BEFORE THE
CALIFORNIA PRIVACY PROTECTION AGENCY
Sacramento, CA 95814

In the Matter of

Notice of Proposed Rulemaking Regarding Updates to Existing CCPA Regulations; Cybersecurity Audits; Risk Assessments; Automated Decisionmaking Technology, and Insurance Companies

COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION

The Consumer Technology Association® ("CTA")®[1] respectfully submits these comments in response to the California Privacy Protection Agency's ("CPPA") Notice of Proposed Rulemaking soliciting comments on updates to existing CCPA Regulations, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology, and Insurance Companies. Specifically, CTA submits comments on (1) the impact that the CPPA's proposed rules concerning automated decisionmaking technologies ("ADMTs") will have on businesses that use or develop ADMTs and (2) the key impacts the CPPA's proposed rules regarding cybersecurity audits will have on businesses more broadly.

CTA's membership includes over 1200 companies from every facet of the consumer technology industry, including manufacturers, distributors, developers, retailers, and integrators, with 80 percent of CTA members being start-ups or small and mid-sized companies. CTA also owns and produces CES® – the most powerful tech event in the world.

CTA member companies continue to lead in the development and implementation of artificial intelligence ("AI") -enabled systems and solutions that are having a positive impact on human and societal development: promoting inclusive growth, improving the welfare and well-being of individuals, and enhancing global innovation and productivity.[2] Perhaps the leading federal agency focused on AI governance and risk management, the National Institute of Science and Technology ("NIST"), has noted

[1] As North America's largest technology trade association, CTA is the tech sector. Our members are the world's leading innovators—from startups to global brands—helping support more than 18 million American jobs. CTA owns and produces CES®— the most powerful tech event in the world.

[2] For example, Google has worked with the ALS Therapy Development Institute to use AI technologies to improve the lives of people with ALS. *Google and ALS TDI: Working Together to Use Data to Improve the Lives of People with ALS*, March 3, 2022, https://www.als.net/news/google-and-als-tdi/. Microsoft's AI for Good Lab is exploring AI solutions to pressing issues such as curbing malnutrition and empowering blind and low-vision individuals to easily navigate their world. *See* AI For Good Lab, https://www.microsoft.com/en-us/research/group/ai-for-good-research-lab/.

that "new AI-enabled systems are revolutionizing and benefitting nearly all aspects of our society and economy – everything from commerce and healthcare to transportation and cybersecurity."[3]

CTA supports efforts to encourage the responsible development of AI, including the need for narrowly focused notice, opt-out and transparency rules for businesses using ADMTs in California. Specifically, CTA has supported efforts at the federal level to develop voluntary risk-based frameworks to address potential AI risks, while enabling stakeholders to maximize the benefits of this technology. Some of those initiatives, such as NIST's AI Risk Management Framework, have led to a flexible and voluntary risk management framework that facilitates organizations' management of potential AI risks, including those that may be implicated by the use of automated decisionmaking systems.[4]

In the past three years, regulators from various sectors and levels of government have begun adopting laws and regulations aimed at addressing potential harms of AI systems. This has resulted in an emerging patchwork of requirements for businesses that develop or deploy AI-enabled systems and solutions (many of which would be classified as ADMTs under the proposed regulations). The CPPA should ensure that its proposed rules do not extend beyond the specific mandates of the CCPA (as amended by the CPRA), or conflict with existing requirements. Specifically, the CPPA should ensure that its final privacy regulations governing ADMTs align with the statutory mandate to develop focused notice, opt-out and transparency rules, and similar privacy obligations that other states have created with regard to these technologies. Creating novel obligations for the development and use of ADMTs would impose unnecessary burdens on businesses operating in California that would undermine further innovation in this critically important area.

