Out Rights.

The Draft Regulations propose new opt-out rights that appear to overlap with existing statutory rights and likely will confuse consumers about their privacy choices. Specifically, the Draft Regulations provide consumers with a new right to opt out of ADMT for behavioral advertising, including cross-context behavioral advertising. However, consumers already have the right to opt out of sharing for cross-context behavioral advertising and the sale of personal information. The Draft Regulations appear to suggest that these choices must be distinct for consumers,[94] but this risks creating consumer confusion. It also creates compliance uncertainty where a consumer has opted out of ADMT for behavioral advertising but has not opted out of sharing for cross-context behavioral advertising. These contradictions underscore the CPPA's overreach of its authority in addressing behavioral advertising opt-outs.[95] To address this concern, the CPPA should remove all requirements for behavioral advertising.

Relatedly, the Draft Regulations create confusing, overlapping requirements for sensitive personal information that frustrate the aims of the statute to provide consumers with "meaningful options" for how their sensitive personal information is used.[96] Specifically, the Draft Regulations would require an opt-out right for training uses of ADMT "capable of" being used for physical or biological identification or profiling,[97] which overlaps with the existing statutory right for consumers to limit the use and disclosure of their sensitive personal information.[98] The statutory text is clear that biometric data reflects physiological, biological, or

[92] *See* Fed. Trade Comm'n, Policy Statement on Deception, *app'd to Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984).

[93] *See* Cal. Civ. Code § 1798.185(a)(3) (permitting the CPPA to establish any exceptions necessary to comply with state or federal law, "including, but not limited to, those relating to trade secrets and intellectual property rights").

[94] Draft Regulations § 7221(c).

[95] *See* Section I.C.

[96] CPRA Ballot Initiative, § 3(A)(2).

[97] Draft Regulations § 7200(a)(3)(C).

[98] Cal. Civ. Code § 1798.121; Draft Regulations § 7027.

behavioral characteristics to "establish individual identity,"[99] which shares substantial overlap with the "physical or biological identification or profiling" definition, *i.e.*, "identifying or profiling a consumer using information that depicts or describes their physical or biological characteristics, or measurements of or relating to their body."[100] Where a business processes biometric data, it must allow consumers the choice to limit the business's use and disclosure of that sensitive personal information, which functionally serves as an opt-out.[101] In effect, this creates overlapping, confusing choices for consumers to untangle and underscores how requirements related to physical or biological identification or profiling exceed the authority permitted in the statutory text.[102]

The Draft Regulations should make clear that a business may provide more granular ADMT opt-out options for consumers to limit how their personal information is processed by ADMT for certain uses. This approach aligns with the requirements in the existing CCPA Regulations for deletion options, which permit a business to present a consumer with the choice to delete select portions of their personal information.[103] A single opt-out choice for ADMT incorrectly presumes that all ADMT uses subject to the Draft Regulations lack benefits to consumers. Furthermore, the single opt-out structure does not advance the interests of California consumers, who might want to opt out of some, but not all, uses of ADMT.

B. The Draft Regulations On ADMT Overlook Statutory Exemptions.

The CPPA must revise the Draft Regulations to clarify that all statutorily mandated exemptions are incorporated to avoid impermissible inconsistencies between the Draft Regulations and the statutory text. Importantly, the agency cannot cherry-pick which broad statutory exemptions it would like to apply in different scenarios. Consistent with the other exemptions under the statute, such as those for certain healthcare entities and commercial credit data, the Draft Regulations should be revised to address the following:

- The Draft Regulations create a new concept of security, fraud prevention, and safety uses of ADMT.[104] A business need not provide the ADMT opt-out right if it uses ADMT that is "necessary to achieve" and "used solely" for these purposes, but the Draft Regulations leave other obligations in place, such as the access right and pre-use notice requirement. The specified security, fraud prevention, and safety exemption in the Draft Regulations overlaps with the existing statutorily-created exemptions, such as exemptions to exercise or defend legal claims, to comply with the law or legal process, to protect the rights of others, and where a natural person is at risk of death or serious physical injury.[105] Of course, the agency has no authority to amend or impair the statute, and any attempt to do so would be unlawful. Accordingly, the agency should clarify that all the statutory

[99] Cal. Civ. Code § 1798.140(c).

[100] Draft Regulations § 7001(gg).

[101] The CCPA's right to limit the use and disclosure of sensitive personal information is subject to certain exceptions, including where the processing activity is one outlined in Draft Regulations § 7027(m).

[102] *See* Section I.A.

[103] Draft Regulations § 7022(h).

[104] Draft Regulations § 7221(b) (outlining specific activities that qualify for the security, fraud prevention, and safety exemption, such as to ensure the physical safety of natural persons).

[105] *See, e.g.*, Cal. Civ. Code §§ 1798.145(a)(1)(A)-(B), (D)-(E).

exemptions apply to the ADMT Draft Regulations and nothing in the regulations limits or amends the blanket exemptions contained in the statute.[106]

- The proposed ADMT training requirements overlook explicit exemptions in the statute, such as the explicit recognition in the statute that "publicly available information" does not constitute personal information[107] and that businesses are not required to relink information maintained separately in the ordinary course of business.[108] Importantly, the Draft Regulations do not reflect the technical realities of how ADMT training works in practice. For example, much of the data used for ADMT training is sourced from datasets that are publicly available, and therefore, out of the scope of the CPPA's authority. Additionally, the Draft Regulations should recognize the statutory language that deidentified and aggregated data used for ADMT training is not subject to requirements.[109] The Draft Regulations should focus on requirements that will have a meaningful impact on consumer privacy, rather than empty obligations that ignore existing rights and exemptions in the statutory text, by removing requirements related to ADMT training.

- The Draft Regulations' ADMT access provisions conflict with the statutory text. For example, the Draft Regulations would require granular, specific disclosures about how ADMT systems operate, which largely implicate business-sensitive and other intellectual property-protected information. In doing so, the Draft Regulations ignore the explicit statutory exemption for trade secrets.[110] The Draft Regulations should extend the exemption for commercial credit data to ADMT access provisions, as ADMT access requirements in the commercial credit context do not provide meaningful information to individual consumers. Additionally, the disclosure of information related to the outputs generated by ADMT and how those outputs influence decisions conflicts with other statutory exemptions, such as the recognition that the statute does not require a business to process personal information that would limit the business's ability to exercise or defend legal claims or comply with the law.[111]

Notwithstanding our contention that ADMT training requirements impermissibly enlarge the statute, CalChamber urges the CPPA to recognize the benefit to California consumers of research and testing of ADMT and ensure the exclusion of those uses from prescriptive regulations. Specifically, the Draft Regulations should not hamper other internal

[106] Robust fraud and safety exemptions for ADMT use help keep consumers safe, *see, e.g.*, Edward McNicholas, et al., *AI's Impacts on Cybersecurity & Legal Requirements*, Bloomberg L. (Jan. 2024), https://www.bloomberglaw.com/external/document/XFFFPLEG000000/incident-breach-management-professional-perspective-ai-s-impacts (AI tools to identify patterns of threat actor activity and cybersecurity red team exercises); Org. Econ. Coop. & Dev., *Generative Artificial Intelligence in Finance,* 15 (2023) (AI to combat money laundering), and promote interoperability, *see, e.g.*, Colo. Rev. Stat. § 6-1-1304(3)(a)(X); Colo. Rev. Stat. § 6-1-1701(9)(b)(II)(A) (exempting anti-fraud technology that does not include facial recognition technology).

[107] Cal. Civ. Code § 1798.140(v)(2). To the extent that publicly available places is retained in the Draft Regulations, the CPPA should clarify that publicly available places excludes the internet, similar to the EU AI Act, by specifically noting that it includes a physical place open to the public.

[108] *Id.* at § 1798.145(j)(1).

[109] *Id.* at § 1798.140(v)(3).

[110] *Id.* at § 1798.100(f).

[111] *See, e.g., id.* at §§ 1798.145(a)(1)(A)-(B), (D)-(E).

testing activities by the business that redound to the benefit of consumers, such as self-testing to identify, mitigate, or prevent discrimination or otherwise ensure compliance with the law.[112] Such recognition would also create parity between the ADMT opt-out right and the requirement to provide consumers with a right to limit the use and disclosure of their sensitive personal information. In the context of the sensitive personal information right, a business need not post a Notice of Right to Limit if it processes sensitive personal information "[t]o verify or maintain the quality or safety of" or "improve, upgrade, or enhance" a service or device that is "owned, manufactured by, manufactured for, or controlled by the business."[113] Accordingly, any ADMT opt-out right or related obligation should not apply when ADMT is used for such purposes. As further support, the value of internal research and testing has been widely recognized by the NIST AI Risk Management Framework, the Colorado AI Act, and other regulators.[114]

C. The Draft Regulations Impose Requirements On Extensive Profiling That Are In Tension With Statutory Rights And Exemptions.

The requirements with respect to "extensive profiling" overlap with other obligations.

The Draft Regulations define extensive profiling to include profiling a consumer through systemic observation in his or her role as a student or worker. Importantly, the proposed requirements for "extensive profiling" of students and workers are already addressed through the opt-out right, access right, and risk assessment requirements for the use of ADMT to reach "significant decisions," which the Draft Regulations broadly define to include hiring, promotion and demotion, and termination decisions.[115] Additionally, the scope of the profiling definition underscores the redundancy of the extensive profiling concept. Because the statute defines profiling as automated processing "to evaluate certain personal aspects concerning that natural person," requirements for significant decisions already encompass those activities that the Draft Regulations describe as "extensive profiling."[116]

Extensive profiling also includes profiling a consumer through systematic observation of a publicly accessible place, which ignores the CCPA's explicit exemption for publicly available information. In exempting "information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience,"[117] the statute makes plain that information and activities that the consumer makes available to the public generally do not present heightened risks to consumer privacy, and are thus outside of the scope of the statute. Moreover, a business need not reidentify or relink information that in the ordinary course is not maintained in a manner that would be considered

[112] This exception is recognized in other AI frameworks, such as the Colorado AI Act, which states that algorithmic discrimination specifically excludes efforts to conduct "self-testing to identify, mitigate, or prevent discrimination or otherwise ensure compliance with state and federal law." Colo. Rev. Stat. § 6-1-1701(1)(b)(I)(A).

[113] Draft Regulations § 7027(m)(7).

[114] *See, e.g.*, Colo. Rev. Stat. § 6-1-1705(1)(h) (exempting from the statute internal research); Va. H.B. 2094, § 59.1-607 (carving out of the definition of AI system models used for research activities before the model is made available to consumers).

[115] Draft Regulations § 7150(b)(3)(A)(ii).

[116] Cal. Civ. Code § 1798.140(z).

[117] *Id.* at § 1798.140(v)(2)(B)(i)(III).

personal information.[118] As a practical matter, the expansive scope of the public profiling concept will capture a number of everyday activities, such as identifying where delivery vehicles or IT assets are located. Further, the Draft Regulations should limit ADMT requirements to significant decisions to ensure that the Draft Regulations do not restrict California consumers from accessing services they choose to engage with, such as tools to map fitness routes or traffic. To the extent that the extensive profiling in public places concept is intended to address mass facial recognition, those concerns are already addressed separately through the existing requirements related to the processing of biometric data.[119]

The Draft Regulations improperly stretch the "extensive profiling" concept to include use of first-party data already lawfully in a business's possession to determine whether a consumer would find protected commercial speech useful or interesting—*i.e.*, "behavioral advertising." The statute, however, *expressly excludes* from its scope personal information arising from activities with "the business, distinctly branded internet website, application, or service with which the consumer intentionally interacts."[120]

Furthermore, through the "extensive profiling" concept, the CPPA attempts to pursue a course of action that the Legislature has already rejected. The California Legislature previously considered, and declined to advance, employee privacy legislation that would have addressed ADMT.[121] Notably, the proposed Workplace Technology Accountability Act ("WTAA") would have required employers that use ADMT to make or assist in an employment-related decision to complete an "Algorithmic Impact Assessment" prior to using the system, which would have involved comparing the risks and benefits of using the ADMT. The WTAA would also have granted employees the right to access whether their data was being used as an input in ADMT or generated as an output of ADMT, required employers to provide notice prior to using ADMT, and prohibited employers from using ADMT to make certain predictions about an employee's behavior (among other prohibitions). The WTAA, which the Legislature declined to act upon in the 2021-2022 Regular Session, has never been reintroduced and would have chilled innovation, made workplaces less safe, and penalized small businesses for even good faith mistakes.[122] Accordingly, the CPPA acts beyond the scope of its authority and acts where the Legislature made a decision not to implement such requirements for California businesses.

III. CalChamber Encourages the CPPA To Harmonize The Draft Regulations With Other Legal Frameworks And Standards.

The Draft Regulations must promote interoperability with other privacy frameworks and well-established standards.[123] Harmonization benefits consumers' privacy and security by helping consumers understand and exercise their privacy rights and fostering a consistent

[118] *Id.* at § 1798.145(j)(1).

[119] If the CPPA does not remove the public profiling exception, which CalChamber urges it to do, the systemic observation language should make clear that it does not encompass services that consumers specifically chose to engage with, such as fitness trackers, interactive maps, and location trackers.

[120] Cal. Civ. Code § 1798.140(k) (defining cross-context behavioral advertising).

[121] CA AB 1651, 2021–2022 Leg. (Ca. 2022).

[122] *See* Ronak Daylami, *CalChamber Tags AB 1651 as a Job Killer* (Apr. 26, 2022), https://advocacy.calchamber.com/2022/04/26/calchamber-tags-ab-1651-as-a-job-killer/.

