U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

January 14, 2025

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

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

The U.S. Chamber of Commerce ("Chamber") respectfully submits the following comments in response to the California Privacy Protection Agency's ("Agency") November 22 Notice of Proposed Rulemaking ("Proposed Rules").[1] The Chamber supports privacy protections for all Americans; however many of the Proposed Rules[2] exceed the Agency's statutory authority and its requirements, particularly those establishing requirements for privacy risk assessments and Automated Decision-making Technology ("ADMT") will be harmful to economic growth, innovation, and small businesses.

I. Introduction, Costs, and Burden on Interstate Commerce

The Chamber shares many of the same concerns as those expressed by the leading advocate and author of the California Privacy Protection Act ("CPPA" or "Act"). Agency Board Member Alastair Mactaggart stated during the Agency's November 2024 meeting that during board meetings in December 2023, March 2024, and July 2024, he "opposed these regulations" and "voice concern about their overreach, their lack of privacy protection, and the high likelihood of legal challenges" to them.[3] He also added that "at this point, the scope remains unchanged. And I believe this undermines privacy rather than protecting it."[4]

Furthermore, the Chamber, the world's largest business federation which represents all sizes of business in all fifty states, expresses concerns that the Proposed Rules on Cyber Audits, Risk Assessment, and ADMT impose an undue and impermissible burden on interstate commerce. Furthermore, the costs of the Proposed

[1] California Privacy Protection Agency—Notice of Proposed Rulemaking (Nov. 22, 2024) *available at* https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_notice.pdf.
[2] CALIFORNIA PRIVACY PROTECTION AGENCY – PROPOSED TEXT OF REGULATIONS (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations) (Nov. 2024) *available at* https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf.
[3] California Privacy Protection Agency Board Audio Transcription of Recorded Public Comment Session at 99 lines 5-11 (Nov. 28, 2024) *available at* https://cppa.ca.gov/meetings/materials/20241108_audio_transript.pdf.
[4] *Id.*

Rules outweigh the benefits.[5] According to the State of California's own Regulatory Impact Analysis ("RIA"), the Proposed Rules will impose a $3.5 billion direct cost on businesses "subject to the CCPA."[6] In comparison, the Congressional Review Act defines a federal "major rule" as one that has "an annual effect on the [United States] economy of $100,000,000 or more."[7]

The Agency's estimated $3.5 billion cost estimate significantly underestimates the true costs of the Proposed Rule as the RIA "anticipate[s] overall costs for these rules to be comparatively low compared to the other rulemaking given many of the requirements described in the proposed regulation were already required by existing laws, such as existing requirements under the CCPA and other state privacy laws."[8]

The Proposed Rules will have an outsized and significant impact on the national economy particularly with regard to AI. Between 2013 and 2023, private investment in AI has amounted to $335.2 billion[9] with many of the leading AI developers operating in California. The Proposed Regulations are the first in the nation to define on an economywide basis that using personal information for training generative AI is a "significant risk"[10] thus subjecting the technology to novel regulations only found in the Proposed Rules. One of these novel regulations is that generative AI data processing, among other practices, is prohibited if its benefits are outweighed by risks.[11] This contrasts with the RIA's description that costs of the Proposed Rules on ADMT will be mitigated because current laws cover most of the regulated activity already. Given this reality, it is very likely the true costs of the Proposed Rules significantly exceed the $3.5 billion estimated by the Agency and will have a significant and negative impact on the national economy.

Moreover, the RIA failed to account for the costs on businesses for providing opt-out rights for a wide range of everyday systems. Additionally, the RIA fails to assess the burdens on consumers if they have to sift through and make decisions about those opt-out rights. The RIA does not consider the harm to businesses of restricting their ability to personalize advertisements and offers to their own customers. Further, it is highly unlikely the Proposed Rules' cost will impact only businesses "subject to the CCPA."

---

[5] *See e.g.* Minnesota v. Clover Leaf Creamery Co, 449 U.S. 456. 471 (1981).
[6] Standardized Regulation Impact Analysis (Oct. 2024) *available at* https://cppa.ca.gov/meetings/materials/20241004_item6_standardized_regulatory_impact_assessment.
[7] 5 U.S.C. § 804(2).
[8] *Supra* n. 6 at 57.
[9] Charted, U.S. is the private sector A.I. leader, *Axios* (July 9, 2024) *available at* https://www.axios.com/2024/07/09/us-ai-global-leader-private-sector.
[10] *Supra* n. 2 at 103.
[11] *Id.* at 114.

II. Definitions

A. Artificial Intelligence

The Agency proposes defining "Artificial Intelligence." The CPPA should remove all AI terms and requirements from the Proposed Rule altogether as they expand beyond the scope of the ADMT mandate in the CCPA. The Agency's authority does not extend to regulating AI or creating obligations related to AI, as the CCPA's section on rulemaking authority does not explicitly mention AI. The inclusion of AI into the definition of ADMT is overly broad, encompassing nearly all imaginable software.

