

From: **Privacy ITNcorp** [REDACTED]
To: **regulations@cpha.ca.gov** <regulations@cpha.ca.gov>
Subject: Advertising Cookies must be a part of "Do Not Share" button
Date: 14.07.2022 09:58:12 (+02:00)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear CPPA,

The Text of Proposed Regulations - subsection (a)(4) of sec.7026:

"... because cookies concern the collection of personal information and not the sale or sharing of personal information. ..."

It is not a secret that majority of concerns regarding selling or sharing of personal information relate to the extensive processing of cookies. Cookies as unique identifiers are almost the only tool allowing to Ad Networks to organise profitable cross-context behavioral advertising.

When covered businesses allow Ad Networks to collect cookies such businesses SHARE personal information for cross-context behavioral advertising.

Thus, when consumers click "DO Not Share My Personal Information" the results of such a "click" must include also opting-out from "cookie sharing for cross-context behavioral advertising".

As a result, please kindly correct subsection (a)(4) of sec.7026 in order to allow businesses to include "sharing of cookies" (for cross-context behavioral advertising) into the "opt out from sharing".

Sincerely,

ITNCorp

From: **Thomas Gerhart** [REDACTED]
To: **regulations@cpha.ca.gov** <regulations@cpha.ca.gov>
Subject: CPHA Public Comments
Date: 25.07.2022 23:11:10 (+02:00)
Attachments: Comment - 45-Day Verificaiton Period.docx (2 pages), Comment - Deleting SPI.docx (2 pages), Comment - Indirect Collection.docx (1 page), Comment - Omitted Any.docx (1 page), Comment - Verification Process.docx (1 page)

Comment

What happens if a business creates a labyrinthine and dilatory verification process that cannot reasonably be completed in less than 45 days? (See, e.g., Text of Proposed Regulations, 11 Cal. Code Regs. § 7021 (proposed July 8, 2022) (“If the business cannot verify the consumer within the 45-day time period, the business may deny the request.”)).

Illustrative Example

Consumer has a business relationship with Business A. Business A and Business B have a business relationship where Business A passes consumer information to Business B for marketing. Consumer, not wanting Business B’s marketing, submits a Right to Delete request to Business B, whose process involves submitting Consumer’s information to Business B’s request web portal.

A few weeks after submitting the request, Business B sends Consumer a generic email that says Consumer must log into Business B’s web portal because action is required to complete the request. Consumer follows Business B’s instructions, which includes authenticating their identity via a secured access code sent to Consumer’s email address on file (which expires in 15 minutes from when it is requested). Once logged in, Consumer learns that Business B is asking them to verify their identity and the authenticity of the request. Consumer replies to Business B’s message in the web portal, confirming that the request is authentic by providing the name, phone number, and address that Business B has on file for Consumer.

Days later, Business B sends another uninformative and generic email to Consumer that indicates there is some unspecified thing Consumer must complete in their web portal. Again, Consumer logs in using the secured access code. However, this time, Business B is not sending Consumer the secured access codes for at least 30 minutes after they are requested, and the code expires 15 minutes after it is *requested*. Given the delayed access codes, it takes a few days before Consumer can log into the portal. For this additional step, Business B is now asking for information related to Consumer’s relationship with Business A (e.g., the VIN, make, model, and year of the car that Consumer purchased from Business A, which Business B has on file). Consumer submits that information via the web portal.

A week later, Business B sends another uninformative and generic email to Consumer, indicating there is some unspecified thing Consumer must complete in their web portal. As before, the secured access codes are expiring before they are emailed to Consumer.

This is where the example ends because I have not seen where this request to delete is going next. In theory, these verifications could result the verification taking longer than 45 days, meaning Business B could deny the request to delete as not being verified within that time frame.

Applicable Statute:

- Cal. Civ. Code § 1798.185 (amended Nov. 3, 2020, by initiative Proposition 24, Sec. 21. Effective Dec. 16, 2020. Operative Jan. 1, 2023, pursuant to Sec. 31 of Proposition 24.).

Relevant Regulation:

- Text of Proposed Regulations, 11 Cal. Code Regs. § 7021 (proposed July 8, 2022).

Possible Solution

Clarify that the 45-day window does not include delays on the part of or verifications being performed by the business. Rather, that it would be tied to inactivity on the part of the consumer.

Comment

May a business take consumer information, label it as something else, and refuse to delete that information when it receives a consumer's Request to Delete? In many instances, the category of Sensitive Personal Information, as defined in statute, should not be something that a business can refuse to delete because "it is reasonably necessary for the business, service provider, or contractor to maintain the consumer's personal information" for "internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business and compatible with the context in which the consumer provided the information." (Cal. Civ. Code §§ 1798.135(ae), 1798.105(d)(7)).