[123] *See* CPRA Ballot Initiative, § 3(C)(8) ("To the extent it advances consumer privacy and business compliance, the law should be compatible with privacy laws in other jurisdictions.").

compliance environment. Specifically, CalChamber requests that the CPPA address the following:

- In addition to contravening the statute, the broad definition of ADMT is out of step with the approach taken by other state privacy laws, international standards,[124] and the CPPA's own role as a privacy regulator. Even if the agency ignores the various limitations in the statute, the ADMT definition should be revised to encompass only those technologies that (1) involve processing of personal information in a way that presents a significant privacy risk, (2) are not subject to human involvement, and (3) reach a significant decision to target obligations to activities most likely to present a heightened risk of harm to consumers, as commonly recognized by other U.S. privacy frameworks.[125]

- The Draft Regulations propose an overly broad definition of "security incident" that deviates from federal standards, such as those outlined in the Cyber Incident Reporting for Critical Infrastructure Act of 2022,[126] Federal Information Security Modernization Act,[127] and the Presidential Policy Directive on Cyber Incident Coordination.[128] The Draft Regulations should instead align with the definition already created under California law in the state's breach notification statute, which uses the term "breach of security of the system."[129] Alternately, the CPPA can consider focusing on unauthorized access or compromise of critical systems and data that impact personal information.[130]

- Even if the agency ignores its other statutory mandates, ADMT opt-outs should align with U.S. state privacy statutes and global frameworks that limit opt-outs to ADMT used in furtherance of decisions with legal or similarly significant effects – specifically, significant decisions made without human involvement and that present a significant risk to consumer privacy.[131] Furthermore, the scope of significant decisions should promote interoperability with other privacy frameworks, including by removing references to "access to" certain opportunities.[132] Such amendments would help address two current flaws in the Draft Regulations – the overly broad scope of significant decisions as compared to other state privacy frameworks and the CPPA's overreach into

[124] *See, e.g.*, Colorado Privacy Act Rule 9.04(B); Conn. Gen. Stat. § 4(A)(5)(C); EU General Data Protection Regulation, Regulation (EU) 2016/679, art. 22.

[125] *See, e.g.*, November 8, 2024 Board Meeting Transcript, 106 (reflecting Board Member Mactaggart's feedback that "[i]f a human is materially involved in a decision, no opt-out should be required").

[126] *See* 6 U.S.C. § 681(5).

[127] *See* 44 U.S.C. § 3541, *et seq.*

[128] *See* Presidential Policy Directive-41 (PPD-41): U.S. Cyber Incident Coordination; 44 U.S.C. § 3552(b)(2).

[129] Cal. Civ. Code § 1798.82 (defining breach of security of the system to mean "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business").

[130] *See id.*

[131] *See, e.g.*, Conn. Gen. Stat. § 42-518(a)(5)(C); Del. Code tit. 6 § 12D-104(a)(6)(c). Importantly, no other U.S. state privacy statute provides an opt-out right or defines decisions with legal or similarly significant effect to encompass ADMT training.

[132] *See* Draft Regulations §§ 7150(b)(3)(A); 7200(a)(1).

areas not germane to its role as a privacy regulator. This also avoids establishing a confusing and overbroad choice regime that goes far beyond appropriately scoped ADMT provisions in other states.

- The threshold activities that require risk assessments far exceed those required by other U.S. privacy statutes and do not focus on the processing of personal information in a manner that presents a significant risk to consumers' privacy.[133] The CPPA should harmonize risk assessment thresholds to those activities where there is settled consensus that such assessments should be performed. These include: (1) the sale of personal information, (2) the sharing of personal information for targeted advertising, (3) the processing of large amounts of sensitive personal information,[134] and (4) significant decisions that pose significant privacy risks.[135]

- The Draft Regulations specify a narrow exemption to the ADMT opt-out for security, fraud prevention, and safety that is out of step with other U.S. privacy statutes, which recognize a broader exemption for fraud, security, and consumer safety.[136]

- Multiple, sometimes overlapping, notice requirements diverge from other privacy statutes and contribute to consumer confusion. Where other laws require a single, easy-to-locate privacy policy,[137] the Draft Regulations propose a separate pre-use notice requirement that would be presented on top of the information in the mandated privacy policy and notice at collection. CalChamber urges the CPPA to remove the prescriptive pre-use notice requirement that is out of step with notice requirements under other privacy statutes, creates ambiguity for businesses, and runs counter to the goal of providing meaningful transparency to consumers about the processing of their personal information by contributing to notice fatigue.

- The Draft Regulations propose numerous distinct topics that "must" be included in risk assessments, which should instead mirror the approach taken by other statutes and

[133] *See, e.g.*, Conn. Gen. Stat. § 42-522(a); Mont. Code § 30-14-2814(1); Tenn. Code Ann. § 47-18-3206(a); Va. Code Ann. § 59.1-580(A); *see also* Initial Statement of Reasons, 58 ("Fifteen other states generally require a risk assessment prior to selling personal information or sharing that information for targeted advertising.").

[134] The Draft Regulations should incorporate a threshold volume for sensitive personal information processing that triggers requirements, as the definition of sensitive personal information in the CCPA is broader than other U.S. privacy frameworks, as it includes, for example, account credentials. *See* Cal. Civ. Code § 1798.140(ae).

[135] This revision would also be supported by the statute. *See* Cal. Civ. Code § 1798.185(14) (permitting the creation of regulations requiring a business whose processing of "consumers' personal information presents significant risk to consumers' privacy" to complete a privacy risk assessment).

[136] *See, e.g.*, Colo. Rev. Stat. § 6-1-1304(3)(a)(X); Conn. Gen. Stat. § 42-524(a)(9); Fla. Stat. § 501.716(1)(f); Ind. Code § 24-15-8-1(a)(7); Iowa Code § 715D.7(1)(g); Mont. Code § 30-14-2816(1)(i); Tex. Bus. & Com. Code § 541.201(a)(6); Va. Code Ann. § 59.1-582(A)(7).

[137] *See, e.g.*, Conn. Gen. Stat § 42-520(c); Utah Code § 13-61-302(1)(a); Va. Code Ann. § 59.1-578(C).

permit a business flexibility to address topics appropriate for the nature and context of processing.[138]

- The Draft Regulations transform the types of risk assessments required under U.S. privacy statutes into an entirely different exercise that is more akin to a GDPR-like privacy impact assessment. Specifically, the Draft Regulations prohibit the processing activity if the risks to consumers outweigh the benefits, suggesting that the assessment must be concluded before the processing activity begins.[139] Importantly, privacy impact assessments are typically exercises with respect to a particular project or product, whereas a risk assessment is intended to cover overall processing at a category level. Accordingly, mandating granular assessments of 9 topics and 22 sub-topics for a privacy risk assessment is inappropriate. Additionally, this paperwork exercise requirement will divert resources towards compliance functions that will not benefit California consumers.

- The Draft Regulations should recognize a meaningful safe harbor for risk assessments and cybersecurity audits. The limited risk assessment safe harbor requires businesses to supplement existing assessments, which, in practice, renders the safe harbor an empty provision that departs from U.S. privacy statutes.[140] Relatedly, the Draft Regulations should recognize a safe harbor for cybersecurity audits undertaken in accordance with internationally recognized standards or frameworks, which would comport with best practices[141] and other existing cybersecurity laws, including state laws that provide safe harbors for entities that adopt certain cybersecurity standards.[142]

- The Draft Regulations, which require annual submission, depart from U.S. statutes and international frameworks that require submission of a risk assessment only upon request from the regulator.[143] Accordingly, the Draft Regulations should interpret "periodic

[138] *See, e.g.*, Conn. Gen. Stat. § 42-522(b) ("Data protection assessments. . . shall identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks."); Mont. Code § 30-14-2814(2)(a) (substantially same); Tenn. Code Ann. § 47-18-3206(b) (substantially same).

[139] Draft Regulations § 7154(a).

[140] *See, e.g.*, Colorado Privacy Act Regulations Rule 8.02; Conn. Gen. Stat. § 42-522(e); Mont. Code § 30-14-2814(5); Tenn. Code Ann. § 47-18-3206(e); Tex. Bus. & Comm. Code § 541.105(e).

[141] *See* ISO/IEC 27000; NIST Cybersecurity Framework; 23 NYCRR § 500.09, (New York Department of Financial Services cyber assessment requirement); DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (2022); *see also* NIST Cybersecurity Framework 1 (2014) (highlighting the importance of streamlining cybersecurity frameworks to "address and manage cybersecurity risk in a cost-effective way . . . without placing additional regulatory requirements on businesses").

[142] *See, e.g.*, W.V. Ann. Code §31A-8H-1 (providing an affirmative defense to a tort claim for entities that implement reasonable information security controls); Utah Code Ann. § 78B-4-702 (providing an affirmative defense for any claims brought under Utah law or in Utah courts and that alleges that a person failed to implement a reasonable security program); Conn. Stat. Ann. § 42-901 (providing a safe harbor against punitive damages for entities that maintain a cybersecurity program).

[143] *See, e.g.*, Colorado Privacy Act Rule 8.06; GDPR Art. 58(1)(a). Notably, even EU regulators have expressed that there must be discretion with respect to the reporting of processing activities to regulators.
(continued…)

submissions" to mean the submission in the context of an investigation and with important protections for confidential and sensitive business information and privileges. Relatedly, the cybersecurity audit reporting requirements are not only out-of-step with other state laws, but also conflict with widely accepted cybersecurity frameworks, standards, and controls, such as those set forth by NIST and ISO.

- Unlike the approaches taken by other U.S. privacy statutes,[144] the Draft Regulations omit detail as to whether submitting the risk assessment materials (either in abridged form, which is required as a matter of course, or in an unabridged format upon request) weakens or waives claims of attorney-client privilege or work product protection. Such revisions would also reflect an approach already endorsed by the California Legislature.[145]

- The Draft Regulations impose burdensome and prescriptive cybersecurity reporting and audit requirements that run counter to federal frameworks, including the White House's National Cybersecurity Strategy[146] and Office of the National Cyber Director,[147] and are not required by other state privacy frameworks.[148] CalChamber urges the CPPA to align the Draft Regulations with global and federal cybersecurity standards and frameworks, which foster a balanced, risk-based approach to cybersecurity governance.

- The Draft Regulations impose board of director oversight and reporting on a broad scope of processing activities that significantly depart from other cybersecurity frameworks and the appropriate role of directors. Although some frameworks, like those established by the New York Department of Financial Services and the Security and Exchange Commission, address board oversight of cybersecurity, this oversight never requires that

See GDPR Recital 89 ("Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes.").

[144] *See* Colo. Rev. Stat. § 6-1-1309(4); Va. Code Ann. § 59.1-580(D).

[145] The California Age Appropriate Design Code contemplates that a business may conduct data protection impact assessments under attorney-client privilege, and businesses are not required to provide state authorities with these assessments unless specifically requested. *See* Cal. Civ. Code § 1798.99.31(a)(4).

[146] *See* The White House, National Cybersecurity Strategy (2023) (emphasizing harmonization to "minimize the cost and burden of compliance, enabling organizations to invest resources in building resilience and defending their systems and assets"). Additionally, Congress has consistently reiterated the importance of harmonizing cybersecurity regulations, emphasizing that eliminating inconsistent and duplicative requirements is essential for strengthening the nation's cybersecurity posture. *See, e.g.*, Harmonization Is Needed (Jul. 25, 2024), Before the Subcomm. on Cybersecurity, Information Technology, and Gov't Innovation, H. Comm. on Oversight & Accountability, 118th Cong. (2024).

[147] *See, e.g.*, Statement from Harry Coker, Jr., *We Need to Harmonize Cybersecurity Regulations, What We Heard From our Partners* (Jun. 4, 2024) ("Already we are working with our partners to build a pilot reciprocity framework") ("we more clearly see that regulatory harmonization is a hard problem, exactly the kind of hard problem ONCD was created to solve on behalf of our nation").

[148] *See, e.g.*, Colo. Rev. Stat. § 6-1-1309(2); Conn. Gen. Stat. § 42-522(a); Del. Code tit. 6 § 12D-108(a); Fla. Stat. § 501.713(1); Ind. Code § 24-15-6-1(b); Mont. Code § 30-14-2814(1); SB 255 § 507-H:8(I) (N.H. 2024); Tex. Bus. & Com. Code § 541.105(a); Va. Code Ann. § 59.1-580(A).

a board member attest that they understand the specific findings of an audit, especially if the finding is minimally relevant under a risk-based approach.[149]

- ADMT requirements should provide businesses with 24 months to come into compliance. This approach would align with other U.S. state privacy statutes, which provide a period of time before the statutes' requirements come into effect.[150] Such timing also creates consistency with the 24-month implementation period for cybersecurity audits and privacy risk assessments,[151] which the Initial Statement of Reasons describes as "balanc[ing]" the requirement while providing "sufficient time to establish the processes."[152]

IV. The CPPA Should Revise The SRIA To Accurately Reflect The Substantial Costs The Draft Regulations Impose On Businesses Subject To The CCPA.

As detailed in Michael Genest's memo submitted by CalChamber to the CPPA,[153] the SRIA[154] substantially understates the cost of the Draft Regulations. For example, the SRIA excludes out-of-state businesses subject to the CCPA from its market analysis, ignores significant ongoing compliance costs, and overstates savings. CalChamber encourages the CPPA to update the SRIA to: (1) reflect the impact on out-of-state businesses that are nonetheless subject to the statutory requirements; (2) accurately reflect operational costs of cybersecurity audits and risk assessments; (3) account for the significant technical and operational burden of ADMT opt-out and access rights; (4) reflect the impact on businesses related to the suppression of behavioral advertising; and (5) address elements required under California law, including an evaluation of the Draft Regulations' impact on "the incentives for innovation in products, materials, or processes."[155]

More specifically, the SRIA misrepresents the costs and benefits related to cybersecurity audits, risk assessments, and ADMT requirements. For example:

- The SRIA underestimates the costs associated with the Draft Regulations' broad thresholds for cybersecurity audits, risk assessments, and ADMT obligations that are not targeted to activities likely to present a significant risk to consumers' privacy and

[149] *See* 23 NYCRR § 500.04 (requiring only that a "CISO report on the Covered Entity's cybersecurity program and material cybersecurity risks"); NYDFS § 500.17(b) (requiring certification of material noncompliance to be signed by the highest ranking executive and the CISO and not including a board oversight requirement); U.S. Securities and Exchange Commission, Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 33-11216 (Jul. 26, 2023).

[150] For example, the Colorado Privacy Act was passed in 2021, but "[t]o allow companies time to change their practices and operations to comply with this new law, it will not take effect until July 1, 2023." *See* Colorado Attorney General, *Colorado Privacy Act (CPA)*, https://coag.gov/resources/colorado-privacy-act/. *See also, e.g.*, Ind. Code § 24-15-1-1 (entering effect January 1, 2026 after 2023 passage).

[151] Initial Statement of Reasons, 43, 75.

[152] *Id.* at 43.

[153] CalChamber SRIA Comment.

[154] *See* CPPA, Standardized Regulatory Impact Assessment (Aug. 2024), https://cppa.ca.gov/meetings/materials/20241004_item6_standardized_regulatory_impact_assessment [hereinafter SRIA].