B. Automated Decision-making Technology

The Agency's Proposed Definition of ADMT is overly broad and not sufficiently tailored to focus on high-risk tools that operate without human oversight. Additionally, a technology that "substantially facilitates human decisionmaking" is not an automated decisionmaking technology and should not be treated as such. We strongly encourage the Agency to work with federal agencies, such as NIST, as well as industry representatives and standards development groups to determine appropriate definitions and terminology.

C. Behavioral Advertising

The Agency should strike the proposed the definition of "Behavioral Advertising," a term not included in the Act. The Agency proposes to define "behavioral advertising" as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity—both across businesses, distinctly-branded websites, applications, or services, and within the business's own distinctly-branded websites, applications, or services." This would be a significant expansion of the existing statutory definitions that would encompass first-party marketing and advertising activities.

The Proposed Rules would consider companies that use automated technology to conduct behavioral advertising as engaging in "extensive profiling" subjecting them to conduct a risk-assessment. At the same time, such conduct would be deemed by the Proposed Rules as a "significant risk."

The inclusion of behavioral advertising as a category of "extensive profiling" covered by the ADMT requirements is an incoherent approach to data protection, basic internet functionality, and serving consumers. Ads themselves are not "decision makers" - they are avenues for awareness that businesses use, across many communications channels, to promote their products and services. To run an ad, an advertiser sets up their creative, objective, and desired audiences, which are all

critical aspects of ad delivery, including delivery that involves ADMT. Conceptually, this is similar to an advertiser choosing to place their ad in a sports magazine, because of their estimation of interest to the community that reads these magazines. The Proposed Rules, as a regulation originating from the state's privacy statute, should be limited to the use of ADMT to make significant decisions about an individual. Instead, Proposed Rules follow a misguided approach of equating the use of ADMT in behavioral advertising to making a significant decision about an individual.

Additionally, the use of ADMT to conduct behavioral advertising would be subject to the Proposed Rule's Section 7200 opt-out right. Given the breadth of the behavioral advertising definitions, such an all or nothing approach to an advertising opt-out would deprive the consumers of small businesses of the benefits of personalized advertising. These tools also allow those small businesses to compete with larger companies. Sixty-six percent of small businesses nationwide have stated that losing the ability to personalize advertising will harm their operations, without achieving any meaningful consumer privacy goals.[12]

Finally, the proposed definition "behavioral advertising" would restrict first-party advertising. The Proposal's inclusion in this definition of "the targeting of advertising to a consumer based on the consumer's personal information obtained from . . . the business's own distinctly-branded websites, applications, or services" goes beyond the CCPA's text, which regulates "Cross-Contextual Behavioral Advertising" and carves out first-party data.[13] This statutory carve-out is important because it provides businesses the ability to market directly to their own customers on their own properties using data they have directly collected or inferred. For example, under the Proposed Rule's definition of "behavioral advertising" a restaurant or delivery service sending a promotion based on ordering history with that company would be "extensive profiling" subject to rigorous risk assessments and potential prohibitions. The result is that consumers will be inundated with irrelevant adds to provide them less value than personalized promotions.

D. Significant Decision

Both Articles 10 and 11 of the Proposed Rules define a "significant decision." Companies that use ADMT for a "significant decision" would be subject to the Proposed Rule's risk assessments, processing prohibitions, and consumer opt-out rights. An overly broad or ambiguous definition of "significant decision" could significantly impair innovation and the offering of affordable and tailored products and services to consumers.

---

[12] U.S. Chamber of Commerce, "Empowering Small Business: The Impact of Technology on U.S. Small Business," at 25 (Sept. 2024) *available at* https://www.uschamber.com/assets/documents/Impact-of-Technology-on-Small-Business-Report-2024.pdf.

[13] Cal. Civ Code § 1798.140(k).

Both Articles would define "significant decision" to mean "a decision… that results in access to, or the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice (e.g., posting of bail bonds), employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services (e.g., groceries, medicine, hygiene products, or fuel)."[14]

Consistent with a plain reading of the statute, the Proposed Rules should clarify how the existing access and opt-out rights apply in the context of ADMT. There is no basis in the statute for the Agency to create its own broad definition of "significant decision."

The focus of the Proposed Rules should be on risk assessments for high-risk ADMT that result in a denial rather than on low-risk uses such as administration of services such as health care or insurance. The proposed definition of "substantial decision" does not align with existing privacy law norms that focus on decisions that have a "material legal or similarly significant effect on the *provision or denial*" of certain benefits or opportunities.[15] For this reason and to harmonize with other states, we encourage the Agency to strike "results in access to, or" from the definition of "significant decision" in Sections 7150(b)(3)(A) and 7200(a)(1).

The Proposed Rules further define "[e]mployment or independent contracting opportunities or compensation" to include the "[a]llocation or assignment of work; salaries, hourly or per-assignment compensation, incentive compensation such as bonuses, or other benefits." This definition is also overbroad and captures HR administrative activities that are necessary parts of any job and are not considered to be high risk (i.e. allocation of work, administration and setting of payrolls). The definition of "employment or independent contracting opportunities or compensation" should align with activities that are generally considered high risk, such as recruitment, hiring, and promotion.