While I understand the necessity to retain some categories of Sensitive Personal Information for other reasons (e.g., retaining a Social Security Number for completing a transaction or to ensure a former customer pays a debt or risks being turned over to collections), in some cases there is no internal use that a consumer would expect for a business to maintain some forms of Sensitive Personal Information (e.g., a Social Security Number) after a business relationship has ended.

I leave room here for some Sensitive Personal Information (e.g., genetic information), which I could see a company maintaining in a disaggregated form. However, a disaggregated Social Security Number can still have severe, long-lasting consequences for a consumer in the event of a data breach.

Illustrative Example

Consumer has had a business relationship (customer/service provider) with Business A, a telecommunications company, for multiple years. Consumer, whose account is in good standing and has no outstanding balance, changes cell phone providers and transfers their phone number to the new provider. Consumer, aware that Business A collected Sensitive Personal Information when their business relationship first began, submits a Request to Delete that information. Business A asks Consumer to authenticate their identity by providing their name, phone number, and address. When a customer transfers their phone number to another provider, Business's practice is to delete the phone number from the account number field in their system and set the former customer's account number as their Social Security Number. Therefore, because Consumer transferred their phone number to a different provider, Business A cannot locate their information and asks for their Social Security Number instead. Consumer provides Business A with their Social Security Number, and Business A confirms it was able to use that number to locate Consumer's old account.

Consumer asks whether Business A will delete Consumer's Social Security Number under this request. Business A explains that it will "never delete that number" because Consumer transferred their phone number to the new provider. When Consumer transferred their number, Business A set Consumer's Social Security Number as Consumer's "account number" because the previous value in that field was Consumer's phone number. Now, Business A is maintaining Consumer's, as well as many other consumers', Social Security Numbers as an identifier for former customers under these circumstances. Most problematically, the business refuses to delete the Sensitive Personal Information because they now classify it as an "account number" and claim it is reasonably necessary for business purposes.

Applicable Statutes:

- Cal. Civ. Code § 1798.105(d) (amended Nov. 3, 2020, by initiative Proposition 24, Sec. 5. Effective Dec. 16, 2020. Operative Jan. 1, 2023, pursuant to Sec. 31 of Proposition 24.).
- Cal. Civ. Code § 1798.135(ae) (amended Nov. 3, 2020, by initiative Proposition 24, Sec. 13. Effective Dec. 16, 2020. Operative Jan. 1, 2023, pursuant to Sec. 31 of Proposition 24.).

Relevant Regulations:

- Text of Proposed Regulations, 11 Cal. Code Regs. § 7002(b) (proposed July 8, 2022).
- Text of Proposed Regulations, 11 Cal. Code Regs. § 7022 (proposed July 8, 2022).

Possible Solution

Clarify that re-classifying consumer information is insufficient to constitute deletion. Possibly create a carve out for some forms of Sensitive Personal Information where disaggregation is insufficient because of the latent harm that a data breach would still carry. Under these regulations, it is not “reasonably necessary” for a business to use Sensitive Personal Information for a purpose that otherwise could be served by data that is not sensitive.

Comment

Does the phrase “collected from the consumer” include “indirect collection”? If not, including that term would close a regulatory loophole. Without that term, a consumer’s right to delete information from a business could be limited only to a business that has had direct contact with the consumer. It could limit a consumer’s complete control over their data if a business received the consumer’s information either via sharing or purchase. A byproduct of this omission could result in businesses setting up strawman entities to collect data and then share it with the main company, thereby circumventing the consumer’s ability to request the deletion.

Illustrative Example

Consumer provides information to Business A, who then sells or shares that information with Business B. Later, Business A closes permanently. Business B targets marketing at Consumer, who never had contact with Business B. Consumer submits a request to Business B to delete the information it has about the consumer. Business B denies the request because, while it has Consumer’s information, it did not directly collect that information from Consumer.

Applicable Statute:

- Cal. Civ. Code § 1798.105(a) (amended Nov. 3, 2020, by initiative Proposition 24, Sec. 5. Effective Dec. 16, 2020. Operative Jan. 1, 2023, pursuant to Sec. 31 of Proposition 24.) (“A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.”).