[155] CalChamber SRIA Comment, 4 (noting that "[p]olicies that stifle even a small fraction of ADMT adoption and utilization would have impacts ranging into the tens of billions per year . . . .").

security. For example, the evaluation underestimates costs of building and maintaining ADMT access and opt-out rights, which could be significant given the scope of the activities that may be subject to these requirements. The SRIA also does not address the costs associated with reduction in revenue to the state and the cost of CPPA operations, which could meaningfully impact the projected operating deficit for the state.[156]

- The SRIA also ignores the revenue impacts of the Draft Regulations, including costs related to the suppression of behavioral advertising.[157] The SRIA fails to reflect the breadth of these activities and, in doing so, overlooks the scope of the impact and true costs the Draft Regulations would impose on businesses who may have to scale back or eliminate this kind of commonplace advertising. It also does not address the impact on consumers who will receive fewer offers and promotions for products and services that are most likely to be valuable to them.

- The SRIA omits discussion of the year-over-year costs associated with the yearly audit and risk assessment requirements.[158] For example, a business subject to yearly reporting requirements under the Draft Regulations will need to implement processes to track, document, and maintain compliance – a substantial feat for any business, especially small- and medium-sized businesses in the state.

- The SRIA fails to address the diversion of already scarce privacy and cybersecurity resources toward administrative compliance. This dynamic reduces businesses' ability to invest in proactive security measures, leaving them more vulnerable to cyberattacks. This directly undermines the objectives of the statutory requirement for a cybersecurity audit.

- The SRIA should recognize the costs required to potentially hire independent auditors to conduct cybersecurity audits, including an accurate reflection of the cost for independent auditors that reflects the likely increase in demand for such services while the supply remains fixed (at least in the near term).[159]

- The SRIA fails to acknowledge the impact and costs of the ADMT pre-use notice requirements,[160] which are not justified by the limited benefit to consumers who already receive multiple notices from businesses subject to the CCPA containing redundant information.

Additionally, CalChamber encourages the next iteration of the SRIA to satisfy all of the requirements under California law, including the prognosis on California innovation, and to align with the ballot initiative's direction to the CPPA to "balance the goals of strengthening

[156] Although these projections do not account for cost of regulations, the California Legislative Analyst's Office projected that the state will face a double-digit operating deficit in the years to come. Agencies are projected to contribute to a 14.3% average annual growth between years 2023-29. *See* LAO, *The 2025-26 Budget California Fiscal Outlook*, Appendix 1, https://lao.ca.gov/Publications/Report/4939#Appendix.

[157] *See* CalChamber SRIA Comment, 4.

[158] *See id.*

[159] *See id.* at 3 (noting that "contractor rates used [in the SRIA] also appear low . . . in view of recent increases in accounting rates.").

[160] *See* CalChamber SRIA Comment, 4.

consumer privacy while giving attention to the impact on businesses."[161] Governor Newsom has consistently emphasized the need to "maintain [California's] dominance" and "maintain [Californian] innovation."[162] However, as currently drafted, the Draft Regulations' broad applicability, prescriptive and granular requirements, and inflexibility would stifle ADMT development and technological innovation in California,[163] as well as burden consumers through numerous and confusing notices and opt-out choices.[164]

V. The Draft Regulations Conflict With Fundamental Constitutional Protections.

The Draft Regulations should be significantly revised to address tensions with the First Amendment, Supremacy Clause, and Due Process Clause.

A. The Draft Regulations Raise Concerns Over Compelled Speech In Violation Of The First Amendment.

The Draft Regulations should be revised to address concerns that requirements would chill constitutionally protected speech in violation of the First Amendment.[165] The First Amendment of the U.S. Constitution protects freedom of speech, which includes both the right to speak and "the right to refrain from speaking at all."[166] Importantly, the Supreme Court has recognized that the government unconstitutionally compels speech when it requires companies to adopt a given policy.[167]

The Supreme Court has articulated three basic steps to assessing a compelled speech claim. *First*, the court considers whether the challenged law compels "speech as speech," or whether it only incidentally compels speech as part of regulating conduct.[168] If the former, then the law implicates the First Amendment; if the latter, it may still implicate the First Amendment if the conduct is inherently expressive.[169] *Second*, if the law implicates the First Amendment, then the court must determine what level of scrutiny applies. Laws that compel speech ordinarily receive strict scrutiny, meaning that they must be narrowly tailored to serve a compelling state interest.[170] Laws that compel "commercial" speech, however, receive lesser

[161] CPRA Ballot Initiative, § 3(C)(1).

[162] Taryn Luna & Wendy Lee, *Careful not to stifle innovation, Newsom hesitates on major tech bills,* L.A. Times (Sept. 30, 2024), https://www.latimes.com/california/story/2024-09-30/newsom-tech-california.

[163] CalChamber SRIA Comment, 4 (noting that "[p]olicies that stifle even a small fraction of ADMT adoption and utilization would have impacts ranging into the tens of billions per year . . . .").

[164] CPRA Ballot Initiative, § 3(C)(1) (requiring that the regulations be implemented with the "goal of strengthening consumer privacy while giving attention to the impact on business and innovation").

[165] *See Stanley v. Georgia*, 394 U.S. 557, 564 (1960); *Sorrell v. IMS Health Inc.,* 564 U.S. 552, 566 (2011) ("Lawmakers may no more silence unwanted speech by burdening its utterance than by censoring its content.").

[166] *Wooley v. Maynard*, 430 U.S. 705, 714 (1977).

[167] *See Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc.*, 570 U.S. 205 (2013) (holding that a law violated the First Amendment where it conditioned funding for certain organizations on their adopting a particular "policy" opposing prostitution).

[168] *Nat'l Inst. of Fam. & Life Advocs. v. Becerra* ("*NIFLA*"), 585 U.S. 755, 770 (2018).

[169] *See Rumsfeld v. F. for Acad. & Institutional Rts., Inc.*, 547 U.S. 47, 62, 65–66 (2006).

[170] *See NIFLA*, 585 U.S. at 766.

scrutiny.[171] *Finally*, the court decides whether the law is constitutional under the applicable scrutiny standard.

The Supreme Court has recognized that the government unconstitutionally compels speech when it requires companies to adopt or articulate a given policy. In *Agency for International Development v. Alliance for Open Society International, Inc.*, the Court held that a law violated the First Amendment where it conditioned funding for certain organizations on their adopting a particular "policy" opposing prostitution.[172] The Court stated that the policy requirement would also "plainly violate the First Amendment" if it were "enacted as a direct regulation of speech."[173] Similarly, in *X Corp. v. Bonta*, the Ninth Circuit concluded that a California law that required social media companies to prepare a report detailing their content moderation practices implicated the First Amendment. The Ninth Circuit concluded that "insight into whether a social media company" considers certain factors in its content moderation practices reflects "constitutionally protected speech" that the state cannot compel without satisfying strict scrutiny.[174]

The Draft Regulations require significant revision to minimize tension with First Amendment protections, including with respect to the following topics:

- The CPPA's overbroad cybersecurity audits and privacy risk assessments compel speech and do not satisfy strict scrutiny. Cybersecurity audits and privacy risk assessments reflect more than mere facts about a business's operations. Rather, these documents reflect opinions and judgments about how the business protects consumer personal information, what safeguards are appropriate, and a description of how the business has weighed risks with consumer benefits. For example, cybersecurity audits must "document and explain why [a] component is not necessary" to the business's cybersecurity efforts.[175] The Draft Regulations' approach to privacy risk assessments likewise reflects embedded opinions about the privacy risks and benefits of processing activities, including through the identification of "negative impacts" to consumers associated with the processing, such as intangible considerations like reputational or psychological harms.[176] Even assuming that these requirements further a compelling government interest, their sheer breadth makes plain that they are not narrowly tailored.

- The prescriptive, granular ADMT pre-use notice and access rights compel the disclosure of detailed information about the technology in violation of the First Amendment. For example, the pre-use notice and responses to access requests must include the "intended output" of this technology and "how the business plans to use the output."[177] These

[171] *X Corp. v. Bonta*, 116 F.4th 888, 900 (9th Cir. 2024).

[172] *Agency for Int'l Dev.*, 570 U.S. at 208, 221.

[173] *Id.* at 213; *see also Knox v. Serv. Emps. Int'l Union*, 567 U.S. 298, 309 (2012) ("The government may not . . . compel the endorsement of ideas that it approves.").

[174] *X Corp.*, 116 F.4th at 902.

[175] Draft Regulations § 7123(b).

[176] *Id.* at § 7152(a)(5).

[177] *Id.* at §§ 7220(c)(5); 7222(b)(2)-(3).

explanations about the business' intent and judgments about its process reflect expressive content.

- The Draft Regulations compel speech by requiring that a business that trains ADMT make available documentation, which constitutes compelled speech. Specifically, even though the Draft Regulations style these disclosures as "facts" necessary for the recipient business to conduct its risk assessment, such disclosures require a subjective determination by the business, including about any "requirements or limitations" for the permitted use of the ADMT.[178] To the extent that there is a compelling interest in facilitating the disclosure of information, the CPPA has not established that the required documentation is a narrowly tailored means of achieving that end.

B. Sections Of the Draft Regulations Are Preempted By Federal Law.

The Draft Regulations should be revised because they seek to regulate areas that are preempted by federal law. The Supremacy Clause of the U.S. Constitution prohibits states from regulating conduct "in a field that Congress, acting within its proper authority, has determined must be regulated by its exclusive governance."[179] State laws are also preempted when they conflict with federal law, including when they stand "as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."[180]

For example, federal law protects trade secrets under the Defend Trade Secrets Act ("DTSA"), including "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes" that are kept "secret" and have "independent economic value . . . from not being generally known."[181] While the DTSA does not "preempt or displace any other remedies provided by United States Federal [or] State . . . law for the misappropriation of a trade secret,"[182] California may not entirely abrogate the protections granted to a business's trade secrets.[183]

Notwithstanding the points raised above that the Draft Regulations ignore the express trade secret exemption in the CCPA, a number of requirements contemplate disclosure of trade secrets that would be preempted by federal law. For example, Section 7222 of the Draft Regulations requires a business to share commercially sensitive information with consumers, including the logic, assumptions, limitations, and key parameters of ADMT. Depending on the technology and business in question, and the level of detail expected by regulators, this

[178] *Id.* at § 7153(b).

[179] *Arizona v. United States*, 567 U.S. 387, 399 (2012).

[180] *Id.* (*quoting Hines v. Davidowitz*, 312 U.S. 52, 67 (1941)).

[181] 18 U.S.C. § 1839(3); *see also Adams Arms, LLC v. Unified Weapon Sys., Inc.*, 2016 WL 5391394, at *5 (M.D. Fla. Sept. 27, 2016) ("DTSA is intended to provide a 'single, national standard for trade secret misappropriation with clear rules and predictability for everyone involved.') (quoting 2016 U.S.C.C.A.N. 195, 200).

[182] 18 U.S.C. § 1838.

[183] *See Mik v. Fed. Home Loan Mortg. Corp.*, 743 F.3d 149, 165 (6th Cir. 2014) (holding that a federal statute with similar saving clause for state laws providing greater protection for tenants preempted a state law that was less protective of tenants because it presented an obstacle to the federal law's objective of ensuring that tenants have notice of foreclosure).

information could constitute a business's trade secrets, required disclosure of which is preempted by federal law.

C. Terms And Concepts In The Draft Regulations Are Impermissibly Vague.

Both the federal and California Due Process Clause prohibit the enforcement of laws – including administrative rules – that are so vague that they do not give fair notice to the public regarding the conduct being regulated. A "fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required."[184] A law is unconstitutionally vague if it "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement."[185] Well-settled California law reflects similar concerns with vagueness, as a "statute violates due process of law if it forbids or requires the doing of an act in terms so vague that persons of common intelligence must necessarily guess at its meaning and differ as to its application."[186]

The Draft Regulations invite a number of concerns regarding unconstitutional vagueness, including through the use of unclear definitions and the potentially unbounded scope of requirements:

- As noted above, the ADMT definition reflects an unworkably broad standard, as it requires a business to guess at its meaning and what technologies would be in and out of scope.

- Throughout the Draft Regulations, the CPPA refers to ADMT "capable" of certain uses. In particular, it states that the requirements apply to a business that trains ADMT that is "capable" of being used (1) for a significant decision concerning a consumer, (2) to establish individual identity, (3) for physical or biological identification or profiling, (4) for the generation of a deepfake, or (4) for the operation of generative models, such as large language models.[187] Given the potential broad applicability of ADMT, the "capable of" descriptor is meaningless, as ADMT could be "capable" of innumerable uses. For example, generative AI systems hypothetically could be "capable of" generating a deepfake if used by a bad actor in violation of the business' acceptable use policy. Likewise, spreadsheets and calculators could be "capable of" a significant decision if used in certain contexts. Accordingly, the Draft Regulations are void for vagueness under federal and California law to the extent they rely on this term.

- The cybersecurity audit sections require subjective judgment of the auditor about the sufficiency of cybersecurity protocols. Because the Draft Regulations would not provide an auditor with sufficient clarity to understand how to conduct audits, they are unconstitutionally vague.

[184] *F.C.C. v. Fox Television Stations, Inc.*, 567 U.S. 239, 253 (2012).

[185] *Id.* (quotation marks and citation omitted).

[186] *Teichert Constr. v. California Occupational Safety & Health Appeals Bd.*, 140 Cal. App. 4th 883, (2006).

[187] Draft Regulations §§ 7150(b)(4); 7200(a)(3) (not reflecting requirements for training ADMT capable of being used for the operation of generative models).

Finally, in closing, CalChamber urges the agency to allow for a full 24 months to come into compliance with the updated regulations and the new articles. The cybersecurity audit and risk assessment timelines already recognize a 24-month time frame. Accordingly, the ADMT requirements and the modifications to the existing regulations should also be afforded a 24-month time frame for compliance. Furthermore, CalChamber requests that the CPPA make clear that the regulations apply only to processing activities that occur after the regulations enter into effect.

CalChamber appreciates the CPPA's consideration of these comments, and we look forward to continuing to work with the agency on these important issues.

