March 27th, 2023

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

To Whom It May Concern:

Re: Notice of Proposed Rulemaking, California Privacy Protection Agency (March 27th, 2023)

The U.S. Chamber of Commerce's Technology Engagement Center ("Chamber" or "C_TEC") appreciates the opportunity to provide public comment on its Proposed Rulemaking to amend California's privacy regulations to implement the California Privacy Rights Act ("CPRA"). Consumers deserve strong privacy protections and innovative products and services. Businesses need certainty, uniformity, and protection. It is, for this reason C_TEC supports national privacy legislation that does all these things. The California Privacy Protection Agency's ("CPPA" or "Agency") proposed rules will impact businesses beyond the borders of the Golden State, which is why we believe it is essential that the agency looks for every opportunity to harmonize with already implemented policies, such as GDPR and the provisions of other state privacy laws. Therefore, we offer the following comments promoting consumer protection and business clarity that fall within the limits of CPRA.

I. Cybersecurity Audits

Among other things, the proposed rulemaking calls on CCPA to issue regulations requiring businesses "whose processing of consumers' personal information presents significant risk to consumers' privacy or security" to perform annual cybersecurity audits, "including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent."

A large number of businesses conduct cybersecurity audits either because of a legal obligation or as a best practice. Any new regulation in this area should have sufficient flexibility to allow businesses to align their existing auditing programs and processes with requirements that the agency develops. In addition, CPPA should expressly allow businesses to leverage industry-led, widely accepted cybersecurity best practices, frameworks, and standards as a basis for regulatory and legal liability safeguards.[1]

Trigger. CPPA should ensure that the trigger for a cybersecurity audit is distinct from businesses' assessments relating to consumer privacy risks. The trigger for a cybersecurity audit should be based on a significant cybersecurity incident consistent with the definition of a covered cyber incident under the Cyber Incident Reporting for Critical Infrastructure Act of

[1] The U.S. Chamber of Commerce's January 2023 comment letter to the New York Department of Financial Services on the department's second amendment to its cybersecurity requirements for financial services companies. This letter is available upon request.

2022 (P.L. 117-113).[2] CPPA should avoid overly broad interpretations of what constitutes a significant risk. The statutory text supports this. Section 1798.185(a)(15) of the CPRA directs CPPA to develop regulations relating to cybersecurity audits and risk assessments for the "processing of personal information [that] presents significant risk to consumers' ... security." Without a finely tuned definition or definitions, businesses could be forced into considerable auditing activity—in essence, pulling business resources away from managing the cybersecurity of both their enterprises and the consumers they serve.

CPPA should also distinguish between security risks and privacy risks, and limit the trigger for auditing requirements to the former. As noted at the outset, many businesses already perform cybersecurity audits. Standards and best practices for cybersecurity audits focus on security risks, which are different from privacy risks. Different frameworks and processes for identifying, classifying, and remediating cybersecurity and privacy risks exist for this very reason.[3]

It is important to spotlight that the statutory text reflects the same approach. Indeed, section 1798.185(a)(15) directs the agency to develop standards relating to processing that presents "significant risks" to "privacy or security" and contemplates separate vehicles for doing this—(1) a cybersecurity audit that includes "the factors to be considered in determining when processing may result in significant risk to the security of personal information"; and (2) a risk assessment, which includes the processing of sensitive information and sets forth a high-level framework similar to data protection requirements under other state, as well as global, data privacy frameworks.

Scope. The statute calls for an annual cybersecurity audit. Regulations should be reasonable in scope, covering the security program for the relevant segment of an organization that processes consumers' personal information. This is a common approach of widely recognized standards, such as NIST special publications.

The regulations should not mandate audits for low-impact or insignificant cyber activity. Such a mandate would place businesses in a perpetual state of unproductive auditing that would likely conflict with related examinations and/or requirements. Requiring multiple audits would generate substantial activity and costs but yield little to no return on security and resilience. In short, CPPA should prioritize harmonizing its regulation regarding cybersecurity audits with existing laws and requirements that businesses already follow.

CPPA asks stakeholders whether they recommend that officials consider the cybersecurity audit models created by other laws as the regulations are written. Existing laws and regulations typically apply to specific sectors. The Chamber recommends that CPPA officials develop regulations that permit the entities that are required to abide by sector-specific auditing requirements and existing federal guidelines to leverage these for their compliance with any CPPA requirement. Existing regulations include nuanced considerations and

[2] https://www.congress.gov/bill/117th-congress/house-bill/2471

[3] National Institute of Standards and Technology (NIST) has developed frameworks for managing cybersecurity and privacy risks.

enforcement mechanisms that are specific to each sector and are neither easy nor prudent to generalize across industry. California policymakers should maintain, and not duplicate, these existing regulations for entities that are covered under their provisions to prevent regulatory overlap.

