U.S. Chamber of Commerce

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

August 19, 2022

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd.
Sacramento, CA 95834

To Whom It May Concern:

Re: Notice of Proposed Rulemaking, California Privacy Protection Agency (July 8, 2022)

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")[1]. Consumers deserve strong privacy protections and innovative products as services. Businesses need certainty, uniformity, and protections against abusive litigation. It is for this reason that the Chamber 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. Therefore, we offer the following comments promoting consumer protection and business clarity that fall within the limits of CPRA.

I. The Proposed Explicit Consent Requirement for "Incompatible" Data Practices Could Unlawfully Chill Societally Beneficially Uses of Data.

Secondary uses of data are instrumental in serving consumers better as well as helping solve many of society's greatest challenges and providing a public interest benefit.[2] For example, it is being used to combat online fraud, expand financial inclusion, and examine social determinants of health. It is critical for these societally beneficial uses of data to continue to be reaped. This would allow flexibility while still giving consumers choice in this matter so as not to dry up the data pools necessary to achieve these positive goals of public safety and inclusion.

The Proposed Regulations without statutory justification threaten the use of secondary data by requiring a business obtain "explicit consent…before collecting, using, retaining, and/or sharing the consumer's personal information for any purpose that is unrelated or incompatible with the purpose(s) for which the personal information collected or processed."[3] The Proposed

[1] https://cppa.ca.gov/regulations/pdf/20220708_text_proposed_regs.pdf
[2] https://americaninnovators.com/wp-content/uploads/2020/01/CTEC_DataForGood_v4-DIGITAL.pdf
[3] Proposed Regulations § 7002(a).

Regulation reads contrary to the plain text of the CRPA which only requires notice if personal information and sensitive personal information are used for additional purposes "that are incompatible with the disclosed purpose for with the personal information was collected."[4] In addition, the proposed regulation ignores the secondary use standard in the CPRA, which allows personal information to be used for other disclosed purposes that are compatible with the context in which the personal information was collected. Instead, the Agency would apply an ambiguous "average consumer" standard that could give it discretion to effectively change the CPRA text from a notice requirement to an opt-in obligation. The explicit consent requirement also goes beyond the Federal Trade Commission's standard for non-material changes. To comply with the text of the CPRA, the Agency should strike the explicit consent requirement.

The Proposed Regulations are also inconsistent with federal law. For example, the "explicit consent" standard before a business may collect any new category of personal information is inconsistent with the FTC's standard for material, prospective changes. Additionally, the Proposed Regulations example relating to Business D sharing information with Business E and then requiring Business E to obtain explicit consent to market their products likely conflicts with the U.S. CAN-SPAM Act, which preempts state law and allows the transfer of email addresses for commercial email marketing as long the consumer has not opted out.

II. The Proposed Global Opt-Out Mandate Exceeds the CPPA's Statutory Authority.

Section 7025 of the Proposed Regulations mandates obligations on businesses who receive opt out preference signals and to treat such signals as a verified request to opt out. Specifically, Section 7025(b) states "[a] business *shall* process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing."[5] The CPRA does not authorize the CPPA to legislate this new mandate.

The CPRA provides companies with an option of one of two methods to honor a request by a consumer to opt out of the "selling" or "sharing" of personal information. One method to honor a verified opt-out request is to post a "Do Not Sell or Share My Personal Information" link and if applicable a "Limit the Use of My Sensitive Personal Information" link.[6] Alternatively, businesses do not need to offer such a link "*if* the business allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal…"[7] The statute's use of the word "if" makes it clear that CPRA treats responses to opt-out preference signals as voluntary. The voluntary nature of opt-out preference signals is further evidenced by other language such as "[a] business that *allows* consumers to opt out of the sale or sharing of their personal information

[4] Cal. Civ. Code § 1798.100(a)(1),(2).
[5] Proposed Regulations § 7025(b).
[6] CAL. CIV. CODE § 1798.135(a).
[7] *Id*. At § 1798.135(b)(1) (emphasis added).

and to limit the use of their sensitive personal information pursuant to paragraph (1) may provide a link to a web page that enables the consumer to consent to the business ignoring the opt-out preference signal...."[8]

As many of the Chamber's members operate nationwide including in the state of California, it is in the interest of both consumers and the business community to eliminate confusion and potentially conflicting data rights. For this reason, Section 7025(b) should be revised to conform to CPRA and treat recognition of global opt-out preference signals as voluntary and not mandatory.