Relevant Regulations:

- Text of Proposed Regulations, 11 Cal. Code Regs. § 7000(v) (proposed July 8, 2022).
- Text of Proposed Regulations, 11 Cal. Code Regs. § 7000(bb) (proposed July 8, 2022).
- Text of Proposed Regulations, 11 Cal. Code Regs. § 7011(e)(2)(B) (proposed July 8, 2022).

Possible Solution

Specify that collection may be direct or indirect and define those terms for purposes of these regulations.

Comment

Regarding Requests to Delete, the regulations do not adopt the same language as the statute does regarding what information may be deleted. The statutes say, “A consumer has the right to request that a business delete *any* information . . .” (emphasis added). However, the regulations omit the “any” twice. (*See, e.g.*, Text of Proposed Regulations, 11 Cal. Code Regs. § 7000(v) (proposed July 8, 2022) (“‘Request to delete’ means a consumer request that a business delete ~~any~~ personal information . . . pursuant to Civil Code section 1798.105”).).

I know regulations cannot eliminate a right granted by statute, but not all people or businesses may be aware of that fact. A discrepancy like this could result in a business attempting to make a good faith argument that uses this regulation as a basis for not deleting certain information. Would it not be in the best interest of the California Privacy Protection Agency to resolve this discrepancy now and potentially avoid needless litigation about whether this difference has merit?

Illustrative Example

n/a

Applicable Statute:

- Cal. Civ. Code § 1798.105(a) (amended Nov. 3, 2020, by initiative Proposition 24, Sec. 4. Effective Dec. 16, 2020. Operative Jan. 1, 2023, pursuant to Sec. 31 of Proposition 24.) (“A consumer shall have the right to request that a business delete **any** personal information about the consumer which the business has collected from the consumer.”) (emphasis added).

Relevant Regulations:

- Text of Proposed Regulations, 11 Cal. Code Regs. § 7000(v) (proposed July 8, 2022).
- Text of Proposed Regulations, 11 Cal. Code Regs. § 7000(bb) (proposed July 8, 2022).

Possible Solution

Include the word “any” in between “delete” and “personal information” in the identified locations.

Comment

I am concerned that there are still avenues for a business to make a Request to Delete unnecessarily cumbersome by requiring a requestor to authenticate information that, while the information may not necessarily be wrong, is out of date.

Illustrative Example

Consumer has had a business relationship with Business for multiple years. After the relationship ends, Consumer moves multiple times and changes their phone number. Consumer realizes they submitted Sensitive Personal Information to Business and submits a Request to Delete that information. Business asks Consumer to authenticate their identity by providing their name, phone number, and address. Consumer provides their current information, and the request is denied because, as they are told, the information on file does not match what they provided. Consumer tries again with their former address but is wrong again because they had moved multiple times. Now, Business need not reply to Consumer's requests for 12 months.

Applicable Statute:

- Cal. Civ. Code § 1798.185 (amended Nov. 3, 2020, by initiative Proposition 24, Sec. 21. Effective Dec. 16, 2020. Operative Jan. 1, 2023, pursuant to Sec. 31 of Proposition 24.).

Relevant Regulation:

- Text of Proposed Regulations, 11 Cal. Code Regs. § 7060 (proposed July 8, 2022).

Possible Solution

One current, widespread practice is used when a customer is locked out of their account. Businesses (including those that handle sensitive financial information) deem it sufficient to authenticate the customer's identity by emailing or text messaging a secured access code to the phone number or email address on file. If that is the only thing a business needs to authenticate the customer for purposes of giving them access to their account, perhaps something similar could be employed to authenticate a person's identity for a Request to Delete. It is not reasonable for a business to ask for more information in a Request to Delete than it would ask in order to give a customer access to a locked account.

By requiring a requestor to have access to the phone number or email address associated with their information, that would make it harder for an imposter to fraudulently request an account deletion. It also uses a system that many businesses already have in place without requesting more information than is necessary.

From: **Chris Riley** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment of R Street
Date: 10.08.2022 10:27:08 (+02:00)
Attachments: R Street CPPA Public Comment.pdf (5 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello,

Please find attached the public comment of the R Street Institute in the CPPA's pending rulemaking proceeding, and feel welcome/encouraged to contact me with any follow up or questions.

Thanks,
Chris Riley



1212 New York Ave. N.W.
Suite 900
Washington, D.C. 20005
202-525-5717

Free Markets. Real Solutions.
www.rstreet.org

COMMENTS OF THE R STREET INSTITUTE

The R Street Institute respectfully submits these comments in response to the Notice of Proposed Rulemaking published July 8, 2022 regarding the California Privacy Protection Agency's (CPPA) proposed changes to the California Code of Regulations to align the existing California Consumer Privacy Act regulations with the Consumer Privacy Rights Act of 2020 (CPRA).