Sincerely,

Lindsey Tonsager
Jayne Ponder
Olivia Vega
Counsel for CalChamber

APPENDIX

CALIFORNIA PRIVACY PROTECTION AGENCY

PROPOSED TEXT (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations)
TITLE 11. LAW

DIVISION 6. CALIFORNIA PRIVACY PROTECTION AGENCY CHAPTER 1. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS

ARTICLE 1. GENERAL PROVISIONS

§ 7001. Definitions.

In addition to the definitions set forth in Civil Code section 1798.140, for purposes of these regulations:

(a) "Agency" means the California Privacy Protection Agency established by Civil Code section 1798.199.10 et seq.

(b) "Alternative Opt-out Link" means the alternative opt-out link that a business may provide instead of posting the ~~**two**~~ separate "Do Not Sell or Share My Personal Information**,**" ~~**and**~~ "Limit the Use of My Sensitive Personal Information" links as set forth in Civil Code section 1798.135, subdivision (a)(3), and specified in section 7015**, and the ADMT opt-out as set forth in section 7221**.

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

(d) "Attorney General" means the California Attorney General or any officer or employee of the California Department of Justice acting under the authority of the California Attorney General.

(e) "Authorized agent" means a natural person or a business entity that a consumer has authorized to act on their behalf subject to the requirements set forth in section 7063.

(f) "Automated decisionmaking technology" or "ADMT" means any **profiling involving solely automated** technology that processes personal information and uses computation **for the primary purpose of making a significant decision about a consumer** ~~**to execute a decision, or replace 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, other data-processing techniques, or artificial intelligence.**~~

(2) ~~**For purposes of this definition, to “substantially facilitate human decisionmaking” means using the output of the technology as a key factor in a human’s decisionmaking. This includes, for example, using automated decisionmaking technology to generate a score about a consumer that the human reviewer uses as a primary factor to make a significant decision about them.**~~

(3) ~~**Automated decisionmaking technology includes profiling.**~~

(4) Automated decisionmaking technology does not include the following technologies~~**, provided that the technologies do not execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking**~~: 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.**~~

(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 includes cross-context behavioral advertising.**~~

(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.**~~

(h) “Categories of sources” means types or groupings of persons or entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity. They may include the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

(i) “Categories of third parties” means types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party. They may include advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.

(j) “CCPA” means the California Consumer Privacy Act of 2018, Civil Code section 1798.100 et seq.

(k) -“COPPA” means the Children’s Online Privacy Protection Act, 15 U.S.C. sections 6501 to 6506 and 16 Code of Federal Regulations part 312.

(l) “Cybersecurity audit” means the **~~annual~~** cybersecurity audit that every business whose processing of consumers’ personal information presents significant risk to consumers’ security as set forth in section 7120, subsection (b), is required to complete.

(m) “Cybersecurity program” means the policies, procedures, and practices that protect personal information from unauthorized access, destruction, use, modification, or disclosure; and protect against unauthorized activity resulting in the loss of availability of personal information.

(n) **~~“Deepfake” means manipulated or synthetic audio, image, or video content that depicts a consumer saying or doing things they did not say or do and that are presented as truthful or authentic without the consumer’s knowledge and permission.~~**

(o) “Disproportionate effort” within the context of a business, service provider, contractor, or third party responding to a consumer request means the time and/or resources expended by the business, service provider, contractor, or third party to respond to the individualized request significantly outweighs the reasonably foreseeable impact to the consumer by not responding, taking into account applicable circumstances, such as the size of the business, service provider, contractor, or third party, the nature of the request, and the technical limitations impacting their ability to respond. For example, responding to a consumer request to know may require disproportionate effort when the personal information that is the subject of the request is not in a searchable or readily-accessible format, is maintained only for legal or compliance purposes, is not sold or used for any commercial purpose, and there is no reasonably foreseeable material impact to the consumer by not responding. By contrast, the impact to the consumer of denying a request to correct inaccurate information that the business uses and/or sells may outweigh the burden on the business, service provider, contractor, or third party in honoring the request when the reasonably foreseeable consequence of denying the request would be the denial of services or opportunities to the consumer. A business, service provider, contractor, or third party that has failed to put in place adequate processes and procedures to receive and process consumer requests in accordance with the CCPA and these regulations cannot claim that responding to a consumer's request requires disproportionate effort.

(p) "Employment benefits" means retirement, health, and other benefit programs, services, or products to which consumers and their dependents or their beneficiaries receive access through the consumer's employer.

(q) "Employment-related information" means personal information that is collected by the business about a natural person for the reasons identified in Civil Code section 1798.145, subdivision (m)(1). The collection of employment-related information, including for the purpose of administering employment benefits, shall be considered a business purpose.

(r) "Financial incentive" means a program, benefit, or other offering, including payments to consumers, for the collection, retention, sale, or sharing of personal information. Price or service differences are types of financial incentives.

(s) "First party" means a consumer-facing business with which the consumer intends and expects to interact.

(t) "Frictionless manner" means a business's processing of an opt-out preference signal that complies with the requirements set forth in section 7025, subsection (f).

(u) -"Information practices" means practices regarding the collection, use, disclosure, sale, sharing, and retention of personal information.

(v) "Information system" means the resources (e.g., network, hardware, and software) organized for the processing of **personal** information, including the collection, use, disclosure, sale, sharing, and retention of personal information.

(w) "Multi-factor authentication" means authentication through verification of at least two of the following types of authentication factors: (1) knowledge factors, such as a password; (2) possession factors, such as a token; or (3) inherence factors, such as a biometric characteristic.

(x) "Nonbusiness" means a person or entity that does not meet the definition of a "business" as defined in Civil Code section 1798.140, subdivision (d). For example, government entities and many non-profits are nonbusinesses because one definition of "business" requires entities to be "organized or operated for the profit or financial benefit of its shareholders or other owners."

(y) "Notice at Collection" means the notice given by a business to a consumer at or before the point at which a business collects personal information from the consumer as required by Civil Code section 1798.100, subdivisions (a) and (b), and specified in these regulations.

(z) “Notice of Right to Limit” means the notice given by a business informing consumers of their right to limit the use or disclosure of the consumer’s sensitive personal information as required by Civil Code sections 1798.121 and 1798.135 and specified in these regulations.

(aa) “Notice of Right to Opt-out of Sale/Sharing” means the notice given by a business informing consumers of their right to opt-out of the sale or sharing of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in these regulations.

(bb) “Notice of Financial Incentive” means the notice given by a business explaining each financial incentive or price or service difference as required by Civil Code section 1798.125, subdivision (b), and specified in these regulations.

(cc) “Opt-out preference signal” means a signal that is sent by a platform, technology, or mechanism, on behalf of the consumer, that communicates the consumer choice to opt-out of the sale and sharing of personal information and that complies with the requirements set forth in section 7025, subsection (b).

(dd) “Penetration testing” means testing the security of an information system by attempting to circumvent or defeat its security features by authorizing attempted penetration of the information system.

(ee) **~~“Performance at work” means the performance of job duties for which the consumer has been hired or has applied to be hired. The following are not “performance at work”: 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.~~**

(ff) **~~“Performance in an educational program” means the performance of coursework in an educational program in which the consumer is enrolled or has applied to be enrolled. The following are not “performance in an educational program”: 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 educational program provider’s information system, including to prevent the disclosure of confidential information or to prevent cheating; or a consumer’s location when they are not performing coursework.~~**

(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).~~**

(hh) “Price or service difference” means (1) any difference in the price or rate charged for any goods or services to any consumer related to the collection, retention, sale, or sharing of personal information, or (2) any difference in the level or quality of any goods or services offered to any consumer related to the collection, retention, sale, or sharing of personal information, including the denial of goods or services to the consumer.

(ii) “Privacy policy,” as referred to in Civil Code sections 1798.130, subdivision (a)(5), and 1798.135, subdivision (c)(2), means the statement that a business shall make available to consumers describing the business’s online and offline information practices, and the rights of consumers regarding their own personal information.

(jj) “Privileged account” means any authorized user account (i.e., an account designed to be used by an individual) or service account (i.e., an account designed to be used only by a service, not by an individual) that can be used to perform functions that other user accounts are not authorized to perform, including but not limited to the ability to add, change, or remove other accounts, or make configuration changes to an information system.

(kk) “Profiling” means any form of **solely** 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.

(ll) “Publicly accessible place” means a **physical** place that is open to or serves the public, **meaning**. ~~**Examples of publicly accessible places include shopping malls, stores, restaurants, cafes, movie theaters, amusement parks, convention centers, stadiums, gymnasiums,**~~ hospitals, medical clinics or offices, ~~**transportation depots, transit, streets, or parks**~~, **airports, educational institutions, and government buildings.**

(mm) “Request to access ADMT” means a consumer request that a business provide information to the consumer about the business’s use of **personal information for** automated decisionmaking technology~~**with respect to the consumer**~~, pursuant to Civil Code section 1798.185(a)(15) and Article 11 of these regulations.

(nn) ~~**“Request to appeal ADMT” means a consumer request to appeal the business’s use of automated decisionmaking technology for a significant decision as set forth in section 7221, subsection (b)(2).**~~

(oo) “Request to correct” means a consumer request that a business correct inaccurate personal information that it maintains about the consumer, pursuant to Civil Code section 1798.106.

(pp) “Request to delete” means a consumer request that a business delete personal information about the consumer that the business has collected from the consumer, pursuant to Civil Code section 1798.105.

(qq) "Request to know" means a consumer request that a business disclose personal information that it has collected about the consumer pursuant to Civil Code sections 1798.110 or 1798.115. It includes a request for any or all of the following:

(1) Specific pieces of personal information that a business has collected about the consumer;

(2) Categories of personal information it has collected about the consumer;

(3) Categories of sources from which the personal information is collected;

(4) Categories of personal information that the business sold, shared, or disclosed for a business purpose about the consumer;

(5) Categories of third parties to whom the personal information was sold, shared, or disclosed; and

(6) The business or commercial purpose for collecting, ~~or~~ selling, or sharing personal information.

(rr) "Request to limit" means a consumer request that a business limit the use and disclosure of the consumer's sensitive personal information, pursuant to Civil Code section 1798.121, subdivision (a).

(ss) "Request to opt-in to sale/sharing" means an action demonstrating that the consumer has consented to the business's sale or sharing of personal information about the consumer by a parent or guardian of a consumer less than 13 years of age or by a consumer at least 13 years of age.

(tt) "Request to opt-out of ADMT" means a consumer request that a business not use automated decisionmaking technology with respect to the consumer, pursuant to Civil Code section 1798.185(a)(15) and Article 11 of these regulations.

(uu) "Request to opt-out of sale/sharing" means a consumer request that a business neither sell nor share the consumer's personal information to third parties, pursuant to Civil Code section 1798.120, subdivision (a).

(vv) "Right to access ADMT" means a consumer's right to request that a business provide information to the consumer about the business's use of **personal information for** automated decisionmaking technology ~~**with respect to the consumer**~~ as set forth in Civil Code section 1798.185(a)(15) and Article 11 of these regulations.

(ww) "Right to correct" means the consumer's right to request that a business correct inaccurate personal information that it maintains about the consumer as set forth in Civil Code section 1798.106.

(xx) “Right to delete” means the consumer’s right to request that a business delete any personal information about the consumer that the business has collected from the consumer as set forth in Civil Code section 1798.105.

(yy) “Right to know” means the consumer’s right to request that a business disclose personal information that it has collected, sold, or shared about the consumer as set forth in Civil Code sections 1798.110 and 1798.115.

(zz) “Right to limit” means the consumer’s right to request that a business limit the use and disclosure of a consumer’s sensitive personal information as set forth in Civil Code section 1798.121.

(aaa) “Right to opt-out of ADMT” means a consumer’s right to direct that a business not use automated decisionmaking technology ~~**with respect to the consumer**~~ as set forth in Civil Code section 1798.185(a)(15) and Article 11 of these regulations.

(bbb) “Right to opt-out of sale/sharing” means the consumer’s right to direct a business that sells or shares personal information about the consumer to third parties to stop doing so as set forth in Civil Code section 1798.120.

(ccc) “Sensitive personal information” means:

(1) Personal information that reveals:

(A) A consumer’s social security, driver’s license, state identification card, or passport number.

(B) A consumer’s account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

(C) A consumer’s precise geolocation.

(D) A consumer’s racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership.

(E) The contents of a consumer’s mail, email, and text messages unless the business is the intended recipient of the communication.

(F) A consumer’s genetic data.

(2) The processing of biometric information for the purpose of uniquely identifying a consumer.

(3) Personal information collected and analyzed concerning a consumer’s health, sex life, or sexual orientation.

(4) Personal information of consumers that the business has actual knowledge are less than ~~**16**~~ **13** years of age. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age.

Sensitive personal information does not include information that is "publicly available" pursuant to Civil Code section 1798.140, subdivision (v)(2).

(ddd) "Signed" means that the written attestation, declaration, or permission has either been physically signed or provided electronically in accordance with the Uniform Electronic Transactions Act, Civil Code section 1633.1 et seq.

(eee) ~~**"Systematic observation" means methodical and regular or continuous observation. This includes, for example, methodical and regular or continuous observation using Wi-Fi or Bluetooth tracking, radio frequency identification, drones, video or audio recording or live-streaming, technologies that enable physical or biological identification or profiling; and geofencing, location trackers, or license-plate recognition.**~~

(fff) ~~**"Train automated decisionmaking technology or artificial intelligence" means the process through which automated decisionmaking technology or artificial intelligence discovers underlying patterns, learns a series of actions, or is taught to generate a desired output. Examples of training include adjusting the parameters of an algorithm used for automated decisionmaking technology or artificial intelligence, improving the algorithm that determines how a machine- learning model learns, and iterating the datasets fed into automated decisionmaking technology or artificial intelligence.**~~

(ggg) "Third-party identity verification service" means a security process offered by an independent third party that verifies the identity of the consumer making a request to the business. Third-party identity verification services are subject to the requirements set forth in Article 5 regarding requests to delete, requests to correct, or requests to know.

(hhh) "Unstructured" as it relates to personal information means personal information that is not organized in a pre-defined manner and could not be retrieved or organized in a pre-defined manner without disproportionate effort on behalf of the business, service provider, contractor, or third party.

(iii) "Value of the consumer's data" means the value provided to the business by the consumer's data as calculated under section 7081.

(jjj) "Verify" means to determine that the consumer making a request to delete, request to correct, request to know, or request to access ADMT is the consumer about whom the business has collected information, or if that consumer is less than 13 years of age, the consumer's parent or legal guardian.