The CPPA should also narrow its approach to regulating ADMTs to ensure that it targets only the highest-risk uses of ADMTs for decisions concerning individuals, and does not stifle innovation by creating unnecessary regulatory duties and obligations, particularly for small- and medium-sized businesses. By the agency's own analysis, up to 52,000 businesses may be regulated by the proposed regulations of ADMTs, including up to 27,000 small businesses, and the potential compliance costs of the ADMT regulations that may be borne by businesses is staggering: upwards of $1.4 billion.[5] The CPPA must not move forward without serious consideration of the impact of these costs on businesses operating in California, especially smaller and medium-sized enterprises. Significant revisions to narrow the scope and reach of these draft regulations would be an appropriate measure to lessen the burden of these regulations.

The CPPA should ensure that existing business management structures and oversight by the board of directors are not negatively impacted by cybersecurity audit requirements. Any audit requirements should also leverage existing cybersecurity frameworks and audit controls to allow for flexible implementation.

Finally, the CPPA should allow businesses a reasonable time to comply with any new regulations. The complexity and novelty of these proposed regulations will require businesses to develop

---

[3] *Artificial Intelligence*, NIST, https://www.nist.gov/artificial-intelligence.

[4] *Comments of the Consumer Technology Association*, AI Risk Management Framework, at 2 (filed Sept. 29, 2022), https://www.nist.gov/system/files/documents/2022/11/16/Consumer%20Technology%20Association%20%28CTA%29.pdf.

[5] *Standardized Regulatory Impact Assessment: California Privacy Protection Agency*, October 2024, https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_impact.pdf.

and implement technical solutions that will take time and significant resources to develop and operationalize. As such, the CPPA should ensure an adequate implementation period of at least twenty-four months between the date the regulations are finalized and the date on which they become enforceable.

I. THE CPPA SHOULD ENSURE THAT ANY NEW REGULATIONS DO NOT CONFLICT WITH EXISTING STATUTES, REGULATIONS AND VOLUNTARY COMMITMENTS

The CPPA should ensure that its proposed regulations do not overburden businesses that develop or deploy ADMTs. As explained below, these businesses must already contend with a growing patchwork of statutes, regulations, and commitments that apply to ADMTs.

Numerous state privacy laws regulate "profiling" in furtherance of decisions that have legal or similarly significant effects. These state laws generally define "profiling" as the use of ADMTs to process personal data to make predictions about or analyze certain personal aspects of individuals.[6] California's ADMT regulations should avoid conflicting with or extending further than other states' regulations of similar technology.

California has been active in this area in other ways. The legislature recently enacted measures governing the development and deployment of AI models, including AB 2013, which requires developers of generative AI systems to publicly disclose a summary of the datasets used in the development of their systems. The CPPA's proposed pre-use notice obligations, which would require entities that train models for covered purposes to disclose the categories of personal information used to train the models, would substantially overlap with the requirements of AB 2013. In addition, the California legislature is likely to consider additional proposals in the upcoming legislative session and may pass new measures intended to govern and regulate AI, and by extension many automated decisionmaking technologies. To ensure that it does not interfere with legislative efforts to regulate in this area, the CPPA should narrowly focus instead on implementing its specific grant of authority to issue privacy rules regarding "access" and "opt-out" rights in the context of ADMTs.

New state AI consumer protection laws like those recently passed in Colorado and Utah also regulate various AI applications. Specifically, Utah's Artificial Intelligence Policy Act creates disclosure requirements for businesses who use generative AI models to interact with consumers,[7] and Colorado's Artificial Intelligence Act imposes substantial new restrictions and compliance obligations on developers and deployers of high-risk AI systems that are intended to interact with consumers and make, or be a substantial factor in making, "consequential decisions" in areas such as employment, insurance, housing, credit, education, and healthcare.[8]

Businesses already face a complex regulatory environment that imposes overlapping and sometimes inconsistent sectoral and state-specific requirements. The CPPA should avoid overburdening

[6] *See, e.g.*, Colo. Rev. Stat., § 6-1-1306(1)(a)(C); Gen. Stat. of Conn., § 42-518(a)(5)(c); Va. Code § 59.1-577(A)(5).