Many "automated decisions" in the independent contractor context involve things like surfacing the opportunity to engage with a given work or "gig" opportunity (e.g., delivering a given food order or offering a specific ride). Given the control independent contractors have to accept or deny any of these one-off opportunities (in contrast to being "hired" for ongoing employment), these "automated decisions" are not "high risk" and should not be considered "significant decisions" subject to these onerous regulations.

III. Privacy Risk Assessments (Article 10)

[14] Proposed Rule at §§7150(b)(3)(A), 7200(a)(1).
[15] *See e.g.* Colo. Rev. Stat. § 6-1-1303(10)

A. When a Business Must Conduct a Risk Assessment

The Proposed Rules required companies to conduct Risk Assessments for data processing that "presents significant risk to consumer privacy."[16] Among other things, the Proposed Rule would consider significant risks to consumer privacy to include the use of ADMT to make a significant decision or for "extensive profiling." Proposed Section 7150(b)(4) also would consider generative AI training and generation of a deepfake[17] to be a significant privacy risk. For the reasons stated hereinabove, the Chamber asserts that the Agency must make the necessary changes regarding its definitions of "significant decisions" and remove "behavioral advertising" from the term "extensive profiling."

We recommend striking Proposed Section 7150(b)(4) because the risk assessment obligations on AI exceed the CCPA's statutory authority because the Act focuses on ADMT's not AI generally. Training a model is not "automated decisionmaking" in its core—because the "training" does not involve a decision that has an impact on a specific consumer—and so should be out of scope for these rules. The rules aim to cover certain high-risk AI/ADMT applications, such as when used to make a significant decision. But here, the Proposed Rules would also cover developing tools that could provide substantial low-risk processing but would still be in the scope of the rule because they could one day be used for a higher risk application.

The actual use of ADMT/AI systems for these higher-risk applications would still be covered under these rules, and so extending obligations to the training of such tools is both misplaced and unnecessary. In other words, this training category greatly expands the type of technologies that are subject to these obligations because many if not all models "could" be used to make a significant decision. This "theoretical" approach is inconsistent with other risk-based frameworks focused on automated decision-making used to make a significant decision. It is also a different issue because training a model on personal data is different from making a decision about that person (or otherwise creating any risk for them).

---

[16] Proposed Rule § 7150(a).

[17] Regulation of deepfakes is beyond the remit of this privacy rulemaking and is best left to the legislature to address. In 2024, the California legislature passed multiple laws targeting deepfakes across a number of different issues, such as election information, intimate imagery, and publicity rights. Notably, none of these laws grant the CPPA any authority to enact regulations. One of the laws, AB 2839, was promptly challenged and enjoined in federal court as raising significant constitutional concerns. Accordingly, the CPPA's regulation of deepfakes would encroach on the legislature's authority and risks undermining First Amendment principles. Moreover, the draft rules diverge from other legal frameworks in how a "deepfake" is defined, creating further risks of arbitrary and capricious regulation. Accordingly, the CPPA should refrain from attempting to address deepfakes in the regulations and instead defer to the legislature on this topic.

In summary, the Chamber reiterates the position taken by Board Member Mactaggart when he said, "So how are these regs too broad? The risk assessment regs are too broad? Well, just to provide some examples, the definition of artificial intelligence, AI, is essentially all software…"[18] For the practical reasons stated by Mr. Mactaggart as well as the lack of CCPA statutory authority to regulate AI in this manner, we urge the Agency to strike Section 7150(b)(4).

B. The Prohibitions in Sections 7154 Are Impermissibly Vague and Should be Struck.

The Proposed Rule's Section 7154 places a new and potentially unconstitutionally vague prohibition that a "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 processing." For the following reasons, Section 7154 should be struck from the Proposed Regulations.

As drafted this prohibition effectively operates as a catchall outside the explicit obligations and requirements imposed upon business by CCPA. Importantly, the new prohibition on processing with alleged privacy risks does not follow the text of the CCPA itself. The Act gives the Commission authority to require businesses engaged in data processing with significant risks to submit risk assessments to the Agency:[19]

> with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, *with the goal of restricting or prohibiting the processing* if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public. Nothing in this section shall require a business to divulge trade secrets.

The Proposed Rules deem a wide variety of common practices in the digital economy– regardless of whether they in fact pose any meaningful "risks to privacy of the consumer" -- to pose significant risks including data sharing and sales; processing sensitive information; automated decisionmaking in lending, housing, insurance, criminal justice, healthcare; using data for personalized advertising; as well as training and operating AI. Effectively, the agency is saying the any meaningful use of personal information, other than collection, poses a significant risk to consumer privacy and

[18] *Supra* n. 3 at 100.
[19] Cal Civ. Code § 1798.185(15(B) (emphasis added).

should be subject to risk assessments and a vague balancing test to determine the legality of core business practices in the digital economy. Such an approach will chill investment and innovation because businesses will be subject to a highly subjective and unknowable standard if the Agency second guesses whether a business's data processing practices benefits are outweighed by personal or societal risks.