(kkk) ~~**"Zero trust architecture" means denying access to an information system and the information that it processes by default, and instead explicitly granting and enforcing only the minimal access required. 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.**~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155, 1798.175, 1798.185, 1798.199.40, 1798.199.45, 1798.199.50-and 1798.199.65, Civil Code.

ARTICLE 8. TRAINING AND RECORD-KEEPING

§ 7102. Requirements for Businesses Collecting Large Amounts of Personal Information.

(a) A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, shares, or otherwise makes available for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall:

(1) Compile the following metrics for the previous calendar year:

(A) The number of requests to delete that the business received, complied with in whole or in part, and denied;

(B) The number of requests to correct that the business received, complied with in whole or in part, and denied;

(C) The number of requests to know that the business received, complied with in whole or in part, and denied;

~~(D) **The number of requests to access ADMT that the business received, complied with in whole or in part, and denied;**~~

(E) The number of requests to opt-out of sale/sharing that the business received, complied with in whole or in part, and denied;

(F) The number of requests to limit that the business received, complied with in whole or in part, and denied; **and**

~~(G) **The number of requests to opt-out of ADMT that the business received, complied with in whole or in part, and denied; and**~~

(H) The median or mean number of days within which the business substantively responded to requests to delete, requests to correct, requests to know, requests to opt-out of sale/sharing, and requests to limit.

(2) Disclose, by July 1 of every calendar year, the information compiled in subsection (a)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy. In its disclosure, a business may choose to disclose the number of requests that it denied in whole or in part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds.

(b) A business may choose to compile and disclose the information required by subsection (a)(1) for requests received from all individuals, rather than requests received from consumers. The business shall state whether it has done so in its disclosure and shall, upon request, compile and provide to the Attorney General the information required by subsection (a)(1) for requests received from consumers.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135 and 1798.185, Civil Code.

Adopt all of the text in the following Article:

ARTICLE 9. CYBERSECURITY AUDITS

§ 7120. Requirement to Complete a Cybersecurity Audit.

(a) Every business whose processing of consumers' personal information presents significant risk to consumers' security as set forth in subsection (b) must complete a cybersecurity audit.

(b) A business's processing of consumers' personal information presents significant risk to consumers' security if ~~any of~~ the following is true:

(1) **The processing involves sensitive personal information of 1 million or more consumers or households in the preceding calendar year; and** ~~**The business meets the threshold set forth in Civil Code section 1798.140, subdivision (d)(1)(C), in the preceding calendar year; or**~~

(2) **The processing presents a risk of harm to consumers considering the following factors:**

(A) **The size of the business;**

(B) **The complexity of the business;**

(C) **The nature of the processing activities; and**

(D) **The scope of processing activities.**

~~**The business meets the threshold set forth in Civil Code section 1798.140, subdivision (d)(1)(A); and**~~

~~(E)~~ ~~**Processed the personal information of 250,000 or more consumers or households in the preceding calendar year; or**~~

(F) ~~**Processed the sensitive personal information of 50,000 or more consumers in the preceding calendar year.**~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7121. Timing Requirements for Cybersecurity Audits.

(a) A business has 24 months from the effective date of these regulations to complete its first cybersecurity audit in compliance with the requirements in this Article.

(b) After the business completes its first cybersecurity audit pursuant to subsection (a), its subsequent cybersecurity audits must be completed every ~~**calendar**~~ **three (3)** years, and there must be no gap in the months covered by successive cybersecurity audits.

(c) After the business completes its first cybersecurity audit pursuant to subsection (a), it must annually review its cybersecurity program.

(d) For any activity that meets the threshold in Section 7120, subsection (b), the cybersecurity audit must only take into account activities 24 months after the effective date of these regulations.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7122. Thoroughness and Independence of Cybersecurity Audits.

(a) Every business required to complete a cybersecurity audit pursuant to this Article must do so using a qualified, objective, independent professional ("auditor") using procedures and standards generally accepted in the profession of **cybersecurity** auditing.

(1) The auditor may be internal or external to the business but must exercise objective and impartial judgment on all issues within the scope of the cybersecurity audit, must be free to make decisions and assessments without influence by the business being audited, including the business's owners, managers, or employees; and must not participate in activities that may compromise, or appear to compromise, the auditor's independence. For example, the auditor must not participate in the business activities that the auditor may assess in the current or subsequent cybersecurity audits, including developing procedures, preparing the business's documents, or making recommendations regarding, implementing, or maintaining the business's cybersecurity program.

(2) If a business uses an internal auditor, the auditor must report regarding cybersecurity audit issues directly to the business's **Chief Information Security Officer.** ~~**board of directors or governing body, not to business management that has direct responsibility for the business's cybersecurity program.**~~ If no such **officer or equivalent role** ~~**board or equivalent body**~~ **exists,** the internal auditor must report to the business's highest ranking **executive responsible for the organization's cybersecurity program, such as the Chief Risk Officer, Chief Compliance Officer, or another designated individual with appropriate authority and expertise in cybersecurity matters.** ~~**that does not have direct responsibility for the business's cybersecurity program.**~~ **The business's Chief Information Security Officer, or otherwise designated senior executive,** must conduct the auditor's performance evaluation and determine the auditor's compensation.

(b) To enable the auditor to determine the scope of the cybersecurity audit and the criteria the cybersecurity audit will evaluate, the business must make available to the auditor all information in the business's possession, custody, or control that the auditor requests as relevant to the cybersecurity audit (e.g., information about the business's cybersecurity program and information system and the business's use of service providers or contractors).

(c) The business must make good-faith efforts to disclose to the auditor all facts relevant to the cybersecurity audit and must not misrepresent in any manner any fact relevant to the cybersecurity audit.

(d) The cybersecurity audit must articulate its scope, articulate its criteria, and identify the specific evidence (including documents reviewed, sampling and testing performed, and interviews conducted) examined to make decisions and assessments, and explain why the scope of the cybersecurity audit, the criteria evaluated, and the evidence that the auditor examined are (1) appropriate for auditing the business's cybersecurity program, taking into account the business's size, complexity, and the nature and scope of its processing activities; and (2) why the specific evidence examined is sufficient to justify the auditor's findings. No finding of any cybersecurity audit may rely primarily on assertions or attestations by the business's management. Cybersecurity audit findings must rely primarily upon the specific evidence (including documents reviewed, sampling and testing performed, and interviews conducted) that is deemed appropriate by the auditor.

(e) The cybersecurity audit must **take into account the size and complexity of the business and the nature and scope of processing activities. The cybersecurity audit may**:

(1) Assess, document, and summarize each applicable component of the business's cybersecurity program set forth in section 7123;

(2) ~~**Specifically i**~~ **I**dentify any **material** gaps or weaknesses in the business's cybersecurity program;

(3) ~~**Specifically a**~~ **A**ddress the status of any **material** gaps or weaknesses identified in any prior cybersecurity audit; and

(4) ~~**Specifically i**~~ **I**dentify any corrections or amendments to any prior cybersecurity audits.

(f) The cybersecurity audit **may** ~~**must**~~ include the auditor's name, affiliation, and relevant qualifications.

(g) The cybersecurity audit **may** ~~**must**~~ include a statement that is signed and dated by each auditor that certifies that the auditor completed an independent review of the business's cybersecurity program and information system, exercised objective and impartial judgment on all issues within the scope of the cybersecurity audit, and did not rely primarily on assertions or attestations by the business's management.

(h) The cybersecurity audit **described in Section 7123** must be reported to the business's board of directors or governing body, or if no such board or equivalent body exists, to the highest- ranking executive in the business responsible for the business's cybersecurity program**.**

(i) The cybersecurity audit must include a statement that is signed and dated by **the Chief Information Security Officer,** ~~**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**~~ 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.

(j) The auditor must retain all documents relevant to each cybersecurity audit for a minimum of **two (2)** years after completion of the cybersecurity audit.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7123. Scope of Cybersecurity Audit.

(a) The cybersecurity audit must assess and document how the business's cybersecurity program protects personal information from unauthorized access, destruction, use, modification, or disclosure; and protects against unauthorized activity resulting in the loss of availability of personal information **that conform to the NIST Cybersecurity Framework or a comparable standard.**

(b) **Requirements under this Article apply only to activities involving the processing of personal information.**

(c) The cybersecurity audit must **take into account the size and complexity of the business and the nature and scope of processing activities. The cybersecurity audit may** specifically identify, assess, and document:

(1) The business's establishment, implementation, and maintenance of its cybersecurity program, including the related written documentation thereof (e.g., policies and procedures), that is appropriate to the business's size and complexity and the nature and scope of its processing activities, ~~**taking into account the state of the art and cost of implementing the components of a cybersecurity program, including the components set forth in this subsection and subsection (b)(2)**~~; and

(2) Each of the following components of the business's cybersecurity program, as applicable. If not applicable, the cybersecurity audit ~~**must**~~ **may** document and explain why the component is not necessary to the business's protection of personal information and how the safeguards that the business does have in place provide at least equivalent security:

(A) Authentication, including:

(i) Multi-factor authentication (including multi-factor authentication that is resistant to phishing attacks for employees, independent contractors, and any other personnel; service providers; and contractors); and

(ii) Strong unique passwords or passphrases (e.g., passwords that are at least eight characters in length, not on the business's disallowed list of commonly used passwords, and not reused).

(B) Encryption of personal information, at rest and in transit;

~~(C) **Zero trust architecture (e.g., ensuring that connections within the business's information system are both encrypted and authenticated)**~~

(D) Account management and access controls **used to protect personal information**, including:

(i) Restricting each person's privileges and access to personal information to what is necessary for that person to perform their duties. For example:

1. If the person is an employee, independent contractor, or any other personnel, restricting their privileges and access to personal information to what is necessary to perform the respective job functions of each individual, and revoking their privileges and access when their job functions no longer require them, including when their employment or contract is terminated;

2. If the person is a service provider or contractor, restricting their privileges and access to personal information to what is necessary for the specific business purpose(s) **for which it processes personal information** ~~**set forth in, and in compliance with, the written contract between the business and the service provider or contractor required by the CCPA and section 7051;**~~ and

3. Restricting the privileges and access of third parties to whom the business sells or shares personal information to the personal information that is necessary for the limited and specified purpose(s) **for which it processes personal information** ~~**set forth within the contract between the business and the third party required by the CCPA and section 7053;**~~

(ii) Restricting the number of privileged accounts, restricting those privileged accounts' access functions to only those necessary to perform the account-holder's job, restricting the use of privileged accounts to when they are necessary to perform functions, and using a privileged-access management solution (e.g., to ensure just-in-time temporary assignment of privileged access);

(iii) Restricting and monitoring the creation of new accounts for employees, independent contractors, or other personnel; service providers or contractors; and privileged accounts, and ensuring that the accounts' access and privileges are limited as set forth in subsections (b)(2)(D)(i)–(ii); and

(iv) Restricting and monitoring physical access to personal information (e.g., through the use of badges, secure physical file locations, and enforcement of clean-desk policies).

(E) Inventory and management of personal information and the business's information system. This includes**, as applicable**:

(i) Personal information inventories (e.g., maps and flows identifying where personal information is stored, and how it can be accessed) and the classification and tagging of personal information (e.g., how personal information is tagged and how those tags are used to control the use and disclosure of personal information);

(ii) Hardware and software inventories, and the use of allowlisting (i.e., discrete lists of authorized hardware and software to control what is permitted to connect to and execute on the business's information system); and

(iii) Hardware and software approval processes, and preventing the connection of unauthorized hardware and devices to the business's information system.

(F) Secure configuration of hardware and software **used to protect personal information**, including:

(i) Software updates and upgrades;

(ii) Securing on-premises and cloud-based environments;

(iii) Masking (i.e., systematically removing or replacing with symbols such as asterisks or bullets) the sensitive personal information set forth in Civil Code section 1798.145, subdivisions (ae)(1)(A) and (B) and other personal information as appropriate by default in applications;

(iv) Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and

(v) Change management (i.e., processes and procedures to ensure that changes to information system(s) do not undermine existing safeguards).

(G) Internal and external vulnerability scans, penetration testing, and vulnerability disclosure and reporting (e.g., bug bounty and ethical hacking programs) **used to protect personal information**;

(H) Audit-log management, including the centralized storage, retention, and monitoring of logs **used to protect personal information**;

(I) Network monitoring and defenses **used to protect personal information**, including the deployment of:

(i) Bot-detection and intrusion-detection and intrusion-prevention systems (e.g., to detect unsuccessful login attempts, monitor the activity of authorized users; and detect unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information); and

(ii) Data-loss-prevention systems (e.g., software to detect and prevent unauthorized access, use, or disclosure of personal information).

(J) Antivirus and antimalware protections **to safeguard personal information**;

(K) Segmentation of an information system **that involve personal information** (e.g., via properly configured firewalls, routers, switches);

~~(L)~~ ~~**Limitation and control of ports, services, and protocols;**~~

(M) Cybersecurity awareness, education, and training~~, **including:**~~

~~**(i)**~~ ~~**Training for each employee, independent contractor, and any other personnel to whom the business provides access to its information system (e.g., when their employment or contract begins, annually thereafter, and after a personal information security breach, as described in Civil Code section 1798.150); and**~~

(ii) ~~**How the business maintains current knowledge of changing cybersecurity threats and countermeasures.**~~

(N) Secure development and coding best practices, including code- reviews and testing;

~~(O) **Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053;**~~

(P) Retention schedules and proper disposal of personal information no longer required to be retained~~**, by (1) shredding, (2) erasing, or (3) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means**~~;

(Q) How the business manages its responses to security incidents (~~**i.e.**~~**e.g.**, its incident response management);

(i) For the purposes of subsection (Q), "security incident" **has the same** mean**ing**~~**s**~~ **as "breach of security of the system" in Section 1798.82, as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.** ~~**actually or potentially jeopardizes the confidentiality, integrity, or availability of the business's information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of the business's cybersecurity program. Unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information is a security incident.**~~

(ii) The business's incident response management includes:

1. The business's documentation of predetermined instructions or procedures to detect, respond to, limit the consequences of, and recover from **a security incident** ~~**malicious attacks against its information system (i.e., the business's incident response plan)**~~; and

~~**2. How the business tests its incident-response capabilities; and**~~

(R) Business-continuity and disaster-recovery plans, including data- recovery capabilities and backups **as it relates to personal information for cybersecurity-related disruptions**.