We appreciate the challenge facing the Agency: In many ways CPRA directly mandates specific changes to the regulations, whether or not such changes will result in better public policy or better outcomes for Californians. In most instances, we regard the proposed regulations as a reasonable attempt to implement the adopted law, but we note some exceptions that are problematic, for which we will propose an alternative approach.

I. Context

The new privacy regulations are being debated in California even as Congress considers a federal data privacy and security law, which could potentially render all or part of this work moot through federal preemption.¹ At the R Street Institute, we believe a comprehensive federal data privacy and security law is essential for national security, consumers and industry, but we also believe there is a role for states. R Street recently offered multiple recommendations to pass a federal law based on addressing traditional roadblocks through compromise after 120+ stakeholder engagements.²

Part of the compromise requires finding a middle ground between state and federal privacy enforcement and applicability. While we believe in strong preemption to create a uniform federal standard, there should be carve-outs for select state legislation, room for state enforcement and a role for state data protection authorities like the CPPA.³ From that perspective, it is worthwhile to continue with this process

¹ Brandon Pugh and Sofia Lesmes, "Marking Up Momentum: What's Next for the ADPPA," R Street Institute, July 21, 2022. <https://www.rstreet.org/2022/07/21/marking-up-momentum-whats-next-for-the-adppa>.

² Tatyana Bolton et al., "The Path to Reaching Consensus for Federal Data Security and Privacy Legislation," R Street Institute, May 26, 2022. <https://www.rstreet.org/2022/05/26/the-path-to-reaching-consensus-for-federal-data-security-and-privacy-legislation>.

³ Tatyana Bolton et al., "Preemption in Federal Data Security and Privacy Legislation," R Street Institute, May 31, 2022. <https://www.rstreet.org/2022/05/31/preemption-in-federal-data-security-and-privacy-legislation>.

of developing CPPA rules despite the possibility of a federal privacy law, as these efforts are not necessarily contradictory.

As another crucial contextual note, the consideration of cybersecurity provisions and risk assessments is critical to an effective law and the protection of data. However, the Notice of Proposed Rulemaking states that rules on these topics will be covered by a future rulemaking. While we understand the need to limit rulemaking, these sections should be prioritized because there can be no privacy in practice without security, and businesses may have inadequate guidance to conduct audits and assessments. Consider a company that transparently informs its users of its data use practices on the information it collects, but has weak access permissions for this information. There would be inadequate defense against unauthorized access and the company would not be able to provide adequate data protection to its customers.

To mitigate this, a symbiotic relationship between security and privacy should be fostered. This does not mean that the rulemaking now has to mandate certain encryption standards, for instance, but cybersecurity should be taken into consideration at all stages and not shelved for future action.

II. Consequences

The proposed regulations will be costly for California business and, in turn, California citizens. The CPPA estimates that the proposed regulations will have a cost impact of \$127.50 per business, which represents the labor costs of updating website information.⁴ This cost average is misleading in part, because it assumes businesses are in compliance with current laws and it only addresses the new economic impact, with the cost of existing regulations being covered by previous filings. And even beyond that legacy burden, the scale and complexity of just the new requirements would seem to require not only drafting of information, but revamped internal processes to ensure the requested data is available and accurate, and likely legal counsel review to ensure compliance. Together, the broader cost and burden of compliance would seem to be significantly higher, especially for smaller businesses. Given that these regulations are estimated to impact over 66,000 businesses in California, with nearly 44,000 being small businesses, both the individual and collective costs of compliance will be significant in a way that dwarfs the nominal regulatory estimate.⁵

Even more than the implementation cost, R Street is concerned by the possibility of rules that will drown users in excessive and unusable information. In the long history of privacy policy work, perhaps no challenge is more insidious than over-sharing. Numerous studies, such as a 2017 article co-authored by usable privacy expert Professor Lorrie Cranor, indicate that attempts to provide users with all information that may be relevant to a consumer decision are ineffective.⁶ From the history of corporate privacy policies to the European Union's infamous "cookie directive," forcing users to confront significant information at the outset of engagement rarely achieves the right balance of informing and empowering effective consumer choice.

⁴ "Notice of Proposed Rulemaking regarding implementation of the Consumer Privacy Rights Act of 2020," California Privacy Protection Agency, July 8, 2022. https://cppa.ca.gov/regulations/pdf/20220708_npr.pdf.