According to the United States Supreme Court[20],

> It is a basic principle of due process that an enactment is void for vagueness if its prohibitions are not clearly defined. Vague laws offend several important values. First, because we assume that man is free to steer between lawful and unlawful conduct, we insist that laws give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly. Vague laws may trap the innocent by not providing fair warning. Second, if arbitrary and discriminatory enforcement is to be prevented, laws must provide explicit standards for those who apply them. A vague law impermissibly delegates basic policy matters to policemen, judges, and juries for resolution on an *ad hoc* and subjective basis, with the attendant dangers of arbitrary and discriminatory applications.

Proposed Section 7154 as drafted would violate due process for companies who have no discernible standard other than to weigh the benefits and risks of data processing practices. Further complicating this vague standard is the fact that Section 7152 requires companies to identify in a granular manner data processing benefits to consumer and expected financial profits when possible.[21] Yet, the Agency contemplates that businesses will identify privacy risks to consumers as broad and unquantifiable as chilling expression, anxiety, and stigmatization.[22]

Other so-called "privacy" risks identified by the Agency include a broad range of potential "economic harms," like "charging consumers higher prices" or "compensating consumers at lower rates." These are not "risks to privacy" in the ordinary sense of the word (which, per the CCPA, are the only types of risks the CPPA can consider). Rather, the regulation of these broad "economic harms" is well outside the CPPA's authority and properly within the purview of other regulators. If this part of the rules is not changed, the rules would give the CPPA (or the AG) the authority to shut down business activities that, in the agency or AG's judgment, pose a greater risk of "economic harm" to consumers or workers than the potential financial benefits. That is not privacy regulation – that is a potentially sweeping form of commerce, labor, and competition regulation.

---

[20] *Grayned v. City of Rockford,* 408 U.S. 104, 109 (1972).
[21] Proposed Section 7152(a)(4).
[22] *Id.* at § 7152(a)(5).

The primary purpose of a Risk Assessment should be for companies to proactively consider privacy as they build, develop, and implement their data processing practices. While the Proposed Rules in Section 7152 require companies to weigh the benefits of data processing posing a significant risk against the risks to individuals and society, Section 7154 fails to state that the Agency will not second guess the results of the Risk Assessment and use instead its own judgement to determine whether an activity should be prohibited. This is important because the Proposed Rules require businesses to conduct extensive risk and benefit analyses without any clear standards to determine whether individual or societal risks outweigh the benefits of what is pre-determined by the Agency in the Proposed Rules to be a significant risk under Section 7150(b).

As the Agency provides no clear formula for its risk assessment determinations, if two companies effectively conduct the same processing with "significant risks" yet come to different conclusions whether benefits outweigh risks, as drafted the Agency could impose blanket prohibitions on all industry that go beyond the scope of CCPA. Alternatively, under this scenario, the CCPA would be applied unequally across industry.

Without clear indication that the Agency will honor companies' conclusions in their Risk Assessments, the Proposed Rules impose on companies a requirement to establish a record for the Agency to arbitrarily prohibit legitimate processing by weighing metrics which are akin to comparing apples (i.e. economic benefits) and oranges (i.e. intangible harms like reputational risks). The Proposed Rules fail to enumerate a clear standard to determine how a data processing practice's benefits are not outweighed by individual and societal risks, particularly when there are not quantifiable metrics for many of the Agency's contemplated privacy harms. Such authority gives the Agency both legislative and enforcement authority if it chooses to replace its own judgement for what is determined by a company in its Risk Assessment.

Even if the Agency honors a business's Risk Assessment which shows benefits may be outweighed by risks, the Proposed Rules are not narrowly tailored to match the statutory text of the Act. The CCPA states that Risks Assessments should be submitted "with the goal of *restricting or* prohibiting the practice." Instead, the Agency has arbitrarily determined that most meaningful and common data practices and analytics outside of data collection are subject to outright prohibition, not mere restriction, if it believes a privacy risk has outweighed benefits. For example, some data practices could be more harmful to a more sensitive or vulnerable individual yet provide innovative insights on how to solve societal problems for that same category of sensitive or vulnerable people. Given competing interests, benefits, and risks, a data practice might be more suitable for restriction to prevent individual harm that

outright prohibition, but the Proposed Rules provide only for outright prohibition, allowing for only the most aggressive reading of the CCPA and expressly excluding the more tailored statutory option.

Alternatively, if the Agency does intend to determine on its own whether to prohibit practices with substantial risk that outweighs benefits, it should limit the considerations in Risk Assessments or provide much more granular guidance for metrics that are quantifiable and not abstract or subjective standards like chilled expression or anxiety.