(3) For each of the applicable components set forth in subsections (b)(1)–(2), including the safeguards the business identifies in its policies and procedures, the cybersecurity audit **may** ~~**must**~~ describe, at a minimum, how the business implements and enforces compliance with them.

(4) Nothing in this section prohibits an audit from assessing and documenting components of a cybersecurity program that are not set forth in subsections (b)(1)–(2).

(d) The cybersecurity audit **may** ~~**must**~~:

(1) Assess and document the effectiveness of the components set forth in subsections (b)(1)–(2) in preventing unauthorized access, destruction, use, modification, or disclosure of personal information; and preventing unauthorized activity resulting in the loss of availability of personal information;

(2) Identify and describe in detail the status of any **material** gaps or weaknesses of the components set forth in subsections (b)(1)–(2);

(3) Document the business's plan to address the **material** gaps and weaknesses identified and described pursuant to subsection (c)(2), including the resources it has allocated to resolve them and the timeframe in which it will resolve them;

(4) Include the title(s) of the qualified individuals **primarily** responsible for the business's cybersecurity program; and

(5) Include the date that the cybersecurity program and any evaluations thereof were presented to the **Chief Information Security Officer** ~~**business's board of directors or governing body**~~ or, if no such **individual exists** ~~**board or equivalent governing body exists,**~~ to the highest-ranking executive of the business responsible for the business's cybersecurity program**, such as the Chief Risk Officer, Chief Compliance Officer, or another designated individual with appropriate authority and expertise in cybersecurity matters.**

(e) If the business provided notification to **the Attorney General** ~~**affected consumer(s)**~~ pursuant to Civil Code section 1798.82, subdivision **(f)**~~**(a)**~~, the cybersecurity audit must include a ~~**sample**~~ copy of the notification~~**(s)**~~, excluding any personal information; or a description of the notification~~**(s)**~~.

(f) If the business was required to notify any **California** agency with jurisdiction over privacy laws or other data processing authority in California~~**, other states, territories, or countries**~~ **pursuant to Cal. Civ. Code 1798.82**~~**unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information**~~, the cybersecurity audit must include **the materials provided to that agency.** ~~**a sample copy of the notification(s), excluding any personal information; or a description of the required notification(s) as well as the date(s) and details of the activity that gave rise to the required notification(s) and any related remediation measures taken by the business.**~~

(g) If the business has engaged in a cybersecurity audit, assessment, or evaluation that **is reasonably in scope and effect that would otherwise be conducted under** ~~**meets all of the requirements of**~~ this Article, the business is not required to complete a duplicative cybersecurity audit. **Specifically, cybersecurity audits that are conducted to evaluate a business's implementation against the following frameworks satisfy the requirements under this article: SOC 2 Type 2, ISO Certifications, or the National Institute of Standards and Technology Cybersecurity Framework** ~~**However, the business must specifically explain how the cybersecurity audit, assessment, or**~~

~~**evaluation that it has completed meets all of the requirements set forth in this Article. The business must specifically address subsections (a)–(e), including explaining how the cybersecurity audit, assessment, or evaluation addresses each component set forth in subsections (b)(1)–(2). If the cybersecurity audit, assessment, or evaluation completed for the purpose of compliance with another law or regulation or for another purpose does not meet all of the requirements of this Article, the business must supplement the cybersecurity audit with any additional information required to meet all of the requirements of this Article.**~~

(h) **A single cybersecurity audit that meets the requirements set forth in subsection (a) may address a comparable set of processing activities that includes similar activities.**

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7124. Certification of Completion.

(a) Each business that is required to complete a cybersecurity audit pursuant to this Article must submit to the Agency every **three** ~~**calendar**~~ year**s** a written certification that the business completed the cybersecurity audit as set forth in this Article.

(b) 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**~~.

(c) ~~**The written certification must be 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 who is responsible for oversight of the business's cybersecurity-audit compliance. It also must include a statement that certifies that the signer has reviewed and understands the findings of the cybersecurity audit. The signer must include their name and title.**~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

Adopt all of the text in the following Article:

ARTICLE 10. RISK ASSESSMENTS

§ 7150. When a Business Must Conduct a Risk Assessment.

(a) Every business whose processing of consumers' personal information presents significant risk to consumers' privacy as set forth in subsection (b) must conduct a risk assessment before initiating that processing.

(b) Each of the following processing activities presents significant risk to consumers' privacy:

(1) Selling or sharing personal information.

(2) Processing sensitive personal information **of 1 million or more consumers or households in the preceding calendar year**.

(A) A business that processes the sensitive personal information of its employees or independent contractors solely and specifically for purposes of administering compensation payments, determining and storing employment authorization, administering employment benefits, or wage reporting as required by law, is not required to conduct a risk assessment for the processing of sensitive personal information for these purposes. Any other processing of consumers' sensitive personal information is subject to the risk-assessment requirements set forth in this Article.

(3) Using automated decisionmaking technology for a significant decision concerning a consumer ~~or for extensive profiling~~.

(A) For purposes of this Article, "significant decision" means**, unless exempt by statute or as otherwise set forth in these rules,** a decision using **personal** information ~~that is not subject to the exceptions set forth in Civil Code sections 1798.145, subdivisions (c)-(g), or 1798.146, subdivisions (a)(1), (4), and (5)~~, 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 **in emergency situations)**.

(i) Education enrollment or opportunity **means**~~includes~~:

1. Admission or acceptance into academic or vocational programs;

2. Educational credentials (e.g., a degree, diploma, or certificate); and

3. Suspension and expulsion.

(ii) Employment or independent contracting opportunity or compensation **means**~~**includes**~~:

1. Hiring;

2. ~~**Allocation or assignment of work; s**~~ Salary~~**, hourly or per- assignment compensation, incentive compensation such as a bonus, or another benefit (“allocation/assignment of work and compensation”)**~~;

3. Promotion; and

4. Demotion, suspension, and termination.

(B) **For purposes of this Article, a business required to complete a risk assessment under subsection (a)(3) refers to the entity that uses the automated decisionmaking system.**

~~(C)~~ ~~**For purposes of this Article, “extensive profiling” means:**~~

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

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

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

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

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

~~(B)~~ ~~**To establish individual identity;**~~

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

~~(D)~~ ~~**For the generation of a deepfake; or**~~

(E) ~~**For the operation of generative models, such as large language models.**~~

(c) Illustrative examples of when a business must conduct a risk assessment:

(1) ~~**Business A is a rideshare provider. Business A seeks to use automated decisionmaking technology to allocate rides and determine fares and bonuses**~~

~~**for its drivers. Business A must conduct a risk assessment because it seeks to use automated decisionmaking technology for a significant decision concerning a consumer.**~~

(2) Business B is hiring a new employee. Business B seeks to use emotion-assessment **automated decisionmaking** technology, **the result of which will be dispositive as to whether the employee advances further in the hiring process.** ~~**as part of the job interview process to determine who to hire.**~~ Business B must conduct a risk assessment because it seeks to use automated decisionmaking technology ~~**(specifically, physical or biological identification or profiling)**~~ for a significant decision concerning a consumer.

(3) Business C provides a mobile dating application. Business C seeks to disclose consumers' precise geolocation and the ethnicity and medical information **that more than 1 million** ~~**the**~~ consumers provided in their dating profiles to Business C's analytics service provider. Business C must conduct a risk assessment because it seeks to process sensitive personal information of **more than 1 million** consumers.

(4) 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 **(through cross-context behavioral advertising)** 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 **for cross-context behavioral advertising**.

(5) ~~**Business E is a grocery store chain. Business E seeks to process consumers' device media access control (MAC) addresses via Wi-Fi tracking to observe consumers' shopping patterns within its grocery stores. Business E must conduct a risk assessment because it seeks to profile consumers through systematic observation of a publicly accessible place.**~~

(6) Business F is a technology provider. Business F seeks to extract faceprints from **more than 1 million** consumers' photographs to train Business F's facial-recognition technology. Business F must conduct a risk assessment because it seeks to process consumers' **sensitive** personal information **of more than 1 million consumers** ~~**to train automated decisionmaking technology or artificial intelligence that is capable of being used to establish individual identity**~~.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7151. Stakeholder Involvement for Risk Assessments.

(a) The business must ensure that relevant individuals prepare, contribute to, or review the risk assessment, based upon their level of involvement in the processing activity that is subject to the risk assessment. Relevant individuals are those whose job duties pertain to the processing activity. For example, relevant individuals may be part of the business's product~~**, fraud-prevention,**~~ or compliance teams. These individuals must make good faith efforts to disclose all facts necessary to conduct the risk assessment and must not misrepresent in any manner any fact necessary to conduct the risk assessment.

(b) A risk assessment may involve external parties to identify, assess, and mitigate the risks to consumers' privacy. These external parties may include, for example, service providers, contractors, experts in detecting and mitigating bias in automated decisionmaking technology, a subset of the consumers whose personal information the business seeks to process, or stakeholders that represent consumers' or others' interests, including consumer advocacy organizations.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7152. Risk Assessment Requirements.

(a) The business must conduct a risk assessment to **inform its processing activities, including** ~~**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. The business must conduct and document the risk assessment as set forth below:

(1) The business **may** ~~**must**~~ specifically identify its purpose for processing consumers' personal information. ~~**The purpose must not be identified or described in generic terms, such as "to improve our services" or for "security purposes."**~~

(2) The business **may** ~~**must**~~ identify the categories of personal information to be processed and whether they include sensitive personal information. This must include:

(A) The minimum personal information that is necessary to achieve the purpose of processing consumers' personal information.

~~(B)~~ ~~**For uses of automated decisionmaking technology or artificial intelligence as set forth in section 7150, subsections (b)(3)(A)–(4), the business may must identify the actions the business has taken or any actions it plans to take to maintain the quality of personal information processed by the automated decisionmaking technology or artificial intelligence.**~~

~~**(i)**~~ ~~**"Quality of personal information" includes completeness, representativeness, timeliness, validity, accuracy, consistency; and reliability of the sources of the personal information for the business's proposed use of the automated decisionmaking technology or artificial intelligence.**~~

(ii) ~~**Actions a business may take to ensure quality of personal information include: (1) identifying the source of the personal**~~

~~**information and whether that source is reliable (or, if known, whether the original source of the personal information is reliable); (2) identifying how the personal information is relevant to the task being automated and how it is expected to be useful for the development, testing, and operation of the automated decisionmaking technology or artificial intelligence; (3) identifying whether the personal information contains sufficient breadth to address the range of real-world inputs the automated decisionmaking technology or artificial intelligence may encounter; and (4) identifying how errors from data entry, machine processing, or other sources are measured and limited.**~~

(3) The business **may** ~~**must**~~ identify the following operational elements of its processing:

(A) The business's planned method for collecting, using, disclosing, retaining, or otherwise processing personal information, and the sources of the personal information.

~~(B) **How long the business will retain each category of personal information, and any criteria used to determine that retention period.**~~

(C) The relationship between the consumer and the business, including whether the consumer interacts with the business, how they do so (e.g., via websites, applications, or offline), and the nature of the interaction (e.g., to obtain a good or service from the business).

~~(D) **The approximate number of consumers whose personal information the business seeks to process.**~~

(E) What disclosures the business has made or plans to make to the consumer about the processing, how these disclosures were made (e.g., via a just-in-time notice), and what actions the business has taken or plans to take to make these disclosures specific, explicit, prominent, and clear to the consumer.

(F) The names or categories of the service providers, contractors, or third parties to whom the business discloses or makes available the consumers' personal information for the processing; the purpose for which the business discloses or makes the consumers' personal information available to them; and what actions the business has taken or plans to take to make consumers aware of the involvement of these entities in the processing.

(G) The technology to be used in the processing. For the uses of automated decisionmaking technology set forth in section 7150, subsections (b)(3), the business **may** ~~**must**~~ identify:

~~**(i) The logic of the automated decisionmaking technology, including any assumptions or limitations of the logic; and**~~

(ii) The output of the automated decisionmaking technology, and how the business **intends to** ~~**will**~~ use the output.

(4) The business **may** ~~**must**~~ specifically identify 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.**~~

(5) The business **may** ~~**must**~~ specifically identify the negative impacts to consumers' privacy associated with the processing. The business **may** ~~**must**~~ identify the sources and causes of these negative impacts, and any criteria that the business used to make these determinations.

Negative impacts to consumers' privacy that a business may consider include the following:

(A) Unauthorized access, destruction, use, modification, or disclosure of personal information; and unauthorized activity resulting in the loss of availability of personal information.

~~**(B) Discrimination upon the basis of protected classes that would violate federal or state antidiscrimination law.**~~

(C) Impairing consumers' control over their personal information, such as by providing insufficient information for consumers to make an informed decision regarding the processing of their personal information, or by interfering with consumers' ability to make choices consistent with their reasonable expectations.

(D) Coercing or compelling consumers into allowing the processing of their personal information, ~~**such as by conditioning consumers' acquisition or use of an online service upon their disclosure of personal information that is unnecessary to the expected functionality of the service, or requiring consumers to consent to processing when such consent cannot be freely given.**~~

~~**(E) Disclosing a consumer's media consumption (e.g., books they have read or videos they have watched) in a manner that chills or deters their speech, expression, or exploration of ideas.**~~

(F) **~~Economic harms, including limiting or depriving consumers of economic opportunities; charging consumers higher prices; compensating consumers at lower rates; or imposing additional costs upon consumers, including costs associated with the unauthorized access to consumers' personal information~~**.

(G) Physical harms to consumers or to property, including processing that creates the opportunity for physical or sexual violence.

(H) Reputational harms, including stigmatization, that would negatively impact an average consumer. **~~Examples of processing activities that result in such harms include a mobile dating application's disclosure of a consumer's sexual or other preferences in a partner; a business stating or implying that a consumer has committed a crime without verifying this information; or a business processing consumers' biometric information to create a deepfake of them.~~**

(I) Psychological harms, including emotional distress, stress, anxiety, embarrassment, fear, frustration, shame, and feelings of violation, that would negatively impact an average consumer. Examples of such harms include emotional distress resulting from disclosure of nonconsensual intimate imagery**~~; stress and anxiety from regularly targeting a consumer who visits websites for substance abuse resources with advertisements for alcohol; or emotional distress from disclosing a consumer's purchase of pregnancy tests or emergency contraception for non-medical purposes~~**.

(6) The business **may** **~~must~~** identify the safeguards that it plans to implement to address **~~the~~** **any** negative impacts identified in subsection (a)(5). The business **may** **~~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.