Giving businesses the flexibility with respect to recognizing a global opt out preference signal, as envisioned by the statute, is important. There are many uncertainties regarding how such signals would be implemented, how businesses are to treat multiple global opt preference signals that could conflict, and how to ensure that that such signals do not have anti-competitive consequences. There is currently no universal opt-out preference signal capable of effectively communicating a consumer's opt-out preferences to all websites, online platforms, or mobile applications. Universal opt-preference signals should be an optional method for honor opt-outs as outlined in the statute.

Moreover, the proposed regulations ignore important statutory requirements designed to ensure consumers make informed opt-out choices. In particular, the Agency should ensure that any global opt-out preference is free of defaults that presuppose consumer intent, is clearly described and easy to use, and does not conflict with other commonly used privacy settings. A mechanism that fails to accurately identify California residents and inform them of the specific privacy choices under the CPRA would not meet the statutory requirements for obtaining informed consumer consent.

III. The Required Mechanisms for Consumer Rights Request should be Reasonable and Encourage Choice.

The Chamber agrees with the objectives of the Proposed Regulations to prevent consumers from being misled in their privacy choices. However, the Proposed Regulations should not provide consumers with such narrow or limiting options that their autonomy is eroded as well. Consumers may wish to have multiple privacy preferences as opposed to take it or leave it approaches.

The Proposed Regulations require symmetrical choices, including a requirement that "[t]he path for a consumer to exercise a more privacy-protective option shall not be longer than the path to exercise a less privacy-protective option."[9] The Chamber agrees with the spirt of this approach, but the examples of implementation of this Proposed Regulation would indicate

[8] *Id*. At 1798.135(b)(2) (emphasis added).
[9] PR at § 7004(a)(2).

that consumer be given rigid binary choices or perfect symmetry as opposed[10] to more informed alternatives.

The CPPA should provide flexibility to both consumers and businesses that are reasonable and proportionate as opposed to perfect symmetry in presenting privacy options to consumers. There could be examples in which companies may need to inform consumers of the impact of an opt-out, or consumers may want to exercise more informed, nuanced preferences than a limiting "Accept All" or "Deny All."

IV. Dark Patterns and Consent

Under the CPRA, "dark pattern" usage does not constitute "consent."[11] The definition of a "dark pattern" significantly impacts the choice architecture employed by businesses. The Agency proposes to determine "[a] user interface is a dark pattern is the effect of substantially subverting or impairing user autonomy, decision-making, or choice, regardless of a business's intent"[12] or a method not in compliance with its choice symmetry proposals.[13]

The current proposals for the definitions of "dark patterns" could subject businesses to strict liability regarding the development and implementation of user interfaces. Companies that intend to create symmetry could still face liability. This interpretation of the statute's definition of a "dark pattern" creates at least tension with, if not a violation of, First Amendment principles by prohibiting speech, even if truthful and not misleading, that warns consumers of the consequences of their choices.

In theory, the Agency could initiate enforcement against a business experiencing technical, software, hardware, or other technology-related issues beyond its reasonable control. The regulations should consider the intent of a business in determining whether it is employing a "dark pattern" and not define the term in such a way to confer strict liability on businesses.

V. Privacy Policy Obligations Should Reflect the CPRA's Text

Regarding the contents of a privacy policy, the Proposed Regulations mandate "a comprehensive description of the business' online and offline practices regarding the collection, use, sale, sharing, and retention of personal information."[14] The CPRA does not include language in its privacy policy requirements about a "comprehensive description" or "offline and online practices." The final CPRA regulations should follow the authorizing statute and not create unanticipated requirements with undefined vague terms like "comprehensive description."

---

[10] *Id*. At § 7004(a)(2)(C).
[11] Cal Civ. Code § 1798.140(h).
[12] PR at § 7004(c).
[13] *Id.* At § 7004(b).
[14] Proposed Regulation § 7011(e).