Finally, the CCPA states that Risk Assessments should be submitted with the "*goal* of restricting or prohibiting the practice." Given the many difficult to compare and unquantifiable metrics as well as the competing societal, individual, business, customer-supporting, and innovation interests, the statute does not explicitly state the Agency *must* restrict or prohibit processing practices. The *goal* of Risk Assessments could be to encourage companies to voluntarily restrict or stop their own practices to protect their customers, assets, and reputation. From a government perspective, if a *goal* of the Act is to enact further legal restrictions or prohibitions on business, it would be more appropriate for the Agency to be informed by Risk Assessments to make recommendations to the California legislature for amendments to CCPA that deal with discrete risky data practices.

C. Timing and Submission of Risk Assessment to the Agency

The Agency Proposes in Section 7157(a) to require businesses to submit Risks Assessments to the Agency within 24 months of the effective date of the regulations and then every year after. No other jurisdiction in the United States requires such a proactive submission schedule.[23] To harmonize with other state laws, the Agency should require an initial impact assessment and submission upon request by the Agency or Attorney General in the context of an investigation.

Proposed Section 7157(d) would require businesses to turn over their unabridged Risk Assessments to the Agency or Attorney General within ten days. Given the broad scope of the assessments, we suggest that response time should be thirty days.

The Proposed Rules at Section 7155(a)(3) would also require companies to conduct a new risk assessment "immediately" upon a "material change" to a processing activity. We would encourage the Agency to require this new assessment to be completed done within a "reasonable time" instead.

[23] *See e.g.* Colorado Revised Statutes § 6-1-1309.

We also urge the Agency to allow for interoperability of other privacy impact assessment requirements in other states. For example, if a submission of a company's Privacy Impact Assessment under the Colorado Privacy Act adequately addresses California's requirements, companies should not be required to complete and submit duplicative assessments.

IV. Cybersecurity Audits (Article 9)

A. Article 9 Generally

Article 9[24] of the Proposed Rules would require businesses that process personal information in such a way that poses a "significant risk" to an individual's privacy or security to conduct and submit an annual cybersecurity audit. The cybersecurity requirements proposed in sections 7120 through 7124 represent a bold departure from standard cybersecurity requirements currently employed throughout the U.S. industry landscape and will impose a possibly insurmountable compliance burden on businesses with operations in California, particularly small and medium-sized businesses. At a foundational level, the Chamber believes that any proposed cybersecurity law or regulation must be harmonized with existing regulations to the greatest extent possible and be based on risk.

Furthermore, we question the statutory authority of the Agency to impose specific cybersecurity requirements and practices on businesses. Indeed, Section 1798.185(a)(14)(A) of the CCPA allows the Agency to issue regulations exclusively with respect to an audit:

> *"Perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent. The factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities."*[25]

This language provides the Agency authority to require cybersecurity audits with a defined scope, but it does *not* provide the Agency any authority to require a business to establish specific security processes.

That being stated, the following represent comments, questions, and suggested changes to Sections 7120 through 7124 of the Agency's proposed regulations.

B. Section 7120 – Requirement to Complete a Cybersecurity Audit

[24] Supra n.2 at 91.

[25] https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Section 7120 introduces the annual cybersecurity audit requirement and outlines the applicability threshold under which businesses must operate. As written, the proposed regulations suppose that any business that processes personal information poses a significant risk to consumer security. This threshold is too low, both in terms of the breadth of businesses as well as the type of activities deemed a "significant risk." The Agency should instead focus its audit requirements on activities that pose significant risk to the most sensitive data. At the very least, the Agency should refer to its own text in Article 10, Section 7150, which acknowledges the following as presenting a significant risk: selling or sharing personal information, processing sensitive personal information, using ADMT to make significant decisions, or using personal information to train ADMT and/or artificial intelligence[26]. While still broad, this language would at least provide a degree of clarity to businesses considering the applicability of the proposed regulations.

C. Timing for Requirements for Cybersecurity Audits

Section 7122 requires that the cybersecurity audits outlined in the proposed regulations occur no more than every 12 months following a business' initial audit[27]. This requirement is inconsistent with all other U.S. privacy laws regarding risk assessment and Data Protection Impact Assessments (DPIA) and should be amended to a less frequent occurrence, such as once every three years. The Agency should also consider allowing businesses to complete an initial audit and subsequently certify that said audit remains valid going forward.

D. Thoroughness and Independence of Cybersecurity Audits

In Section 7122, the proposed regulations outline requirements for businesses to ensure that cybersecurity audits are both thorough and independent. Many of these requirements, particularly those found in Section 7122(a)[28], conflict with existing federal cybersecurity requirements and guidelines, including requirements related to the nature, independence, and characteristics of internal auditors; the requirement that the audit be reported directly to the board; the requirement that the board have direct responsibility over the auditor's performance and compensation; requiring employee training after every data breach; and other prescriptive requirements. In general, we request that requirements concerning the use of an internal auditor be more flexible and harmonized with existing regulations.