(A) Safeguards that a business may consider include the following:

(i) Encryption, segmentation of information systems, physical and logical access controls, change management, network monitoring and defenses, and data and integrity monitoring;

(ii) Use of privacy-enhancing technologies, such as trusted execution environments, federated learning, homomorphic encryption, and differential privacy;

(iii) Consulting external parties, such as those described in section 7151, subsection (b), to ensure that the business maintains current knowledge of emergent privacy risks and countermeasures; and using that knowledge to identify, assess, and mitigate risks to consumers' privacy; and

~~**(iv) Evaluating the need for human involvement as part of the business's use of automated decisionmaking technology, and implementing policies, procedures, and training to address the degree and details of human involvement identified as necessary in that evaluation.**~~

~~(B)~~ ~~**For uses of automated decisionmaking technology set forth in section 7150, subsection (b)(3)(A), the business may 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 discriminate based upon protected classes ("evaluation of the automated decisionmaking technology"); and**~~

(ii) ~~**The policies, procedures, and training the business has implemented or plans to implement to ensure that the automated decisionmaking technology works as intended for the business's proposed use and does not discriminate based upon protected classes ("accuracy and nondiscrimination safeguards"). For example, if a business determines that the use of low-quality enrollment images creates a high risk of false- positive matches in its proposed use of facial-recognition technology, the business must identify the policies, procedures, and training it has implemented or plans to implement to ensure that it is using only sufficiently high-quality enrollment images to mitigate that risk.**~~

~~**(iii) Where a business obtains the automated decisionmaking technology from another person, the business must identify the following:**~~

~~**1. Whether it reviewed that person's evaluation of the automated decisionmaking technology, and whether that person's evaluation included any requirements or limitations relevant to the business's proposed use of the automated decisionmaking technology.**~~

2. ~~**Any accuracy and nondiscrimination safeguards that it implemented or plans to implement.**~~

(7) The business **may** ~~**must**~~ identify whether it will initiate the processing subject to the risk assessment.

(8) The business **may** ~~**must**~~ identify the contributors to the risk assessment. In the risk assessment or in a separate document maintained by the business, the business **may** ~~**must**~~ identify the individuals within the business and the external parties that contributed to the risk assessment.

(9) The business **may** ~~**must**~~ identify the date the assessment was reviewed and approved~~**, and the names and positions of the individuals responsible for the review and approval. The individuals responsible for the review and approval may must include the individual who decides whether the business will initiate the processing that is subject to the risk assessment. If the business presented or summarized its risk assessment to the business's board of directors or governing body for review, or if no such board or equivalent body exists, to the business's highest-ranking executive who is responsible for oversight of risk-assessment compliance for review, the business must include the date of that review.**~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

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

(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), must provide all facts 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 another person to use that automated decisionmaking technology or artificial intelligence, must provide to the person a plain language explanation of any requirements or limitations that the business identified as 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.**~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

~~**§ 7154. Prohibition Against Processing If Risks to Consumers' Privacy Outweigh Benefits.**~~

(a) ~~**The business must not process personal information for any processing activity identified in section 7150, subsection (b), if the risks to consumers' privacy outweigh the benefits to the consumer, the business, other stakeholders, and the public from the processing.**~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 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) ~~**At least once every three years, a**~~ **A** business must review, and update as necessary, its risk assessments to ensure that they remain accurate in accordance with the requirements of this Article.

(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 material change is one that is likely to affect whether a reasonable consumer would interact with the product or service based on the change in processing activity.** ~~**A change relating to the processing activity is material if it diminishes the benefits of the processing activity as set forth in section 7152, subsection (a)(4), creates new negative impacts or increases the magnitude or likelihood of previously identified negative impacts as set forth in section 7152, subsection (a)(5), or diminishes the effectiveness of the safeguards as set forth in section 7152, subsection (a)(6).**~~

~~**Material changes may include, for example, changes to the purpose of the processing; the minimum personal information necessary to achieve the purpose of the processing; or the risks to consumers' privacy raised by consumers (e.g., numerous consumers complain to a business about the risks that the business's processing poses to their privacy).**~~

(b) ~~**A business must retain its risk assessments, including original and updated versions, for as long as the processing continues or for five years after the completion of the risk assessment, whichever is later.**~~

(c) Requirements under this Article apply only to activities involving the processing of personal information.

(d) Requirements under this Article apply only to processing activities initiated after this Article enters effect.

(e) For any processing activity identified in section 7150, subsection (b), ~~**that the business initiated prior to the effective date of these regulations and**~~ that **begins** ~~**continues**~~ after the effective date of these regulations, the business must conduct and document a risk assessment in accordance with the requirements of this Article within 24 months of the effective date of these regulations.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7156. Conducting Risk Assessments for a Comparable Set of Processing Activities or in Compliance with Other Laws or Regulations.

(a) A business may conduct a single risk assessment for a comparable set of processing activities. A "comparable set of processing activities" that can be addressed by a single risk assessment is a set of similar processing activities that present similar risks to consumers' privacy.

(1) For example, Business G sells toys to children and is considering using in- store paper forms to collect names, mailing addresses, and birthdays from children that visit their stores, and to use that information to mail a coupon and list of age-appropriate toys to each child during the child's birth month and every November. Business G uses the same service providers and technology for each category of mailings across all stores. Business G must conduct and document a risk assessment because it is processing sensitive personal information **of more than 1 million consumers**. Business G may use a single risk assessment for processing the personal information for the birthday mailing and November mailing across all stores because in each case it is collecting the same personal information in the same way for the purpose of sending coupons and age-appropriate toy lists to children, and this processing presents similar risks to consumers' privacy.

(b) If the business has conducted and documented a risk assessment for the purpose of complying with another law or regulation that **is reasonably similar in scope and effect that would otherwise be conducted under**~~ meets all the requirements of~~ this Article, the business is not required to conduct a duplicative risk assessment. ~~**If the risk assessment conducted and documented for the purpose of compliance with another law or regulation does not meet all of the requirements of this Article, the business must supplement the risk assessment with any additional information required to meet all of the requirements of this Article.**~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7157. Submission of Risk Assessments to the Agency.

(a) Timing of Risk Assessment~~ **Submissions**~~.

(1) ~~**First Submission.**~~ A business has 24 months from the effective date of these regulations to **complete a risk assessment** ~~**submit the risk assessment materials regarding the risk assessments that it has conducted from the effective date of these regulations to the date of submission ("first submission"). The risk assessment materials are set forth in subsection (b) and must be submitted to the Agency as set forth in subsection (c).**~~

(2) ~~**Annual Submission. After the business completes its first submission to the Agency as set forth in subsection (a)(1), its subsequent certification of conduct risk assessment materials must be submitted every calendar year to the Agency, and there must be no gap in the months covered by successive submissions of risk assessment materials ("subsequent annual submissions").**~~

(b) **~~Risk Assessment Materials to Be Submitted. The first submission and subsequent annual submissions of the risk assessment materials to the Agency must include the Certification of Conduct 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 Confirmation that the designated executive has reviewed, understood, and approved 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.~~**

(2) Risk Assessments in Abridged Form. For each risk assessment conducted and documented or updated by the business during the submission period, the business **may** **~~must~~** submit an abridged version of the new or updated risk assessment to the Agency **in response to the Agency's request** **~~on a form provided by the Agency that includes~~**:

~~(A)~~ **~~Identification of the processing activity in section 7150, subsection (b), that triggered the risk assessment;~~**

~~(B)~~ **~~A plain language explanation of its purpose for processing consumers' personal information;~~**

~~(C)~~ ~~**The categories of personal information processed, and whether they include sensitive personal information; and**~~

(D) ~~**A plain language explanation of the safeguards that the business has implemented or plans to implement as set forth in section 7152, subsection (a)(6).**~~ A business is not required to provide information that would compromise its ability to prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information; resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions; or ensure the physical safety of natural persons. **A business is not required to provide information that would be business sensitive, confidential, or subject to privilege or other protection.**

(3) Risk Assessments in Unabridged Form. A business also may include in its submission to the Agency a hyperlink that, if clicked, will lead to a public webpage that contains its unabridged risk assessment.

(4) ~~**Exemptions.**~~

~~(A)~~ ~~**A business is not required to submit a Certification of Conduct risk assessment to the Agency if the business does not initiate the processing activity subject to the risk assessment.**~~

(B) ~~**If a business previously conducted a risk assessment for a processing activity in compliance with this Article and submitted an abridged risk assessment to the Agency, and there were no material changes to that processing during a subsequent submission period, the business is not required to submit an updated risk assessment to the Agency. The business must still submit a certification of the conduct of its risk assessment to the Agency.**~~

(c) Method of Submission. The risk assessment 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 ~~1~~30 business days of the Agency's or the Attorney General's request.

(1) **The disclosure of a Risk Assessment to the Agency or Attorney General shall not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.**

(2) **Risk Assessments shall be confidential and shall be exempt from disclosure under the California Public Records Act.**

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

Adopt all of the text in the following Article:

ARTICLE 11. AUTOMATED DECISIONMAKING TECHNOLOGY

§ 7200. When a Business’s Use of Automated Decision making Technology is Subject to the Requirements of This Article.

(a) A business that uses automated decision making technology in ~~**any of**~~ the following way~~**s**~~ must comply with the requirements of this Article:

(1) For a significant decision concerning a consumer. For purposes of this Article, “significant decision” means**, unless exempt by statute or as otherwise set forth in these rules,** a decision using **personal** information ~~**that is not subject to the exceptions set forth in Civil Code sections 1798.145, subdivisions (c)-(g), or 1798.146, subdivisions (a)(1), (4), and (5)**~~, 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 **in emergency situations**).

(A) Education enrollment or opportunity **means** ~~**includes**~~:

(i) Admission or acceptance into academic or vocational programs;

(ii) Educational credentials (e.g., a degree, diploma, or certificate); and

(iii) Suspension and expulsion.

(B) Employment or independent contracting opportunities or compensation **means**~~**includes**~~:

(i) Hiring;

~~**(ii) Allocation or assignment of work;**~~ salaries~~**, hourly or per-assignment compensation, incentive compensation such as bonuses, or other benefits (“allocation/assignment of work and compensation”);**~~

(iii) Promotion; and

(iv) Demotion, suspension, and termination.

(2) ~~**For extensive profiling of a consumer. For purposes of this Article, “extensive profiling” means:**~~

~~(A)~~ ~~**Profiling a consumer through systematic observation when they are acting in their capacity as an applicant to an educational program, job**~~

~~**applicant, student, employee, or independent contractor ("work or educational profiling");**~~

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

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

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

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

~~(B)~~ ~~**To establish individual identity;**~~

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

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

(b) A business that uses automated decisionmaking technology in any of the ways described in section 7200, subsection (a) is not required to comply with this Article where it processes personal information for self-testing to identify, mitigate, or prevent discrimination or otherwise ensure compliance with federal and state law.

(c) A business that uses automated decisionmaking technology in any of the ways described in section 7200, subsection (a) is not required to comply with this Article where it processes personal information for internal research and development.

(d) A business has 24 months from the effective date of these regulations to comply with requirements related to the use of automated decisionmaking technology.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

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

(a) ~~**A business that uses 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 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 emotion-assessment technology on its customer service calls to analyze the customer service**~~

~~**employees' performance at work must conduct an evaluation to ensure that it works as intended for this use and does not discriminate based upon protected classes.**~~

~~(A)~~ ~~**Alternatively, where a business obtains 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 the physical or biological identification or profiling works as intended for the business's proposed use and does not discriminate based upon protected classes.**~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

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

(a) ~~**A business that uses automated decisionmaking technology as set forth in section 7200, subsection (a), may must provide consumers with a Pre-use Notice. The 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 Pre-use Notice must:**~~

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

(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;**~~

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

(1) ~~**A plain language explanation of the specific purpose for which the business proposes to use 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.~~

(2) ~~A description of the consumer’s right to opt-out of ADMT and how the consumer can submit a request to opt-out of ADMT.~~

~~(A) If the business is not required to provide the ability to opt-out because it is relying upon the human appeal exception set forth in section 7221, subsection (b)(2), the business must instead inform the consumer of their ability to appeal the decision and provide instructions to the consumer on how to submit their appeal.~~

~~(B) If the business is not required to provide the ability to opt-out because it is relying upon another exception set forth in section 7221, subsection (b), the business must identify the specific exception it is relying upon.~~

(3) ~~A description of the consumer’s right to access ADMT with respect to the consumer and how the consumer can submit their request to access ADMT to the business.~~

~~(A) If the business proposes to use automated decisionmaking technology solely for training uses of automated decisionmaking technology as set forth in section 7200, subsection (a)(3), the business is not required to include a description about the right to access ADMT, nor how the consumer could submit their request to access ADMT to the business, as set forth in this subsection.~~

(4) ~~That the business is prohibited from retaliating against consumers for exercising their CCPA rights.~~

(5) ~~Additional information about how the automated decisionmaking technology works. The business may provide this information via a simple and easy-to-use method (e.g., a layered notice or hyperlink). The additional information must include a plain language explanation of the following:~~

~~(A) The logic used in the automated decisionmaking technology, including the key parameters that affect the output of the automated decisionmaking technology; and~~

~~(i) For purposes of this Article, “output” includes predictions, content, and recommendations (e.g., numerical scores of compatibility).~~

~~(B) The intended output of the automated decisionmaking technology and how the business plans to use the output, including the role of any human involvement. Illustrative examples follow:~~

~~**(i) If the business proposes to use the automated decisionmaking technology to make a significant decision concerning a consumer, the intended output may be a numerical score of compatibility, which a human may use as a key factor to make a hiring decision.**~~

~~**(ii) If the business proposes to use the automated decisionmaking technology for profiling for behavioral advertising, the intended output may be the placement of a consumer into a profile segment or category, which the business may use to determine which advertisements it will display to a consumer.**~~

~~(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 provide information that would compromise its use of automated decisionmaking technology for these security, fraud prevention, or safety purposes when complying with this subsection.**~~

~~(D)~~ ~~**If the business proposes to use automated decisionmaking technology solely for training uses of automated decisionmaking technology as set forth in section 7200, subsection (a)(3), the business is not required to include the additional information set forth in this subsection.**~~

(d) ~~**A business may provide a consolidated Pre-use Notice as set forth below, provided that the consolidated Pre-use Notice includes the information required by this Article for each of the business's proposed uses of automated decisionmaking technology:**~~

(1) ~~**The business's use of a single automated decisionmaking technology for multiple purposes. For example, an employer may provide a consolidated Pre-use Notice to an employee that addresses the employer's proposed use of productivity monitoring software, which the employer also intends to use as a primary factor in determining the employee's allocation/assignment of work and compensation as set forth in section 7200, subsection (a)(1)(B)(ii).**~~

(2) ~~**The business's use of multiple automated decisionmaking technologies for a single purpose. For example, a business may provide a consolidated Pre-use Notice to a consumer that addresses the business's proposed use of public profiling as set forth in section 7200, subsection (a)(2)(B). The consolidated Pre-use Notice may address the business's proposed use of location trackers and facial-recognition technology to ensure the physical safety of natural persons.**~~

(3) ~~**The business's use of multiple automated decisionmaking technologies for multiple purposes. For example, an educational provider may provide a consolidated Pre-use Notice to a new student that addresses the educational**~~

~~provider's proposed use of: (1) facial-recognition technology to authenticate the student and grant them access to a secured classroom, and (2) software that automatically screens a student's work for plagiarism.~~

(4) ~~The systematic use of a single automated decisionmaking technology. For example, a business may provide a consolidated Pre-use Notice to an independent contractor that addresses the business's methodical and regular use of automated decisionmaking technology to allocate work to its independent contractors, rather than the business providing a Pre-use Notice each time it proposes to use the same automated decisionmaking technology to the same consumers for the same purpose.~~

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.185, Civil Code.