[7] Utah Artificial Intelligence Policy Act, Utah Code Ann. § 13-72-101.

[8] Colorado Artificial Intelligence Act, Colo. Rev. Stat. Ann. § 6-1-1701.

businesses by adding additional duplicative and unnecessary obligations to this already complex environment.[9]

II. THE CPPA SHOULD ENSURE THAT THE SCOPE OF PROPOSED RULES IS APPROPRIATELY TAILORED TO POTENTIAL RISKS OF USING ADMTS

Several definitions within the proposed regulations are overbroad or use vague language that could be interpreted too broadly. By scoping the regulations so broadly, it is likely that businesses using low- or no-risk ADMTs will be subject to the regulations. Because such systems pose little or no risk to consumers, subjecting businesses using those systems to onerous obligations (including costs of compliance and operational changes) without providing any appreciable benefits is unreasonable. As an overarching issue, the CPPA should align its defined terms with similar definitions contained in existing laws and frameworks, such as existing state privacy laws. Indeed, policymakers, regulators, businesses and consumers will have trouble interpreting conflicting terms across regulatory frameworks.

Excessively broad or vague definitions include:

- "Automated decisionmaking technology," which is defined as "any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking." Notwithstanding the limited exclusions in §7001(f)(4), this definition appears to capture an extremely broad range of computer systems that process personal information. To avoid confusion and align with existing regulations, the definition should be limited to only technologies that replace human decisionmaking, by removing references to "executing a decision" and "substantially facilitating human decisionmaking" This would mirror the approach taken in the U.K. and EU GDPR. Indeed, potential harms stemming from the use of ADMTs are only likely to be realized when there is no human involvement in the decisionmaking process. Therefore, the definition should only apply to ADMTs that make decisions with no human oversight or involvement.

- The definition of "artificial intelligence," as well as the use of the term in the proposed regulations, should be removed altogether. The statute directs the CPPA to develop privacy regulations focused on the use of ADMTs, and to the extent that technologies considered "artificial intelligence" fall within the definition of ADMTs, they will already be within the scope of the regulations. The CCPA does not empower the CPPA to regulate "artificial intelligence" generally.

- "Significant decision" means "a decision using information … that results in access to, or the provision or denial of, financial or lending services, housing, insurance, education enrollment 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)." The CCPA should ensure that its

[9] In addition to legal requirements, leading AI companies have also made voluntary commitments regarding AI safety during President Biden's Administration, including commitments to publish reports detailing model or system capabilities, limitations, and domains of appropriate and inappropriate use, including discussion of societal risks, such as effects on fairness and bias. Many, if not all, of the businesses that made voluntary commitments would also be subject to the CPPA's proposed regulations, increasing the complexity of an already complicated compliance framework for these businesses.

definition of "significant decision" aligns with similar definitions in existing state privacy laws—i.e., definitions of "decisions that produce legal or similarly significant effects."

- "Publicly accessible place" means a place that is open to or serves the public. Examples of publicly accessible places could include shopping malls, stores, restaurants, cafes, movie theaters, amusement parks, convention centers, stadiums, gymnasiums, including hospitals, medical clinics or offices, transportation depots, transit, streets, or parks airports, public wi-fi hotspots, workplaces, educational institutions, government buildings. This definition should be restricted to public places that have the potential to reveal sensitive personal information, such as medical clinics, hospitals, airports, educational institutions, and government buildings.