One company told the Chamber that the Health Insurance Portability and Accountability Act of 1996 (HIPAA) tasks the Department of Health and Human Services (HHS) with creating regulations to protect the privacy and security of certain health information, including Personal Health Information (PHI) and now e-PHI. HIPAA includes the Privacy Rule and the Security Rule, which set standards for HIPAA-regulated entities (e.g., health care payers) to follow. HIPAA-regulated entities follow detailed privacy and security provisions to protect data, including the use of the minimum necessary data standard and specific data protection steps. HIPAA-regulated entities also adhere to breach notification and data use requirements.

HIPPA is unlikely to apply to entities outside the health care sector. Yet HIPPA illustrates how CPPA officials can align their cybersecurity auditing regulation with existing laws and rules. Worth noting, too, is that such thinking lines up well with the Biden administration's recent *National Cybersecurity Strategy*, which calls for harmonizing new and existing regulations as a means of strengthening U.S. cybersecurity. The White House stresses that effective regulation minimizes the costs and burdens of compliance, "enabling organizations to invest resources in building resilience and defending their systems and assets."[4]

California Civil Code § 1798.185(a)(15)[5]

(15) Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to:

(A) **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.

(B) **Submit to the California Privacy Protection Agency on a regular basis a risk assessment** 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,

[4] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[5] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.185

the business, other stakeholders, and the public. Nothing in this section shall require a business to divulge trade secrets [emphasis added].

Process. An auditing process needs to be workable. The regulations should grant businesses the flexibility to use either internal cybersecurity auditing processes or retain independent third-party auditors as opposed to mandating one over the other. With respect to internal audits, this concept is not new to California. The state's insurance code permits internal audits that are organizationally independent.[6]

In response to Civil Code § 1798.185(a)(15)(A), private organizations that are already performing annual or semiannual cybersecurity audits (e.g., based on HITRUST or the Payment Card Industry Data Security Standard) will likely want to leverage work they are already doing and any subsequent certifications.

Also, CPPA's notice asks to what degree do other legally required cybersecurity audits, assessments, evaluations, or best practices align with the processes and goals articulated in California Civil Code § 1798.185(a)(15)(A). A firm stressed to the Chamber that CPPA should make reciprocity a feature of its cybersecurity audits regulation vis-à-vis cloud certification programs, such as the Federal Risk and Authorization Management Program (FedRAMP) and the State Risk and Authorization Management Program (StateRAMP). Each program is sufficient to meet the requirements of the CCPA. FedRAMP is the federal government's approach to the risk-based adoption and use of cloud services. An organization that earns a FedRAMP authorization typically completes a readiness assessment and pre-authorization prior to undergoing a full security assessment and authorization.

StateRAMP is a multi-state organization in which California is a member.[7] StateRAMP establishes common security criteria to standardize cloud security verification, which is especially helpful to state and local governments purchasing services. Reciprocity between FedRAMP and StateRAMP provides vendors with the ability to leverage their federally approved security assessments for the StateRAMP Fast Track.[8] Such steps are more than sufficient to provide California and its citizens assurance that an organization is undertaking the types of cybersecurity practices designed to manage cybersecurity risks identified in the CCPA.

Businesses Need Flexibility Regarding Compliance, Including Cybersecurity Audits

Missing from CPPA's proposed requirements are safeguards for businesses that demonstrate their use of existing cybersecurity programs to meet the requirements of the

[6] CA Ins Code § 900.3 (2019) https://law.justia.com/codes/california/2019/code-ins/division-1/part-2/chapter-1/article-10/section-900-3

[7] https://stateramp.org/participating-governments

[8] https://stateramp.org/blog/stateramp-fast-track

CCPA. Businesses with cybersecurity programs that reasonably align with these and other laws and regulations that contain cybersecurity requirements should be entitled to liability protections. CPPA should balance regulatory compliance with greater flexibility in meeting industry-recognized standards, as well as positive incentives to increase the economic security of regulated parties and California.