§ 7221. Requests to Opt-Out of ADMT.

(a) Consumers have a right to opt-out of ADMT as set forth in section 7200, subsection (a). A business must provide consumers with the ability to opt-out of th**is**~~ese~~ use~~s~~ of automated decisionmaking technology~~, except as set forth in subsection (b)~~.

(b) A business is not required to **comply with requirements as set forth in section 7200 and 7222**~~, 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) **Without limiting the exemptions recognized in the statute,** ~~T~~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.

(2) **Without limiting the exemptions recognized in the statute, f**or any significant decision concerning a consumer as set forth in section 7200, subsection (a)(1), if the business provides the consumer with a method to appeal the decision to a qualified human reviewer who has the authority to overturn the decision ("human appeal exception"). To qualify for the human appeal exception, the business must do the following:

(A) The business must designate a human reviewer who is qualified to understand the significant decision being appealed and the consequences of the decision for the consumer. This human reviewer must consider the relevant information provided by the consumer in their appeal and may consider any other sources of information about the significant decision.

(B) The business must clearly describe to the consumer how to submit an appeal and enable the consumer to provide information for the human reviewer to consider as part of the appeal. The method of appeal also must be easy for the consumers to execute, require minimal steps, and comply with section 7004. Disclosures and communications with consumers concerning the appeal must comply with section 7003(a)–(b). The timeline for requests to appeal ADMT must comply with section 7021. Businesses must verify the consumer submitting the appeal as set forth in Article 5.

(3) For admission, acceptance, or hiring decisions as set forth in section 7200, subsections (a)(1)(A)(i), (a)(1)(B)(i), if the following are true:

(A) The automated decisionmaking technology ~~**is necessary to achieve, and**~~ is used solely for, the business's assessment of the consumer's ability to perform at work or in an educational program to determine whether to admit, accept, or hire them; and

(B) The business has conducted an evaluation of the automated decisionmaking technology to ensure it works as intended for the business's proposed use and does not discriminate based upon protected classes ("evaluation of the automated decisionmaking technology"), and has implemented policies, procedures, and training to ensure that the automated decisionmaking technology works as intended for the business's proposed use and does not discriminate based upon protected classes ("accuracy and nondiscrimination safeguards").

(i) Alternatively, where a business obtained the automated decisionmaking technology from another person, the business has reviewed that person's evaluation of the automated decisionmaking technology, including any requirements or limitations relevant to the business's proposed use of the automated decisionmaking technology; and has implemented accuracy and nondiscrimination safeguards.

(4) ~~**For allocation/assignment of work and compensation decisions as set forth in section 7200, subsection (a)(1)(B)(ii), if the following are true:**~~

~~(A)~~ ~~**The automated decisionmaking technology is necessary to achieve, and is used solely for, the business's allocation/assignment of work or compensation; and**~~

~~(B)~~ ~~**The business has conducted an evaluation of the automated decisionmaking technology and has implemented accuracy and nondiscrimination safeguards.**~~

(i) ~~**Alternatively, where a business obtained the automated decisionmaking technology from another person, the business has reviewed that person's evaluation of the automated decisionmaking technology, including any requirements or limitations relevant to the business's proposed use of the automated decisionmaking technology; and has implemented accuracy and nondiscrimination safeguards.**~~

(5) ~~**For work or educational profiling as set forth in section 7200, subsections (a)(2)(A), if the following are true:**~~

~~(A)~~ ~~**The automated decisionmaking technology is necessary to achieve, and is used solely for, an assessment of the consumer's ability to perform at work or in an educational program, or their actual performance at work or in an educational program; and**~~

~~(B)~~ ~~**The business has conducted an evaluation of the automated decisionmaking technology and has implemented accuracy and nondiscrimination safeguards.**~~

(i) ~~**Alternatively, where a business obtained the automated decisionmaking technology from another person, the business has reviewed that person's evaluation of the automated decisionmaking technology, including any requirements or limitations relevant to the business's proposed use of the automated decisionmaking technology; and has implemented accuracy and nondiscrimination safeguards.**~~

(6) ~~**The exceptions in this subsection do not apply to profiling for behavioral advertising as set forth in section 7200, subsection (a)(2)(C), or to training uses of automated decisionmaking technology as set forth in section 7200, subsection (a)(3). A business must provide the ability to opt-out of these uses of automated decisionmaking technology in all circumstances.**~~

(c) A business that uses automated decisionmaking technology as set forth in subsection (a) must provide two or more designated methods for submitting requests to opt-out of ADMT. A business must consider the methods by which it interacts with consumers, the manner in which the business uses the automated decisionmaking technology, and the ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of the business's use of the automated decisionmaking technology. At least one method offered must reflect the manner in which the business primarily interacts with the consumer. Illustrative examples and requirements follow.

(1) A business that interacts with consumers online **may** ~~**must, at a minimum,**~~ allow consumers to submit requests to opt-out through an interactive form accessible via an opt-out link that is provided **on their website or** in the **Privacy Policy** ~~**Pre-use Notice. The link must be titled Opt-out of Automated Decisionmaking Technology.**~~

(2) A business that interacts with consumers in person and online may provide an in-person method for submitting requests to opt-out in addition to the online form.

(3) Other methods for submitting requests to opt-out include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, and a form submitted through the mail.

(4) ~~**A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to opt-out of the business's use of automated decisionmaking technology because cookies concern the collection of personal information and not necessarily the use of automated decisionmaking technology. An acceptable method for submitting requests to opt-out must be specific to the right to opt-out of the business's use of the automated decisionmaking technology.**~~

(d) In lieu of posting an opt-out link, a business may include this additional opt-out on the webpage of the Alternative Opt-out Link in accordance with Section 7015.

(e) A business's methods for submitting requests to opt-out of ADMT must be easy for consumers to execute, must require minimal steps, and must comply with section 7004.

(f) A business must not require a consumer submitting a request to opt-out of ADMT to create an account or provide additional information beyond what is necessary to direct the business to opt-out the consumer.

(g) A business must not require a verifiable consumer request for a request to opt- out of ADMT set forth in subsection (a). A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer whose information is subject to the business's use of automated decisionmaking technology. However, to the extent that the business can comply with a request to opt-out of ADMT without additional information, it must do so.

(h) If a business has a good-faith, reasonable, and documented belief that a request to opt-out of ADMT is fraudulent, the business may deny the request. The business must inform the requestor that it will not comply with the request and must provide to the requestor an explanation why it believes the request is fraudulent.

(i) A business must provide a means by which the consumer can confirm that the business has processed their request to opt-out of ADMT.

(j) In responding to a request to opt-out of ADMT, a business may present the consumer with the choice to allow specific uses of automated decisionmaking technology ~~**as long**~~

~~**as the business also offers a single option to opt-out of all of the business's uses of automated decisionmaking technology set forth in subsection (a)**~~

(k) A consumer may use an authorized agent to submit a request to opt-out of ADMT as set forth in subsection (a) 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.

(l) Except as allowed by these regulations, a business must wait at least 12 months from the date the business receives the consumer's request to opt-out of ADMT before asking a consumer who has exercised their right to opt-out of ADMT, to consent to the business's use of the automated decisionmaking technology for which the consumer previously opted out.

(m) A business must not retaliate against a consumer because the consumer exercised their opt-out right as set forth in Civil Code section 1798.125 and Article 7 of these regulations.

(n) 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.

(o) If the consumer did not opt-out **prior to the commencement of processing**~~**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) Ceasing to **engage in such ADMT in connection with such consumer using the consumer's personal information**~~**process the consumer's personal information 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.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125 and 1798.185, Civil Code.

§ 7222. Requests to Access ADMT.

(a) Consumers have a right to access ADMT when a business uses automated decisionmaking technology as set forth in section 7200~~**, subsections (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 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 ADMT, a business must provide plain language ~~**explanations of**~~ **with** the following information to the consumer:

(1) The ~~**specific**~~ purpose 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 output of the automated decisionmaking technology ~~**with respect to the consumer**~~. ~~**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**~~ **for a significant decision**.

(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 **may** ~~**must**~~ include the role the output played in the business's decision~~ **and the role of any human involvemen**~~t.

(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 **may** ~~**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.**~~

(4) How the automated decisionmaking technology worked~~**with respect to the consumer**~~**, which may include the following**. ~~**At a minimum, this explanation must include subsections and (B):**~~

(A) How the logic **was intended to apply to the consumer**~~**, including its assumptions and limitations, was applied to the consumer**~~; and

~~(B) **The key parameters that affected the output of the automated decisionmaking technology with respect to the consumer, and how those parameters applied to the consumer.**~~

(C) A business also may provide **possible outputs** ~~**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) 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 provide information that would compromise its use of automated decisionmaking technology for these security, fraud prevention, or safety purposes.

(5) That the business is prohibited from retaliating against consumers for exercising their CCPA rights, and instructions for how the consumer can exercise their other CCPA rights. These instructions must include any links to an online request form or portal for making such a request, if offered by the business.

~~(A) **The business may comply with the instructions requirement by providing a link that takes the consumer directly to the specific section of the business's privacy policy that contains these instructions. Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain these instructions, so that the consumer is required to scroll through other information in order to find the instructions, does not satisfy the instructions requirement.**~~

(c) A business's methods for consumers to submit requests to access ADMT must be easy to use and must ~~**not use dark patterns**~~ **comply with Section 7004**. A business may use its existing methods to submit requests to know, delete, or correct as set forth in section 7020 for requests to access ADMT.

(d) A business must verify the identity of the person making the request to access ADMT as set forth in Article 5. If a business cannot verify the identity of the person making the request to access ADMT, the business must inform the requestor that it cannot verify their identity.

(e) If a business denies a consumer's verified request to exercise their right to access ADMT, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business must inform the requestor and explain the basis for the denial, unless prohibited from doing so by law. If the request is denied only in part, the business must disclose the other information sought by the consumer.

(f) A business must use reasonable security measures when transmitting the requested information to the consumer.

(g) If a business maintains a password-protected account with the consumer, it may comply with a request to access ADMT by using a secure self-service portal for consumers to access, view, and receive a portable copy of their requested information if the portal fully discloses the requested information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 5.

(h) A service provider or contractor must provide assistance to the business in responding to a verifiable consumer request to access ADMT, including by providing the business with the consumer's personal information it has in its possession that it collected pursuant to their written contract with the business, or by enabling the business to access that personal information.

(i) A business that used an automated decisionmaking technology **~~with respect to a consumer~~** more than **two** **~~four~~** times within a 12-month period may provide an aggregate-level response to the consumer's request to access ADMT. Specifically, for the information required by subsections (b)(2)–(4), the business may provide a summary of the outputs **~~with respect to the consumer~~** over the preceding 12 months**~~; the key parameters that, on average over the preceding 12 months, affected the outputs with respect to the consumer; and a summary of how those parameters generally applied to the consumer.~~**

(j) A business must not retaliate against a consumer because the consumer exercised their right to access ADMT as set forth in Civil Code section 1798.125 and Article 7 of these regulations.

(k) **~~Additional notice requirement regarding the right to access ADMT when a business used automated decisionmaking technology for certain significant decisions. A business that used automated decisionmaking technology to make certain significant decisions that were adverse to the consumer ("adverse significant decision"), as set forth in subsection (1) below, must provide the consumer with notice of their right to access ADMT as set forth in subsection (2) below, as soon as feasibly possible but no later than 15 business days from the date of the adverse significant decision.~~**

(1) **~~A significant decision concerning a consumer that was adverse to the consumer is a significant decision that:~~**

~~(A)~~ **~~Resulted in a consumer who was acting in their capacity as a student, employee, or independent contractor being denied an educational credential; having their compensation decreased; or being suspended, demoted, terminated, or expelled; or~~**

~~(B)~~ **~~Resulted in a consumer being denied financial or lending services, housing, insurance, criminal justice, healthcare services, or essential goods or services.~~**

(2) **~~The information that a business must provide to the consumer in this notice of their right to access ADMT must include:~~**

~~(A)~~ **~~That the business used automated decisionmaking technology to make the significant decision with respect to the consumer;~~**

~~(B)~~ **~~That the business is prohibited from retaliating against consumers for exercising their CCPA rights;~~**

~~(C)~~ **~~That the consumer has a right to access ADMT and how the consumer can exercise their access right; and~~**

~~(D)~~ **~~If the business is relying upon the human appeal exception set forth in section 7221, subsection (b)(2), that the consumer can appeal the decision and how the consumer can submit their appeal and any supporting documentation.~~**

(3) **~~If a business provides notice to consumers of adverse significant decisions in its ordinary course (e.g., a business ordinarily notifies consumers of termination decisions via email), the business may include the information required by subsection (2) in that notice, provided that the notice overall complies with the requirements of section 7003, subsections (a)–(b). Alternatively, a business may provide a separate contemporaneous notice of the consumer's right to access ADMT that includes the information set forth in subsection (2).~~**

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125 and 1798.185, Civil Code.