⁵ "Economic and Fiscal Impact Statement regarding proposed California Consumer Privacy Act Regulations" California Privacy Protection Agency, June 28, 2022. https://cppa.ca.gov/regulations/pdf/std_399.pdf.

⁶ Florian Schaub et al., "Designing Effective Privacy Notices and Controls," IEEE Internet Computing, June 16, 2017. <https://ieeexplore.ieee.org/document/7950873>.

From that perspective, section 7011 mandates a substantial volume of specific information to be included within privacy policies. While the language includes ample softening descriptors like “explanation” and “in a manner that provides consumers a meaningful understanding” (e.g. 7011(e)(1)(C)), it seems implausible that ordinary consumers will spend the necessary time to read an individual company’s explanations no matter how plain the language. Similarly, few if any consumers are likely to compare across similar services the “categories of personal information the business has collected” (7011(e)(1)(A)) in order to make a choice among possible market options for services. The attempt at homogenizing privacy policies reflected in these regulations appears to make such comparisons more feasible, but for the everyday consumer, it will more likely have the opposite effect, by making it more difficult for a company to compete on the clarity and efficacy of its privacy policies and how it frames its strengths on privacy to the consumer.

To provide an example of the fragility of overly-specific notice obligations in the proposed rules, the proposed 7011(e)(6) requires a business providing a notice at the point of data collection to inform the user of any other businesses (“third parties”) who “control” the collection of such information. Yet, the proposed 7012(g)(1) requires all such third parties to also provide a notice to the user, “at collection.” If “at collection” means that users must have visibility into the third parties’ notice when viewing the first party website, it would seem that users would be presented with a notice from the first party which names or describes the practices of any third parties involved, and also a separate notice from each of the third parties collecting data: double notification regarding each of the third parties. Loading “www.yahoo.com” in Firefox (updated to its most current version) at the time of this writing, twenty four (24) separate domains with tracking content are identified; each of these is designed to collect information from the user, although there is overlap among the parties providing them. Judiciously narrowing this set down to, say, ten unique third parties indicates that a user would be presented with one notice from Yahoo that identifies all ten of these parties, and ten additional, separate notices.

An alternative interpretation of the rules that limits redundancy would be to follow the example presented in 7012(g)(4)(A), where the third party at issue—“Business G”—is directed to provide its notice “on its homepage,” as in the website of the analytics service. Such a website would presumably be designed for Business G’s customers (other businesses) not end users, and it’s unclear whether any would visit Business G’s website in order to read such a notice, as well as whether visiting Business G’s website would turn the relationship into a first party relationship, as the user is now aware of Business G, visiting their website, and expecting to interact with them.

A more general notice that gives more opportunity for businesses to tailor notices related to third party collection and control, in a streamlined manner optimizing for utility to the user, would likely be more effective in practice than the specific guidance offered in the proposed rules.

III. Other concerns

The CPPA is obligated to implement the CPRA’s prohibition on “dark patterns,” the design of user interfaces to encourage a user to make certain business-preferred choices. In theory, this goal is commendable, and helps ensure the smooth and accurate operation of markets through informed and

effective consumer choice. However, the proposed implementation rules regarding “symmetry in choice” would impose paternalistic and artificial limitations on product design that go beyond what is needed to implement the CPRA obligation. Several of the proposed examples create vague risk and the possibility of user frustration:

- Example (A) imposes a hard limit on the number of clicks involved in making a choice, an artificial limitation when some options may involve sub-options, or where their selection may be better informed by presenting the user with additional information before making a decision.
- Example (C) presumes that a user would only wish to choose “Accept All” or “Decline All”, whereas modern practice typically gives users *more* choice than this, including the ability to allow, for example, analytics collection where the website operator may benefit. Ignoring the possibility that the user may wish to support the website operator, while still being protected from cross-site tracking, unnecessarily structures the user and the website in a “hostile by default” relationship.
- Examples (D) and (E) both impose a vague limitation that a business-preferred option not be presented in a more “eye-catching color” than others. Even ignoring that this bears no relation to the rule itself, which is limited to the length of path that must be followed (not the visual appeal of the path), the requirement is vague and undoubtedly will be the subject of litigation, and likely to lead to businesses forcing uniform colors for buttons, unnecessarily and arbitrarily. By extension, though, would positioning the “Accept All” button on the left be viewed as preferable, given that the English language is read from left to right? Presumably this would not be viewed as an unfair advantage or overly major skew on a user’s fair choice.