Relatedly, the CPPA should consider limited modifications to the exceptions contained in sections 7221(b)(1) (security, fraud prevention, and safety); 7221(b)(3)(A) (admission, acceptance, or hiring) 7221 (b)(4)(A) (allocation/assignment of work and compensation); and 7221 (b)(5)(A) (performance at work or in an educational program). Each of these provisions exempts businesses from the opt-out requirement if the ADMT is "necessary to achieve, and is used solely for" the purpose specified in the exception. The regulations should not require that ADMTs be "necessary to achieve" a purpose because this is an extremely high threshold to meet and is too subjective and vulnerable to second guessing by regulators. Requiring that the ADMT be "used solely for" the specified purpose is sufficient to ensure that the exceptions will not be interpreted too broadly. Additionally, the security and fraud exception to the opt-out requirement contained in section 7221(b)(1) should apply to all uses of ADMT set forth in section 7200(a). Concerns about opt-outs undermining ADMTs used for security and fraud prevention in the context of significant decisions about a consumer or public profiling apply equally to the use of ADMTs for security and fraud prevention in the context of advertising or training ADMTs. Further, the CPPA should expand these exceptions to allow for the use of ADMTs to improve and enhance these systems. Such activities include conducting internal research, fixing technical errors, effectuating product recalls, and performing internal operations consistent with the consumer's expectations.

Finally, the rules should not regulate businesses that train ADMTs because the training of models does not involve decisions that impact a specific consumer, and is therefore not automated decision-making, within the scope of the statute. Further, the CPPA's authority does not extend to regulating processes for training these complex systems. Nor does the training of ADMTs present privacy risks to consumers that result from the processing of their personal information. Indeed, other laws that regulate ADMTs do not regulate training uses for these reasons. The potential risk of harm to consumers arises when ADMTs are used to **make a decision** about a consumer without human involvement. The training of ADMT does not involve making decisions about specific consumers., More, the rules already impose obligations related to the use of ADMT for significant decisions, including the right to access information about the use of ADMT for these purposes and the right to opt out, unless the business ensures a certain level of human involvement. To the extent that consumers want to learn about whether their personal information is used for training or correct or delete any personal information used for training, , the CCPA already gives consumers the rights to access information and to correct and delete their personal information.

III. THE CPPA SHOULD RECONSIDER FEASIBILITY OF NEW CONSUMER RIGHTS AND ADOPT TARGETED CHANGES TO REDUCE POTENTIAL COMPLIANCE COSTS

Certain components of the draft regulations for new consumer rights raise technical and practical feasibility questions and concerns. First, as a threshold matter, the CCPA directs the CPPA to issue regulations "governing access and opt-out rights with respect to businesses' use of [ADMTs]."[10] It does not direct the CPPA to require businesses to also provide a pre-use notice to consumers even before the business uses the ADMT.[11] In addition, it may not be technically feasible for businesses to comply with the pre-use notice obligations as framed in the draft regulations. The proposed "Pre-Use Notice" would require businesses to provide information about the logic that their ADMTs use and the key parameters that affect the output of those systems. Based on the current state of the art, ADMTs that are trained on large data sets may not have the technical ability to report the specific parameters that will impact its outputs. Finally, the CPPA should not issue separate and overlapping rules that would require both a pre-use notice and post-use access to information regarding a business's use of ADMTs. Adding another notice to the notices already required under the CCPA's right to know, would overwhelm consumers with information and cause notice fatigue.

Businesses that use ADMTs for significant decisions or for "extensive profiling," as defined in §7200(a)(1)-(2), are also required to provide consumers with a right to access information regarding the ADMT, including how the assumptions and limitations of the ADMT were applied to the consumer and the key parameters that affected the output of the ADMT with respect to the consumer. These obligations may be well intentioned, but given the inherent complexity of the technology at issue, and the underlying machine learning systems, these disclosures are not likely to provide meaningful or actionable information to consumers. Instead, disclosures like this may increase consumer notice fatigue, or confuse consumers who may not understand the underlying technology supporting these systems.