VI. Data Retention Requirements Should be Flexible

The Proposed Regulations mandate businesses at the notice to be given at the time of collection to detail "the length of time the business intends to retain each category of personal information…or if that is not possible, the criteria used to determine the period of time it will be retained."[15] Such prescriptive requirements are difficult to comply with because businesses deal with various factors such as the consumer relationship, transaction duration, and other legal requirements.

VII. Service Provider Restrictions Should Reflect the CPRA Text

The example noted in Sec. 7050(c)(1) of the Proposed Regulations contradicts the CPRA text and should be revised. As currently drafted, the example purports to prohibit a form of advertising based on email addresses. It is unclear what the basis is for doing so, given that this practice is permitted under the statute. This example contradicts the statute and raises new questions and uncertainty for businesses beyond those called out in the example. To address this, the example should be clarified as follows: "*The social media company can also use a customer list provided by Business S to serve Business S's advertisements to Business's customers. However, it cannot use a list of customer email addresses provided by Business S to then target those customers with advertisements based on information obtained from other third-party businesses' websites, applications, or services."*

VIII. CPPA's Audit Authority Should be Used Responsibly.

The Proposed Regulations call for the CPPA to "audit a business, service provider, contractor, or person to ensure compliance with any provision of the CPRA."[16] The Agency proposed that such audits may be done to investigate potential violations, if collection or processing poses a high risk, or if an audit subject has a history of noncompliance with privacy laws.[17] The Agency asserts it need not announce an audit.[18]

Although the CPRA enables the CPPA to conduct compliance audits, the Agency must strike a balance between audits that protect consumer privacy and substantial interference with business operations. An audit is a resource-intensive exercise for both the Agency and a business. Without clear triggers and limitations, the Agency could conduct broad fishing expeditions, leading to mounting pressure to find some basis for an enforcement action. There is no legislative history to suggest that the CPRA's authority to conduct compliance audits was intended to be interpreted so broadly, compared to the much more typical authority granted to a law enforcement agency to seek information and documents from companies when they have

[15] Proposed Regulation § 7012(e)(4).
[16] Proposed Regulation § 7304(a)
[17] *Id*. At §7304(b).
[18] *Id*. At § 7304(c).

reason to believe that an entity may have violated the law. The Agency should also not engage in using third-party auditors who have a financial incentive to find a violation during such audits.

IX. Fair Enforcement

The California Privacy Rights Act required rulemaking to be finalized by July 1, 2022, and enforcement of the rules to begin a year later.[19] The business community understands demands upon the Agency and the delay in initiating the current rulemaking. The Chamber urges CPPA to clarify its plans for enforcement and effective dates of the CPRA regulations. Only some of the anticipated regulations have been drafted, with some of the most complex and potentially complex proposed rules have yet to be promulgated. The Agency should clarify that enforcement, in line with the spirit of the CPRA text, will not being until at least July 2024, and the rules should take effect in no sooner than January 2024. Requiring businesses to attempt to comply prior will lead to both business and consumer confusion as well as hastily implemented and sub-optimal operationalization of complex requirements. The Chamber understands that making rules takes time, but large-scale implementation at companies of complex compliance programming also requires time. Providing companies with sufficient time prior to beginning enforcement will provide consumers with greater protections and will provide predictability for business.

X. Customer Loyalty Programs

The Proposed Regulations misunderstand the key differences between financial incentives and customer loyalty programs. Unlike financial incentives, which are provided in exchange for the collection of consumers' personal information, customer loyalty programs are distinguished by their wholly different purpose, which is to provide price or service benefits within the existing business relationship to current customers who choose to voluntarily participate in these programs. Customer loyalty programs are therefore not offered to entice consumers to disclose personal information, but rather to strengthen an ongoing relationship the consumer already has with the business and that may lead to subsequent purchases by that consumer of the business's goods or services. The Board should amend the regulations to make it clear that a business offering a different price, rate, level, quality or selection of goods or services to an individual, including offering goods or services for no fee, is not offering a financial incentive if the offering is in connection with an individual's voluntary participation in a bona fide loyalty program.

XI. 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

[19] Cal. Civ. Code § 1798.185(d).

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.

If you have any further questions and need clarification, please contact me at jcrenshaw@uschamber.com or (202) 578-0009.

Sincerely,

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