Similarly, the prescriptive requirements for the cybersecurity audits outlined in Section 7122(e) should be harmonized with existing audit requirements and standards,

[26] *Id.* at 103.
[27] *Id.* at 91.
[28] *Id.* at 92.

such as the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF)[29], international frameworks, and other existing cybersecurity standards and requirements already utilized by and familiar to the business sector. If a business reasonably conforms with these standards, then they should be considered in compliance with the Agency's requirements.

An issue of particular concern for businesses are the requirements involving a given business' board of directors, such as language in Section 7122(i)[30] and Section 7124(c)[31] that require a member of a business' board of directors to sign a statement certifying specific facts of the audit as outlined in Section 7123. The Chamber asserts that a board should provide guidance on the organization's strategic direction and plans, monitor management's performance in implementing such plans, and account for the institution's risk appetite, resources, and controls. However, a board of directors should *not* be expected to serve as technical cybersecurity risk management practitioners themselves. Therefore, the Agency should revise the proposed governance requirements to recognize the role that boards play in a business' structure. The board should be allowed to focus on the overall enterprise risk management of the business and leave in-depth reviews and approvals of cybersecurity policies for the cybersecurity experts who possess the capacity to manage those policies daily. This is also true for the proposed requirement to have the board evaluate performance and set the compensation for an internal auditor.

E. Scope of Cybersecurity Audit

Section 7123 describes the various aspects of the cybersecurity audits and includes specific requirements for businesses seeking to comply with the proposed regulations.[32] The details outlined in this section are more extensive and prescriptive than any other government requirements at the federal or state level and are not based on an existing specific cybersecurity framework, nor do they refer to specific standards. Again, the requirements outlined in Section 7123 must be harmonized with existing federal standards to ensure as little a burden as possible for businesses already employing sufficient cybersecurity practices.

In Section 7123(b)[33], the Agency lists the cybersecurity components and requirements that businesses must address and employ to comply with the proposed regulations. As stated above, the Chamber questions the statutory authority of the Agency to require specific cybersecurity practices for businesses. Even with the

[29] NIST Cybersecurity Framework (Feb. 26, 2024) *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.
[30] *Supra* n. 2 at 94.
[31] *Id.* at 102.
[32] *Id.* at 94.
[33] *Id.*

appropriate statutory mandate, the practice of basing regulation around specific cybersecurity requirements is an inappropriate method of regulation and generally unproductive. Further, such a method neglects to acknowledge the ever-changing nature of the current cybersecurity environment as well as the need for businesses to have the flexibility to protect digital infrastructure in the most appropriate manner. Should the Agency continue down this route, it should at least realign these requirements with existing federal cybersecurity frameworks and ensure that this program remains based on risk, rather than prescriptive, requirement-based regulation.

Additionally, it is worth noting that many of the listed cybersecurity requirements do not appear to be limited to the protection of personal data. For example, the requirements contained in Section 7123(b)(2)(F)[34] deal with the secure configuration of hardware or software. The Agency must clarify that these requirements are limited to situations in which personal data is involved. Without such language, these requirements could be read to require an enterprise-wide assessment and retooling, which would be needlessly complex and burdensome as well as outside the statutory purview of the Agency.

Further, in Section 7123(b)(2)(Q)[35], the Agency defines "security incident" as:

> *"...an occurrence that 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."* [36]

This definition is problematic for multiple reasons. For one, the wording "or potentially jeopardizes" would require compliance over an incident that has not yet occurred, which is unnecessarily vague and will demand thorough analysis of any potential threat that has yet to materialize. Furthermore, the phrase "...or availability of a business's information systems 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..." could be read to expand the proposed regulations to a business' entire information system, which goes well beyond the Agency's statutory authority, perceived or otherwise. This definition must be amended to clarify

[34] *Id.* at 97.
[35] *Id.* at 99.
[36] *Id.*

that only information systems dealing with sensitive personal data are covered in this language as well as remove any vagueness related to the types of incidents against which businesses must protect. As an alternative, the Chamber suggests using the "breach of the security of the system" definition contained in California's general breach notification statute (1798.82(g)), which reads:

> *(g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.*[37]

Section 7123(c)(4) requires businesses to include the *"...title(s) of the qualified individuals responsible for the business' cybersecurity program."*[38] For larger organizations, this requirement could include hundreds of employees. This requirement should be focused on those within a business who are "primarily" responsible for a business' cybersecurity program.

Section 7123(e) states:

> *If the business was required to notify any agency with jurisdiction over privacy laws or other data processing authority in California, other states, territories, or countries of 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 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.*[39]

As written, this language would require a business with operations in California to include in the cybersecurity audit any personal data breach occurring in any jurisdiction globally, assuming the jurisdiction required a breach notification. This requirement exists far outside the Agency's purview and represents a huge expansion of state authority. The Agency lacks the authority to regulate activities wholly outside of California. Further, in the case

[37] Cal. Civ. Code § 1798.82(g).
[38] *Supra* n. 2 at 100.
[39] *Id.* at 101.

of some financial institutions, visitorial rights restrict the ability of states to inspect, examine, and generally regulate said institutions in this manner. As such, we strongly urge that this requirement be removed.