While far from a comprehensive listing, CPPA should deem that the following cybersecurity best practices, frameworks, standards, and programs satisfy any cybersecurity auditing requirements under the CCPA:

- The Cybersecurity Framework developed by NIST
- NIST special publication 800-171
- NIST special publications 800-53 and 800-53a
- NIST special publication 800-218
- NIST profile of the Internet of Things Core Baseline for Consumer IoT Products (NIST Internal Report 8425)
- Cybersecurity Maturity Model Certification
- The Federal Information Security Modernization Act of 2014
- Title V of the Gramm-Leach-Bliley Act of 1999, as amended
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- The Security Assessment Framework for FedRAMP
- The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000 family, information security management systems
- The ISO/IEC 30111 and 29147, coordinated vulnerability handling and disclosure
- Critical Security Controls for Effective Cyber Defense developed by the Center for Internet Security
- The Profile developed by the Cyber Risk Institute
- The Payment Card Industry Data Security Standard, as administered by the Payment Card Industry Security Standards Council

In sum, the Chamber strongly urges CPPA officials to align its regulation related to cybersecurity audits with existing ones as well as to leading industry best practices. CPPA should also collaborate closely with businesses to determine the most effective and efficient cadence for cybersecurity auditing and reporting.

II. Risk assessments

1. What laws or other requirements that currently apply to businesses or organizations (individually or as members of specific sectors) processing consumers' personal information require risk assessments?

C_TEC would like to highlight that many organizations and companies are already complying with various laws that require privacy risk assessments. The regulations should leverage existing best practices (such as the NIST Privacy Framework) and existing regulatory

standards, including the EU General Data Protection Regulation (effective May 2018) and other state privacy laws, such as those enacted in Virginia, Connecticut, and Colorado.

a. To what degree are these risk-assessment requirements aligned with the processes and goals articulated in Civil Code § 1798.185(a)(15)(B)?

The CPRA sets out the rulemaking goals for risk assessments to include assessing "whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing . . . against the potential risks to the rights of the consumer associated with that processing." These goals align with the data protection assessment requirements in the privacy laws enacted in Virginia, Connecticut, and Colorado. Taking the Virginia CDPA as an example: this standard requires that businesses (i.e. controllers) conduct and document a data protection assessment of…processing activities involving personal data, and more specifically, the processing of sensitive data and any processing activities involving personal data that present a heightened risk of harm to consumers. The provisions further require that assessments also identify and weigh the benefits [to the controllers] against the potential risks to the rights of the consumers, as mitigated by safeguards that can be employed to reduce such risks. The Connecticut and Colorado standards are identical. This clearly advances the goals of the CPRA.

Moreover, this standard supports a risk-based approach, which is the most meaningful way to advance consumer protections and ensure that a risk assessment doesn't become a "check the box" exercise.. Notably, we are not aware of any existing mandates that call for risk assessments for every processing activity. The GDPR, for instance, mandates data protection assessments when processing "is likely to result in a high risk to the rights and freedoms of a natural person." See Art. 35(1). Such high-risk processing activities include profiling for consequential decisions, the large-scale processing of sensitive data, and the systemic and large-scale monitoring of publicly accessible areas. Art. 35(3).

The CPRA regulations can meaningfully advance consumer privacy standards by aligning the risk assessment requirement with these standards and the NIST Privacy Framework. This will incentivize meaningful assessments of the most impactful processing activities while simultaneously harmonizing.

e. Would you recommend the Agency consider the risk assessment models created through these laws, requirements, or best practices when drafting its regulations? Why, or why not? If so, how?

We support impact assessments for high-risk processing activities and align such risk assessment models to enable efficient and consistent compliance by organizations and consistent protections for consumers.

We note that existing laws currently apply to specific industries and recommend that policymakers refer to sector-specific regulation and existing federal guidelines and enforcement as being compliant with the CPRA's risk assessment requirements. Existing regulations include considerations and enforcement specific to those industries, and

policymakers should maintain and enable the continuation of these regulations for entities that fall under their provisions and avoid regulatory overlap.

5. What would the benefits and drawbacks be for businesses and consumers if the Agency accepted businesses' submission of risk assessments that were completed in compliance with GDPR's or the Colorado Privacy Act's requirements for these assessments?

As noted above, we fully support a harmonized approach to privacy risk assessments. Accepting risk assessments completed in compliance with other laws such as the EU GDPR or Colorado Privacy Act will providing the following:

- Efficiency as businesses will not need to navigate a patchwork of requirements, allowing them to implement more consistent policies and processes.
- Reflection of the global context in which data is processed -- that data processing is rarely limited to individuals located in one state or geographic area; and
- Alignment with current regulatory trends to accept risk assessments conducted in compliance with comparable laws of other jurisdictions.

Benefits to consumers include:

- More efficient respond time by companies to consumer rights requests.
- Consistent protections for consumers, regardless of where a consumer resides.
- More consistent risk evaluation and mitigation.