IV. Conclusion

While the proposed regulations tackle an admirable goal in that they seek to offer useful clarity and examples to help businesses comply, in the context of the volume of notice and obligation under the law, the excessive specificity, potential redundancy, and in some instances vagueness together create unnecessary risk of unjustified litigation and a likelihood of over-compliance that goes beyond protecting users and data and produces unhelpful homogenization and a deluge of detail that will not lead to consumers feeling more informed or empowered.

We recommend that CPPA consider modifications to the proposed rules as follows:

- Prioritize cybersecurity alongside privacy to invest in total user protection;
- Streamline, reduce, and uplevel notice obligations as much as possible within the confines of the statute, giving businesses room to invest in meaningful user notice; and
- Scale back and clarify “symmetry in choice” requirements to realize the statutory duty of limiting “dark patterns” without unnecessary and harmful restrictions on user interface design.

Whether for good or ill, CPRA is part of California law, absent future approved propositions or amendments to the state constitution. The proposed regulations are a reasonable start to providing clarity in the implementation of CPRA, though further improvements and tailoring would help minimize unnecessary obstacles and risk.

Respectfully submitted,

Chris Riley
Senior Fellow, Internet Governance

Brandon Pugh
*Senior Fellow, Cybersecurity and
Emerging Threats*

Sofia Lesmes
*Senior Research Associate,
Cybersecurity and Emerging Threats*

R Street Institute
1212 New York Ave. N.W.,
Suite 900
Washington, D.C. 20005

Contact: 

From: **Donna Steward** [REDACTED]
 To: **Regulations** <Regulations@cpha.ca.gov>
 Subject: CPPA Public Comment
 Date: 11.08.2022 05:31:48 (+02:00)
 Attachments: HITRUST Comment CA CPRA Consumer Rights Regulations 081022.pdf (4 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello –

Attached are comments related to draft regulations implementing the California Privacy Rights Act. These comments are submitted on behalf of HITRUST, a globally recognized data security and risk management organization.

We hope the comments are helpful as this regulation progresses. Please feel free to contact me at [REDACTED] [REDACTED] should you have any questions or desire any additional information as the regulation moves forward.

Sincerely,
 Donna Steward



Donna Steward

Director, Government Affairs

[REDACTED]
 [REDACTED]
 [REDACTED]



CONFIDENTIALITY NOTICE: The contents of this email message and any attachments may contain confidential, proprietary or legally privileged information and/or may be subject to copyright or other intellectual property protection and be legally protected from disclosure. This information is intended only for use of the addressee or addressees named above for its intended purpose. If you are not the intended recipient of this message or their agent, or if this message has been addressed to you in error, please immediately alert the sender by reply email and then delete this message and any attachments. If you are not the intended recipient, you are hereby notified that any use, dissemination, copying, or storage of this message or its attachments is strictly prohibited. CONFIDENTIALITY NOTICE: The contents of this email message and any attachments are intended solely for the addressee(s) and may contain confidential and/or privileged information and/or may be subject to copyright or other intellectual property protection and be legally protected from disclosure. If you are not the intended recipient of this message or their agent, or if this message has been addressed to you in error, please immediately alert the sender by reply email and then delete this message and any attachments. If you are not the intended recipient, you are hereby notified that any use, dissemination, copying, or storage of this message or its attachments is strictly prohibited.



6175 Main Street
Suite 400
Frisco, TX 75034

855.HITRUST
(855-448-7878)
www.HITRUSTAlliance.net

August 10, 2022

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

RE: California Privacy Rights Act Regulation Comment

Dear Mr. Soublet:

Thank you for the opportunity to provide comment on regulations moving forward to implement the California Privacy Rights Act (CPRA). The following comments are submitted on behalf of HITRUST, a globally recognized leader in information risk management and assurance reporting. HITRUST was established in 2007 as a not-for-profit standards development and certification organization that champions programs to safeguard sensitive information and manage information risk for organizations across all industries and in all geographic regions.

The CPRA includes requirements to inform consumers on the types of consumer and sensitive data businesses collect and how the collected data is used and/or sold for use outside of its original intent. The law also requires businesses collecting, storing, and utilizing consumer data to ensure the security of this data. These requirements provide structure for the protection of collected data, but there are ambiguities in the requirements that could still allow for the theft and misuse of consumer information. These ambiguities should be clarified in the regulations in order to improve consumer protections and ensure the intent of the law is fulfilled.