A consistent request made both in this comment submission and by industry in general is the harmonization and alignment of cybersecurity regulations. To that end, the Agency provides some flexibility with existing cybersecurity regulations in Section 7123(f)[40] where it clarifies that a business is "not required to complete a duplicative cybersecurity audit" if the audit "meets all of the requirements of this article." While the intention of this language is generally appreciated, it does not go far enough and, in certain cases, will inadvertently create additional burdens for businesses seeking compliance. For example, the language requires that businesses "specifically explain how the [external] cybersecurity audit…meets all of the requirements set forth in this article." Instead of avoiding duplication, this language adds further burdens to businesses executing cybersecurity measures while already managing a duplicative, overlapping, and at times contradictory regulatory framework.

V. Automated Decision-making Technology (Article 11)

A. Article 11 Generally

The Chamber wishes to express its concerns regarding the proposed rule, specifically the Automated Decision-Making Technology (ADMT) sections, which exceed the agency's statutory authority. We have significant concerns about this duplicative effort, as it overlaps with several ongoing regulatory initiatives in California. Notably, the California Civil Rights Department (CCRD) has proposed modifications to employment regulations concerning automated decision systems within the employment context. Concurrent regulatory initiatives from different agencies create significant challenges for the business community, leading to unnecessary confusion and potentially conflicting regulations. We believe provisions of Article 11 exceeds the authority granted to the Agency under the CCPA.

The Chamber believes that the CPPA should halt further efforts to regulate ADMT until it has been granted statutory authority to proceed with such rulemaking. We offer the following feedback on Article 11: Automated Decision-Making Technology (ADMT).

B. Scope of ADMT Regulation

[40] *Id.*

The Agency's expansion of the scope of ADMT regulation is problematic and potentially duplicative. We are particularly concerned about the expansion into areas such as generative AI and behavioral advertising, which extend beyond the scope of the voter-approved statute. These advertisements are not decisions but instead means to raise consumer awareness and personalize experiences.

Moreover, the activities covered by Article 11 sweep extremely broadly. For example, Proposed Sections 7220 and 7222 are tantamount to full-scale AI Impact Assessment legislation as opposed to mere access rights which were contemplated in the text of CCPA.

C. Broad Definition of ADMT

As we highlighted hereinabove, we are deeply concerned that the definition of ADMT is overly broad and not sufficiently tailored to focus on high-risk tools that make significant decisions about consumers and operate without human oversight.

We urge you to reconsider concerns raised by Mr. Mactaggart with the Proposed Rule's definition of ADMT[41] that "our definition of ADM includes the use of almost any computerized technology in a way that describes how humans have used computers for 30 or 40 years." The author of the Act's ADMT provision is stating the intent is not to create new rules around specific technology but in a technology neutral way address privacy harms.[42]

D. Opt-Out Provisions

The Agency's requirement for consumers to have the "Right to Opt-Out," irrespective of the technology's risk level, is highly problematic and impractical. Providing these opt-out rights is impractical, particularly because of the expansive range of systems that are captured by the overbroad definition of ADMT. The result is that businesses must evaluate a wide range of systems – many of which have little or no connection to consumer privacy risks -- to determine when an opt-out process needs to be built or whether an exception to the opt-out exists. We are also concerned about the requirement for businesses to disgorge personal information previously processed upon a consumer's opt-out request, as this could lead to significant operational challenges and may be unworkable.

We recommend that only verifiable requests be subject to opt-out requirements, as well as a need for an exception to be added for critical security and fraud tools. These will ensure user preferences are accurately followed, and companies can proactively protect consumers from unwarranted security and fraud

[41] *Supra* n. 3 at 100.
[42] *Id.*

concerns. This is why, like CCPA and other state privacy laws, they have substantial exemptions for opt-out provisions for activities that prevent and secure against fraud. Section 7221(b)(1)(B) should be strengthened to clarify that the opt-out right does not apply to activities that are aimed "to resist, prevent, and detect, malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions; or[...]."

E. Pre-Use Notice Requirements

The Proposed Rules would require businesses to explain detailed uses and purposes for ADMT, which is excessively burdensome. Additionally, the prohibition of standard business terms such as "to improve our services" is overly restrictive. We are concerned that pre-use notice requirements could be construed as requiring companies to disclose trade secrets and sensitive business information. The overbroad definition of ADMT will bring in a wide range of everyday business systems that will overwhelm consumers and make it harder for consumers to find important vital information. Furthermore, we believe the agency should provide clarification that any requirements set forth within the regulations is prospective and not retroactive and excludes third parties which have no ability to provide notice.

F. Clarity on Exemptions

The Chamber expresses concern that the current draft of the rule does not align with the established precedent of exemptions under the California Privacy Rights Act (CPRA). We respectfully request that any revised draft maintain consistency with the statutory language and explicitly state that the exemptions provided under the CPRA are also applicable to the ADMT. For example, the "opt-out" provision not operational because of the lack of a carve out to prevent fraud, but because that the services that a firm provides and offers in many cases may only be through "ADMTs."