This harmonized approach is something that both Virginia, Colorado and Connecticut have recognized the benefits of, as they have included stipulations which allow them to accept privacy risk assessments completed in compliance with the laws of other jurisdictions:

Sec. 59.1-580, E, of the Virginia CDPA, allows that data protection assessments conducted for the purpose of compliance with other laws or regulations be sufficient to comply with Virginia's privacy risk assessment requirement, provided the assessments have a reasonably comparable scope and effect."

Section 6-1-1309(5) of the Colorado Privacy Act provides that "a single data protection assessment may address a comparable set of processing operations that include similar activities."

6. In what format should businesses submit risk assessments to the Agency? In particular: (a) if a business were required to submit a summary risk assessment to the Agency on a regular basis (as an alternative to submitting every risk assessment conducted by the business): (i) What should these summaries include, (ii) In what format should they be submitted, and (iii)How often should they be submitted?

At the outset, we appreciate that the Agency is considering permitting summaries of risk assessments to fulfill the submission requirement rather than requiring the submission of each risk assessment conducted. This is an appropriate balance of resources, both for the

Agency as it reviews the submission and for businesses conducting them. On the latter point, we note that risk assessments are most impactful when they present an opportunity for a full discussion and consideration of the processing activities and ways to mitigate any identified risks of harm. An overbroad requirement to submit each risk assessment would chill the free and open discussion necessary to make this process meaningful. Moreover, risk assessments need to involve various internal stakeholders, including legal counsel. Thus, a mandate to turn over the assessment could chill the ability of legal counsel to advise in the process due to concerns that any privilege could be vitiated from the compelled submission.

In terms of format and procedures for summary submissions, the Agency should consider requirements that recognize that the summaries may be of a signal assessment that addresses comparable sets of processing for similar activities.

III. Automated Decisionmaking

1.What laws requiring access and/or opt-out rights in the context of automated decisionmaking currently apply to businesses or organizations (individually or as members of specific sectors)?

At the outset, we note that the CPRA itself does not confer an opt-out right related to automated decision-making. The statutory text is clear on the opt-outs authorized, which is for sales and sharing of personal data. While the CPRA does state that the Agency is authorized to engage in rulemaking with respect to an "opt-out right" for automated decision-making, this provision raises constitutional questions worth noting regarding the broad nature of the delegation of authority[9].

If the Agency does move forward despite these issues and creates an opt-out right through regulations, it should be guided by two complementary goals: ensuring the opt-out right is meaningful to consumers without disrupting beneficial and low-risk uses of automated decision making and that it is interoperable with other states that have enacted opt-outs. The Agency can achieve both goals by following the approaches in the Virginia, Colorado, and Connecticut privacy laws, which have all incorporated automated decision-making opt-outs limited to automated decision-making used for profiling in furtherance of "decisions that produce legal or similarly significant effects," California's approach should be informed by and consistent with this emerging norm in these three state laws. This balances the opt-out right to empower consumers to exercise their choice for legal decisions or otherwise similarly consequential profiling through the use of automated decision-making, while preserving clearly benign and routine uses of automated decision-making that enhance the customer experience without implicating consequential decisions. It would also avoid imposing duplicative requirements, which would add unnecessary burden onto businesses without promoting consumer privacy.

2.What other requirements, frameworks, and/or best practices that address access and/or opt- out rights in the context of automated decisionmaking are being

[9] [9] *Gerawan Farming, Inc., v. Agricultural Labor Relations Bd.,* 405 P.3d 1087, 1100 (CA. Sup. Ct. 2017) (citing *Carson Mobilehome Park Owners' Assn. v. City of Carson*, 672 P.2d 1297, 1300 (Ca. Sup. Ct. 1983)).

implemented or used by businesses or organizations (individually or as members of specific sectors)?

We believe it is important to clarify that companies, for the most part, don't have requirements, frameworks, or best practices that specifically address access/opt-out requirements when it comes to the use of low-risk automated decision-making. These types of tools which we interact with every day, such as spellcheck, have little to no risk associated with their use, and requiring access or opt-out rights for such tools would be burdensome for users.

C_TEC would like to highlight that there continues to be a significant number of efforts in developing Artificial Intelligence / Machine Learning standards and frameworks, which look to address the development and use of high-risk automated decision-making. These efforts include the recently released National Institutes of Standards and Technology (NIST) AI Risk Management framework created through a collaborative and multi-stakeholder process. Since the framework was published (January 2023), many organizations have sought to utilize NIST's framework. We strongly suggest that the CPPA look at NIST's efforts. It is also important to highlight that NIST's previous work developing Cybersecurity and Privacy Frameworks has become the gold standard in guiding industry practice.