The combined requirements of the California Consumer Privacy Act (CCPA) and the CPRA establish a comprehensive and complex approach to the protection of consumer information in the state. Given the complexity of these laws, it is essential that the implementing regulations clarify ambiguities and provide clear direction to covered businesses to ensure they are able to fulfill their obligations and provide the level of security necessary to protect and preserve consumer data. Toward this end, HITRUST encourages the California Privacy Protection Agency (CPPA) to include the following definitions in the regulations to eliminate ambiguity, clarify data security requirements and improve the overall protection of consumer data:

- I. A strong definition of “reasonable security procedures and practices” that aligns with national recommendations and provides clarity and guidance for those subject to and enforcing the law.
- II. A clear definition of “cybersecurity audit” that comports with the reasonable security procedures and practices implemented by a business subject to the law.

I. Include a clear definition of “reasonable security procedures and practices” that aligns with national recommendations and provides clarity and guidance for those subject to and enforcing the law.

In addition to concerns regarding the unauthorized sale and use of sensitive data by businesses, consumers are faced with ever-evolving cyber threats that expose their personal data to financial and reputational risks. To reduce the likelihood of data theft and other data system incidents, the CCPA requires businesses to “implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”¹ This requirement is an important directive to businesses and should be viewed as the foundation of a business’ data security program. Unfortunately, the current law falls short of defining what constitutes a reasonable security procedure and practice. Failure to establish

¹ California Civil Code 1798.81.5(b)

a clear definition that provides businesses with the direction they need to select the most appropriate procedures could lead to the adoption of security practices that fail to provide desired protections.

Without a clear definition of “reasonable security procedures and practices” businesses have wide discretion regarding which practices to adopt, and due to other needs and demands, may choose practices that provide lower levels of data protection than is required. Businesses may also lack a fundamental understanding of which security practices provide the best protection, resulting in choices that make it impossible for them to ensure adequate protections are in place. Each of these situations can lead to security gaps and system vulnerabilities that will make it very difficult for a system to substantively defend against evolving threats. Quite simply, the privacy objectives of the CCPA and CPRA cannot be achieved without adequate security, and adequate security will require a clear definition of reasonable security procedures and practices.

The need for a clear definition is aptly illustrated by a May 17, 2022, release by the Cybersecurity and Infrastructure Security Agency (CISA) that identified numerous weak controls and other poor cyber hygiene practices that threat actors are continuing to use to gain initial access to a potential victim’s system.² The release underscores the importance of ensuring strong data security practices, i.e. controls, are in place and further focuses the need for organizations to adopt a security framework that helps identify the controls that will provide the highest level of protection for the organization.

To ensure businesses adopt security procedures and practices that are the most applicable to their organization and unique needs, the definition should require businesses adhere to the requirements of an industry recognized security framework and, more specifically, a framework that will help businesses select controls based on an analysis of risk. Such security frameworks provide a reliable, standardized, systematic way to mitigate risk, regardless of a business’ complexity, and can act as a blueprint for helping an organization identify and adopt the security controls necessary to effectively manage that organization’s risk.

The NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework)³ is quickly becoming the de facto standard for communicating desired cybersecurity objectives to internal and external business stakeholders and supports the integration of security controls from a multitude of frameworks to achieve those objectives. In fact, multiple frameworks are readily available, and many are already highly familiar to thousands of organizations that have either independently chosen or are required to use such a framework. Many frameworks are industry and data agnostic, such as those provided by NIST, the International Standards Organization (ISO) / International Electrotechnical Commission (IEC), and HITRUST, while other more specific data security requirements have moved forward as a result of industry regulation such as those provided by the Payment Card Industry Security Standards Council.

The most effective security frameworks emphasize holistic security controls as the primary means to protect systems and collected information, include elements of data privacy protections, and are flexible and scalable so that a business can evaluate their unique needs and develop a comprehensive program that is commensurate with the business size

² Cybersecurity and Information Security Agency. *Alert (AA22-137A) - Weak Security Controls and Practices Routinely Exploited for Initial Access*. Accessed May 17, 2022, from <https://www.cisa.gov/uscert/ncas/alerts/aa22-137a>.

³ NIST (2018, 16 Apr). *Framework for Improving Critical Infrastructure Cybersecurity (v1.1)*. Gaithersburg, MD: Author. Accessed Aug 8, 2022, from <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

and resources. Industry recognized frameworks such as NIST SP 800-53,⁴ ISO/IEC 27701,⁵ and the HITRUST CSF,⁶ which integrates both NIST and ISO/IEC frameworks (among many others), each contain the elements listed above and provide some of the highest levels of protection. It may also be helpful to note that NIST SP 800-53 and the HITRUST CSF are available at no cost to organizations throughout the country, and ISO/IEC 27701 is available for a nominal fee, providing access for all with interest and need.