In addition, the notice obligations under §7220(c)(1)(A) require businesses to identify the "specific uses [for which] the [ADMT] is capable of being used," which could encompass a wide range of potential use cases depending upon the nature of the underlying AI model upon which the ADMT is deployed. The consolidated Pre-use Notice proposal addresses this concern, in part, by recognizing that a single ADMT may be used for multiple purposes. But that form of notice may be unwieldy, complex or difficult for consumers to comprehend if the ADMT may be used for multiple purposes. Notably, if this obligation falls on businesses that develop multi-purpose ADMTs, particularly those that develop multi-modal foundation models, it is unreasonable to require such businesses to describe in advance all possible purposes for which another entity may use the ADMT.

The proposed rules would also give consumers the right to opt out of the use of ADMTs to deliver "behavioral advertising," which is defined broadly to include even first-party ads that do not involve the "sale" or "sharing" of personal information within the scope of the CCPA. This requirement conflicts with the CCPA, which authorizes opt outs of only "cross-context behavioral advertising"—a

[10] Cal. Civ. Code § 1798.185(a)(16).

[11] Nor does the statute direct the agency to promulgate new rules about the "logic used" and "key parameters that affect the output," as well as the "intended output" and how the business plans to use it. Here again the CPPA's proposed regulations extend beyond the statutory mandate.

much narrower type of advertising based on personal information collected across the internet over time. Section 1798.140(k) expressly excludes from the definition of "cross-contextual behavioral advertising" any advertising based on personal information obtained from activities with "the business, [or its] distinctly-branded website, application, or service with which the consumer intentionally interacts."

The proposed rules' broader definition of advertising to which the right to opt out would apply would upend the carefully calibrated framework that the California voters established for online advertising when they approved Proposition 24 - the California Privacy Rights Act of 2020 - which amended the CCPA. It would also conflict with all other state privacy laws, which regulate information sharing with third parties and not a business's own use of lawfully collected information. The proposed rules also raise significant First Amendment issues, both to the extent they compel subjective and editorial speech about an entity's own advertising activities and to the extent they burden protected commercial speech. For all of these reasons, the CPPA should eliminate this requirement, and any attendant obligations, such as pre-use notice.

It is also unclear how the new rights to opt out of automated decision making will operate in practice. For example, if an individual opts out of automated decision making, it is not clear whether the business deploying the ADMT would be required to provide its services via other means. If a business is not able to provide its service by another means, it may violate the non-retaliation provisions of the regulations. Specifically, section 7222(l) of the draft regulations states that "a business must not retaliate against a consumer because the consumer exercised their opt-out right as set forth in [CCPA] §1798.125 and Article 7" of the regulations. While section 1798.125 of the CCPA and Article 7 of the regulations provide some flexibility for businesses to engage in reasonable business practices that may otherwise conflict with the prohibition against "retaliation," those carve outs are limited to allowing businesses to offer different prices or services to consumers who have exercised their opt-out rights if the difference is reasonably related to the value of the consumer's personal information. This exception works for the provisions to which it applies in the CCPA because those provisions involve the exchange of personal data for something of value, but it is inapplicable under the new requirements that the CPPA seeks to impose through these regulations. The CPPA should ensure that businesses have similar flexibility under the proposed rules.

In the context of ADMTs, it may not be possible for businesses to offer different services that are based on the value of a customer's data. The CPPA should reconsider, or clarify, the operational impact of these processes, and should clarify that businesses using covered ADMTs are not required to provide their services by other means, if doing so would be technically infeasible.

In addition, the proposed regulations would require businesses that use ADMTs for multiple purposes to provide a description of all such uses but just a single opt-out mechanism. Businesses may use ADMTs for many different purposes, however, and it would likely run counter to consumer expectations to have one opt-out control for all use cases. This rule could force consumers to opt out of all use cases—even those from which they would benefit—just to avoid certain high-risk use cases. The proposed regulations should be clarified to enable businesses, at their option, to implement tailored opt-out mechanisms and provide explanations that are specific to the individual use cases of the technology concerning the specific consumer. In addition, the proposed regulations should include an additional exception to the requirement to provide an opt-out mechanism when use of the ADMT is necessary to provide a product or service that a consumer has requested or is actively and knowingly engaged.