G. ADMT Access Rights

The Chamber has significant concerns about the requirements for responding to the new "right to access ADMT," as they are overly broad and burdensome for businesses. We recommend that §7222(b) be simplified and aligned with existing legal language. Additionally, the requirement to inform consumers about alternative actions they could have taken to secure a different decision is excessively prescriptive and not consistent with existing laws, which already provide consumers with substantial information rights.

The obligations imposed on service providers to assist businesses with ADMT requests are unnecessary and should be eliminated, as they are already covered by

current CCPA obligations regarding data subject rights. Therefore, §7222(h) should be deleted.

- Prescriptive requirements for using ADMT with a consumer more than four times in 12 months are unnecessary and should be eliminated. Thus, §7222(i) should be deleted.
- The CCPA already ensures that consumers have the general right not to be retaliated against for exercising data subject rights. Therefore, §7222(j) is duplicative and unnecessary and should be deleted.
- Section 7222(k) introduces an additional notice requirement for certain "adverse significant decisions," including "financial or lending" decisions. These additional notice requirements are highly prescriptive and burdensome and should be deleted.

VI. Definitions Broadly

The Proposed Regulations would define "sensitive personal information" ("SPI") to include "[p]ersonal information of consumers that the business has actual knowledge are less than 16 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."[43] Such data would be subject to the full CCPA's consumer data minimization and disclosure limitation rights.

We are concerned that defining personal information of users age thirteen and older would undermine the ability of business to tailor their products and services to deliver age-appropriate experiences for minors. We urge the Agency to remove this overly broad designation.

VII. Revisions to Current Regulations

Certain proposed revisions to Article 3 conflict with other areas of the CCPA, do not consider the operational impact, and create a compliance burden without providing consumers with significantly greater protection. Specifically:

- **Method for submitting CCPA requests and obtaining consent (§7004(a)(2)(A))** – The symmetry in choice requirement does not reflect the fact that there is an inherently different amount of work that is needed in order to opt-in (which can be done by clicking a single link) versus to opt someone out of sharing their information – for example, once they click the link, the business still needs to verify them. The regulations should revert to how they were previously drafted and require symmetry, but not limit opt outs to the "same or fewer" steps.

[43] Proposed Rule §7001(ccc)(4).

- **Method for submitting CCPA requests and obtaining consent (§7004(a)(4)(C)** – The prohibition on using general terms of acceptance conflicts with the CCPA which requires businesses to provide consumers with a notice at collection. This prohibition does not relate to or address dark patterns and should be deleted.

- **Requests to Delete, Know, Opt-Out of Sale/Sharing (§7022(g)(5), §7024(e)(3), §7026(e))** – Requiring businesses to provide consumers a disclosure that they can file a complaint with the CPPA even if there are valid reasons for denial is counterintuitive and will result in unfounded complaints from consumers who interpret the complaint disclosure as a required next step. **Therefore, this provision should be removed.**

- **Requests to Correct (§7023(f)(3)(g)** – the draft regulations require that, if a business denies a right to correct it must then inform the consumer that it will note both internally and to third parties to whom is disclosure the personal information that the accuracy of the PI is contested. This provision goes beyond the scope of the law and should be deleted. The CCPA provides for an obligation to correct and exception to that obligation. The CPPA should not place additional and burdensome requirements on businesses that will not be practical to operationalize.

- **Requests to Know (§7024(d)(2)** – the draft regulations require businesses to provide consumers with a way for consumers to confirm that SPI information is the same as what the consumer expects it to be, while also prohibiting businesses from disclosing such SPI. It is unclear to comply with this requirement without disclosing such information.

- **Revisions to Sections 7022, 7024, and 7026** would require businesses to inform consumers they can file a complaint with the CPPA. However, disclosure that they consumers can file a complaint with an Agency even if there are valid reasons for denial is counterintuitive and will result in unfounded complaints from consumers who interpret the complaint disclosure as a required next step.

VIII. Insurance Companies

The Agency Proposes defining insurance companies for the purposes of the rules as persons subject to the California Insurance Code. Proposed Article 12 would impose the obligations and requirements of the CCPA to insurance companies with regard to any personal information not subject to the Insurance Code and its regulations. For example, those insurance companies "shall comply with the CCPA for personal information that is collected for purposes not in connection with an insurance transaction, as that term is defined in Insurance Code, section 791.02."

Insurance companies are subject to more laws and regulations that merely the Insurance Code. We proposed that the Agency strike the language stating "For example, those insurance companies shall comply with the CCPA for personal information that is collected for purposes not in connection with an insurance transaction, as that term is defined in Insurance Code, section 791.02" to align with this reality and avoid duplicative regulation.

If you have any questions, please contact Jordan Crenshaw at jcrenshaw@uschamber.com. For questions concerning Article 9, please contact croberti@uschamber.com.

Sincerely,

Jordan Crenshaw
Senior Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce

Christopher D. Roberti
Senior Vice President
Cyber, Space, and National Security
Policy Division
U.S. Chamber of Commerce