January 25, 2024

Via Electronic Mail: (regulations@cppa.ca.gov)

California Privacy Protection Agency
Attn: Chairperson Jennifer M. Urban
2101 Arena Boulevard
Sacramento, CA 95834

Re: Rulemaking on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking Technology

Dear Chairperson Urban and Members of the California Privacy Protection Agency Board:

On behalf of the Computer & Communications Industry Association ("CCIA"),[1] I write in response to the California Privacy Protection Agency's effort to implement and enforce the California Consumer Privacy Act of 2018 ("CPPA"), including the substantive and ongoing rulemaking comment periods regarding Proposition 24, the California Privacy Rights Act ("CPRA").

CCIA has long supported the evolution of privacy policy to keep pace with evolving technologies. The Association supports and appreciates the Agency's efforts to adopt and implement privacy regulations to guide businesses and protect consumers. To date, CCIA has been directly engaged in the CPPA's formal rulemaking process, having submitted comments on draft regulations,[2] modifications to the draft regulations[3] and, finally, on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking.[4] CCIA's comments largely center on ensuring that businesses can understand and meet compliance expectations and that consumers are able to understand their data privacy rights, which is particularly difficult when those standards differ across jurisdictions.

Following the Agency's December 8, 2023 discussion of the draft regulations covering Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking Technology (ADMT), we'd like to reiterate several important areas of concern. CCIA greatly appreciates the Board's ongoing collaborative efforts to consider stakeholder feedback.

---

[1] CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For over fifty years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. For more information, visit www.ccianet.org.
[2] Comments of CCIA, CPPA Public Comment, (Aug. 18, 2022), https://www.ccianet.org/wp-content/uploads/2022/08/2022-8-18_CCIA-Comments-to-CPPA-on-Draft-Regulations.pdf.
[3] Comments of CCIA, Proposed Modifications to Draft Regulations (Nov. 21, 2022), https://ccianet.org/library/comments-to-cppa-on-modifications-to-draft-regulations/.
[4] Comments of CCIA, Preliminary Comments on Proposed Rulemaking on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking (Mar. 27, 2023), https://ccianet.org/library/ccia-comments-to-cppa-invitation-on-cyber-ads-risk/.

The Agency has an opportunity to provide clarity and guidance for businesses and consumers with its next set of rulemaking to fully implement the CCPA. However, some of the proposed changes go beyond the aims of the statute, potentially halting the safe, responsible, and innovative work around AI and other technologies in California. For example, a proposed revision would amend the CCPA definition of "sensitive data" to cover the information of consumers under the age of 16. Raising this age threshold from 13 to 16 not only diverges from the privacy laws in other states but invites conflict with the age set by Congress in the Children's Online Privacy Protection Act. CCIA urges the Agency to further revise the draft regulations to ensure they align with the aims of the CCPA and actually "harmonize"[5] with other states' privacy frameworks.

On ADMTs. CCIA has serious concerns about several aspects of the proposed regulations addressing the use of Automated Decisionmaking Technology, some of which go beyond the CCPA's statutory mandate.

First, the CCPA provides limited rulemaking regarding an individual's opt-out rights. Yet, the proposed regulations would create new opt-out rights that are not found in the statute, including profiling for "behavioral advertising" and "processing the personal information of consumers to train" ADMTs. The Agency should not create new rules that go beyond the statutory mandate, especially ones that are inconsistent with the existing CCPA regulations on advertising.

Second, the proposed broader definition of ADMT would cover a sweeping number of routine low-risk technologies such as small business' use of spreadsheets and calculators. The proposed definition would also apply before a decision is made and even if a human was involved – meaning, *even if a human was involved,* this still would constitute an "automated" decision. Notably, the opt-out would apply when an ADMT is used as "part of a system" to "facilitate human decisionmaking", encompassing most if not all software. As a result, any personal information, which is broadly defined under California law, used in an ADMT would likely be subject to this opt-out.

Third, the expansive definition of ADMTs and the new opt-out rights risk disrupting basic business operations. The proposed regulations would apply to any software or system that uses personal information for product research or improvement of an online service or product. This could result in breaking basic website features and updates including performing A/B testing and analysis for improving website functionality for consumers. Many businesses rely upon this information to measure how their customers and audience use their online services and products. The software that these businesses rely upon enables them to effectively reallocate resources to improve their products and this automatic optimization also helps spot trends or possible disruptions that may occur during a busy season. Preventing companies from utilizing software to optimize their websites should not be included in these rules.