3.With respect to the laws and other requirements, frameworks, and/or best practices identified in response to questions 1 and 2:

a. *How is "automated decisionmaking technology" defined? Should the Agency adopt any of these definitions? Why, or why not?*

To succeed in creating a regulatory framework for the use of Automated Deployment Technology, it is imperative that there be a clear legal definition that provides precise legal certainty and harmonizes with others. This is why we believe it is important for alignment with federal agency guidance and standards development groups that continue to advance work, including definitions, in this space. This includes ongoing AI initiatives around best practices, including the NIST work groups developing voluntary AI Risk Management guidance and standards to define and measure types of bias in AI. We also stress that it is essential for definitions to be precise and align with terms and standards developed by established consensus-based entities.

4. How have businesses or organizations been using automated decisionmaking technologies,
including algorithms? In what contexts are they deploying them? Please provide specific examples, studies, cases, data, or other evidence of such uses when responding to this question, if possible.

C_TEC would like to highlight that the use of Automated Decisionmaking Technologies (ADT) continues to become more prevalent within businesses and organizations as they provide essential efficiencies, especially to small businesses. C_TEC released a report last year which

indicated that 27%[10] of small businesses currently plan to utilize artificial intelligence in their practices. Using ADT and data analytics is essential in allowing small businesses to compete by streamlining important tasks like hiring and tailoring services.

5. What experiences have consumers had with automated decision-making technology, including algorithms? What particular concerns do consumers have about their use of businesses' automated decisionmaking technology? Please provide specific examples, studies, cases, data, or other evidence of such experiences or uses when responding to this question, if possible.

C_TEC would like to highlight that consumers interact with automated decision-making technologies every day, which provide a constant benefit to them. From navigation software that provides consumers with the most time-efficient directions to their destination, to digital calendars, which update consumers on when they should leave their current location to meet their following obligation based on current traffic patterns. At the Cleveland Clinic AI is being used to "identify and triage the sickest COVID-19 patients, allowing its physicians and nurses to allocate resources effectively and provide more personalized care.[11]" The use of technology is providing enormous benefits to society, and its utilization assists consumers by providing them with enhanced accuracy, cost savings, and overall efficiencies in their daily lives.

7. How can access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling, address algorithmic discrimination?

Having excellent and robust data is the foundation for addressing algorithmic discrimination within ADT. For this reason, we would like to highlight the importance of the use of data such as race/ethnicity for the purpose of preventing bias. Regulators should also look at other ways to provide incentives, such as safe harbors to companies and organizations proactively looking to prevent bias that may result from the use of algorithms, by looking at specific impacts on different user groups, including minority groups.

8. Should access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling, vary depending upon certain factors (e.g., the industry that is using the technology; the technology being used; the type of consumer to whom the technology is being applied; the sensitivity of the personal information being used; and the situation in which the decision is being made, including from the consumer's perspective)? Why, or why not? If they should vary, how so?

We believe it is important for regulators to understand that the risks, concerns, and benefits in relation to the use of the technology vary depending on specific sectors. Therefore, it is essential for the agency to defer to those sector-specific regulating agencies when addressing potential concerns regarding the use of the technology.

---

[10] https://americaninnovators.com/wp-content/uploads/2022/08/Empowering-Small-Business-The-Impact-of-Technology-on-U.S.-Small-Business.pdf

[11] https://www.uschamber.com/assets/documents/CTEC_AICommission2023_Report_v5.pdf

We continue to stress that each sector to look for harmonization with others on critical issues in the development of technology, as a patchwork approach could create unnecessary compliance burdens. This issue is currently being seen as different CA agencies promulgating rules on automated decision systems — CA Civil Rights Council is in the process of its rulemaking to regulate automated decision systems, in addition to what the CPPA is expected to put forth. We are strongly concerned that this presents issues of overregulation, inconsistent standards for businesses subject to varying rules, and confusion for the consumers they seek to protect.

Regarding opt-out rights with respect to business, we believe it is important to highlight that the use of automated decision-making by businesses, even in "high-risk" uses of the technology, is highly beneficial to consumers. Things such as healthcare providers who uses someone's geolocation to determine the closest medical facility, to banks using the ADT for fraud detection. It is important to highlight that opt-out requirements of such tools could significantly harm consumers.

Conclusion:

The Chamber stands ready to work with you to ensure that the CPPA protects the laudable goals of giving consumers the right to access, correct, delete, and opt-out of sharing information, among others. At the same time, we urge the Agency to carefully follow the statutory text, which will provide the certainty needed for a thriving innovation economy.

Sincerely,

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