Finally, the proposed regulations requiring pre-use notices and right to access do not contain clear exceptions for trade secrets. While CCPA §1789.00(f) provides that "[n]othing in this section shall require a business to disclose trade secrets," the CCPA also contemplates that the CPPA will issue regulations detailing exceptions to protect trade secrets and intellectual property. The CPPA should revise its draft regulations to expressly carve out trade secret information from the pre-use notice and right to access duties and confirm that nothing in the proposed regulations would require businesses to disclose trade secrets.

IV. THE CYBERSECURITY AUDIT RULES SHOULD NOT INTERFERE WITH EXISTING MANAGEMENT NORMS

The CPPA should revise the draft regulations to harmonize with existing legal requirements and industry expectations of a company's board of directors. The board of directors is intended to serve in a strategic supervisory position, while providing high-level oversight to a business's overall direction. The board is not intended to handle day-to-day management of a business and asking them to do so creates confusion and risk. As drafted, sections 7122 and 7124 create new managerial responsibilities which far exceed the oversight role of a publicly-trade company's board of directors, including requirements that:

- The company's board of directors conduct the auditor's performance evaluation and determine the auditor's compensation.
- The audit be reported to the board of directors.
- The board of directors sign and approve the audit.
- A board member must sign a written certification that includes a statement that the "signed has reviewed and understands the findings of the cybersecurity audit."

The auditor's performance evaluation and compensation should be determined by a senior employee in the business who is familiar with the business's information security program and has the designated authority to enter into contracts on behalf of the business. It is neither realistic nor advisable to strip the person(s) with the day-to-day knowledge of these responsibilities and hand them to a board member who may not have the operational knowledge to appropriately conduct this activity. The board of directors is not in a position to either (i) conduct performance evaluation of outside, third-party providers, or (ii) adequately determine compensation of a process that requires detailed operational knowledge of the company's technology infrastructure.

The audit should only be reported to the board of directors as necessary, and through proper channels. Not all audits or audit findings may need to be reported to the board of directors and creating a requirement to do so may lessen the ability of the board to act when needed. Only audits or findings deemed significant by the Chief Information Security Officer ("CISO") should be reported. Additionally, if audits are to be reported to the board of directors, they should be presented by the CISO to ensure that proper technical and managerial aspects of the audit are conveyed to the board. The audit materials, absent the guidance of the CISO, may only create confusion and uncertainty with the board.

Requiring the board to sign and approve the audit similarly goes beyond the scope of the traditional duties of the board of directors, and inappropriately removes responsibility for oversight from the appropriate member of the management team—the CISO. The risk under the proposed rules is that the CISO—the person with the most familiarity and working knowledge of the company's security

operations and concerns—is removed from a process of which they should be in charge. Instead, this requirement should reside with the CISO—or most senior cybersecurity professional in the company—who has both the operational knowledge of the company and subject matter expertise to properly evaluate the audit and execute on any necessary remediation.

The draft regulations expand the duties of the board of directors which is inappropriate, potentially harmful, and unprecedented. Indeed, no other state regulator or federal agency has taken the position that the board of directors should certify an audit or assessment (either as a legislative requirement or even as the result of a settlement issued after a security incident), let alone certify that one "understands" a specific finding that can be extremely technical in detail. Appropriate oversight by a board does not and cannot mean in-depth technical subject matter expertise—it means ensuring management has processes in place to apply such expertise as appropriate. Other regulatory bodies, including the New York Department of Financial Services ("NYDFS"), the Federal Trade Commission ("FTC"), and the Federal Financial Institutions Examination Council's banking regulatory agencies have chosen not to require such extensive and intimate board involvement for these types of activities—California should not impose otherwise.