Lastly, the proposed regulations will be costly to implement, hurting businesses of all sizes that rely upon these widely used tools. A covered business will be required to provide a unique

[5] California Privacy Protection Agency, Agenda Item 3: Explanation of Proposed Modifications to Regulations, (Dec. 2023) https://cppa.ca.gov/meetings/materials/20231208_agenda_item3_chart.pdf

"pre-use" notice that must, amongst other things, include detailed information about the purposes for using the ADMT, the relevant opt-out and access rights, and access to additional detailed information on the logic and key parameters used in the ADMT. In practice, a small coffee or bookshop that uses machine learning to track employees for scheduling or performance would be required to understand and then explain the logic used in this system, along with answering an extensive list of other questions. The final regulations should not impede upon the success small businesses have found with using AI, with a recent study finding that "91% of small businesses using AI have had success in driving revenue, customer outreach and acquisition, or increasing productivity."[6]

On Risk Assessments. The final regulations on risk assessments should seek parity with other states. With states increasingly incorporating requirements around risk assessments, these obligations must be streamlined to avoid businesses having to conduct multiple assessments for substantially similar processing activities. Further, companies should not be required to divulge commercially sensitive information or sensitive security information, including details on technical safeguards that would allow a bad actor to compromise the company's security practices. CCIA recommends the Agency consider an approach that would limit risk assessments to processing that presents a heightened risk of harm to a consumer and the steps being taken to address and mitigate that risk. These risks of harm may include identity theft or fraud, extortion, or physical injury from the disclosure of intimate or other objectively sensitive personal details such as one's sexual orientation. Lastly, a risk assessment needs to be limited to the actual processing of data – it should not be used as a proxy to require a risk assessment of the feature itself as distinct from any processing of data that occurs as part of that feature.

CCIA appreciates the Board's pause about the scope and substance of these draft regulations, especially in light of the recent court holding that enjoined the enforcement of California Age-Appropriate Design Code. However, concerns remain, in particular regarding how intertwined the draft regulations for ADMTs and risk assessments have become. As currently written, a business responding to an access request about their use of an ADMT (ex: use of spam filters or spell check to process resumes) must also address several other costly risk assessment requirements. As a result, the risk assessment rules may become an additional and burdensome step that businesses will have to comply with in addition to the notice and opt-out requirements proposed by the ADMT draft regulations.

On Cybersecurity Audits. Organizations already face an uphill battle to maintain strong cybersecurity practices but the proposed draft rules would make this challenge even more difficult by unnecessarily broadening the scope of these audits, in addition to the expanded threshold for what processing constitutes a "significant risk. For example, these proposed amendments would expand the scope of what is required in an audit, going far beyond what is required in other industry compliance frameworks like SOC2.[7]

[6] Constant Contact, "An AI Awakening: How small businesses are using AI and automation to bolster their business"(Aug. 8, 2023), https://news.constantcontact.com/2023-08-09-Constant-Contact-Research-Reveals-Small-Businesses-Who-Use-AI-Are-More-Likely-to-Save-Money-and-be-Successful

[7] The SOC2 is a widely used and voluntary cybersecurity framework published by the American Institute of Certified Public Accountants. *See,* AICPA, "System and Organization Controls: SOC Suite of Services",

The draft rules propose amending the definition of "cybersecurity incident" to include any unauthorized occurrence that could *potentially* jeopardize the confidentiality, integrity, or availability of a business's information systems or any information the system processes. The proposed regulations would also require that the audit include an assessment of *any* risks stemming from a cybersecurity incident that have or are reasonably likely to materially affect consumers. Further compounding this challenge is the requirement to assess and document any risks from "cybersecurity *threats*", which is broadly defined to include any unauthorized occurrence that may adversely affect the confidentiality, integrity, or availability of a business' information system or any information within them.

The proposed changes may undermine the effectiveness of many security programs by requiring companies to document every possible risk. For example, a company may have various security controls to mitigate against a phishing or ransomware attack. Even if the security tool is effective against the attack, a company must still document this failed attempt simply because it has the potential to affect the availability of the information. Organizations face dozens if not hundreds of digital threats daily, and an overly prescriptive requirement to document them all would create substantial compliance costs for businesses with little to no security benefit to consumers.

* * * * *

CCIA and its members thank the Agency for the opportunity to provide input on how to balance the Rules in ways that protect consumers, are feasible to implement, and maintain flexibility for personalization and innovation. Should you have any questions, please contact Alvaro Marañon at amaranon@ccianet.org

Sincerely,

Alvaro Marañon
Policy Counsel
Computer & Communications Industry Association

https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services (last visited Jan. 16, 2024).