V. THE CYBERSECURITY AUDIT RULES SHOULD ALLOW A FLEXIBLE APPROACH TO CYBERSECURITY IMPLEMENTATION AND OVERSIGHT

The CPPA should revise the audit regulations to allow for a flexible approach to cybersecurity audits while incorporating existing frameworks. As drafted, the regulations include specific security requirements that businesses must meet. These specific requirements put an undo emphasis on certain security controls, while constraining security professionals' ability to properly address and remediate security concerns. The draft regulations are overly prescriptive, are not reflective of existing cybersecurity audit frameworks, and amount to the creation of security requirements, which are beyond the scope of statute.

Overly prescriptive requirements make it difficult for businesses to move fast and fix issues in a timely manner. As an example, section 7123(b)(2)(C) requires that the cybersecurity audit assess "zero trust architecture," and if not, "explain why the component is not necessary to the business's protection of personal information. . ." As described by NIST in a 2020 publication, "[z]ero trust is the term for an evolving set of cybersecurity paradigms . . . ."[12] Mandating a relatively new and evolving type of security controls in an audit puts undue weight on those controls and gives businesses less flexibility in their security implementations. Not all businesses may need to employ zero trust architecture in their environment and making them justify that decision, especially given how quickly the industry thinking on that type of security control may change, is time consuming and unworkable.

The requirement in section 7123(b)(2)(B) to encrypt all personal information is also over-prescriptive. Given the expansive definition of personal information, this requirement is likely to be impractical and over-burdensome for businesses to implement, and should be limited to only require encryption of *sensitive* personal information at rest and in transit.

[12] NIST SP 800-207, "Zero Trust Architecture."

Additionally, these overly prescriptive requirements amount to a list of required security controls, which goes beyond the scope of the underlying statute.[13] Instead, the CPPA should rely on existing frameworks such as the NIST Cybersecurity Framework (CSF).

Similarly, the CPPA should not require businesses to justify the use of compensating controls.[14] Instead, if any requirement on compensating controls remains, it should include a materiality qualifier which only requires reporting for "materials gaps and weaknesses."

The CPPA should leverage existing audit frameworks such as SOC II and ISO 27001 or the NIST CSF maturity level assessment and explicitly state that audits conducted under these frameworks satisfy the requirements of the proposed regulations. These types of industry-standard cybersecurity audit frameworks have already been adopted by numerous businesses, have been implemented by auditors who are familiar with their requirements, and are updated on a regular basis to incorporate new and emerging security trends. These frameworks can provide both a substantive list of requirements for any audit conducted under the California regulations, and should additionally provide a safe harbor exception for California businesses that are already compliant with these frameworks.

These proposed changes will allow businesses to implement a flexible approach to cybersecurity audits while incorporating and relying on existing frameworks.

VI. CONCLUSION

The CPPA should narrow the scope of its proposed regulations of ADMTs to target only the highest-risk applications. In addition, the CPPA should ensure that its proposed regulations are consistent with existing state and federal laws and regulations that already govern ADMTs and that new consumer rights are internally consistent and are technically feasible given the current state of the art. The CPPA also should revise the cybersecurity audit rules so that they give businesses sufficient flexibility for implementation and oversight and do not interfere with current management norms. Finally, the CPPA should include an adequate implementation period of at least twelve months between the date the regulations are finalized and the date on which they become enforceable to ensure covered organizations have sufficient time to come into compliance.

Sincerely,

/s/ J. David Grossman
J. David Grossman
Vice President, Regulatory Affairs

/s/ *Rachel Nemeth*
Rachel Nemeth
Senior Director, Regulatory Affairs

February 19, 2025

[13] See Cal. Civ. Code § 1798.185(15)(A), which only requires that a business "[p]erform a cybersecurity audit on an annual basis" and gives the CPPA authority to "defin[e] the scope of the audit," but does not give authority to create security controls.)

[14] § 7123(c)(2) and (3).