II. Include a clear definition of “cybersecurity audit” that comports with the reasonable security procedures and practices implemented by a business subject to the law.

The CPRA requires businesses whose processing of consumers’ personal information presents significant risk to consumers’ privacy or data security to conduct an annual cybersecurity audit, and charges the CPPA with defining the scope of the audit and the process for determining the audit is thorough and independent.⁷ While HITRUST understands that specifications related to the required audits will be detailed in a separate draft regulation, we believe it is important to ensure cybersecurity audits are commensurate with and considered within the context of reasonable security procedures and practices. To ensure these items are viewed in context with each other, HITRUST suggests that a definition of “cybersecurity audit” should be included in the July 8, 2022, draft, with the details for the audit requirements reserved for the later draft.

Cybersecurity audits (also understood as data protection, information security, or cybersecurity assessments) are critical to completely understanding the processing data flows of personal and sensitive data across business information systems and for determining whether a business has successfully selected and implemented an appropriate set of security practices (controls) enabling it to comply with applicable laws and defend against a range of threats to personal and sensitive data.

The definition of cybersecurity audit should ensure that the audit provides reliable and consistent results no matter how many times the audit is performed or who performs it. A clear definition of the type of audit that is to be performed and the scope of items the audit is to cover will help ensure each audit provides the same level of reliability. Audits that are merely high-level checklists or lack the strength or confidence / assurances necessary to meaningfully evaluate the data processing environment and associated compliance levels, will fail to provide meaningful information on the system’s ability to protect consumer data.

To be meaningful, the definition of audit must ensure the results provide reliable information about a business’ ability to safeguard information and meet its compliance obligations. In order to do so, the audit must evaluate the selection, implementation and use of the reasonable security procedures and practices employed by the business. The structure of the audit must also ensure the audit results can be reasonably replicated irrespective of the individual or organization performing the review.

In order for the required audit to demonstrate reliability and meet the law’s objectives in a meaningful way, we suggest developing a clear definition for “cybersecurity audit” that, at a minimum, includes the following characteristics:

- Transparency – The audit report produced should clearly state the audit approach used (e.g., inquiry only, documentation-based review), who performed the audit (e.g., self, independent third-party auditor), the specific

⁴ JTF (2020, Sep). *Security and Privacy Controls for Information Systems and Organizations* (NIST SP 800-53 Rev. 5). Gaithersburg, MD: NIST. Accessed August 8, 2022, from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>.

⁵ ISO/IEC (2013). *Information Technology - Security Techniques - Information Security Management Systems - Requirements* (ISO/IEC 27001:2013). Geneva: Author. Accessed August 8, 2022, from <https://www.iso.org/standard/54534.html>.

⁶ HITRUST (2022). HITRUST CSF: *One Framework, One Assessment, Globally*. Accessed from <https://hitrustalliance.net/product-tool/hitrust-csf/>.

⁷ California Civil Code 1798.185(a)(15)(A)



6175 Main Street
Suite 400
Frisco, TX 75034

855.HITRUST
(855-448-7878)
www.HITRUSTAlliance.net

security practice controls and procedures assessed, how those controls and procedures were evaluated and scored, and the final audit results.

- Scalability – The audit requirements must allow the approach to be suitably scaled to the size and type of the business (e.g., self-assessment for the lowest volume businesses, evidence-based audits by independent auditors for highest volume businesses) based on factors such as volume of personal and sensitive records processed and other relevant inherit risk factors specific to the business’ operations.
- Consistency – The audit’s evaluation, documentation, and reporting requirements must be extremely clear, so that audits are uniformly performed, documented, and reported—regardless of the individual or professional services firm performing the audit.
- Accuracy – The audit results must accurately reflect the state of the controls implemented in the business’ environment and must identify the mechanisms in place to facilitate the accurate evaluation and scoring of the implemented controls and procedures.
- Integrity – The audit must include processes to ensure it is conducted faithfully and that the audit results are reported accurately and truthfully.

Even with the flurry of media activity highlighting the vulnerability of systems to breach by increasingly sophisticated threat actors and nation states, the number of reported breaches continues to go up. Most unfortunate in these situations is that many breached organizations believed they had adequate and appropriate controls in place. In order for a cybersecurity audit to provide meaningful information, it is essential that it be transparent, scalable, consistent, accurate and ensure overall integrity of the assessment process.

Further, HITRUST recommends that the state address ambiguity over whether a business can “carve out” review of the data processing operations performed by third-party organizations on their behalf. When determining the scope of any audit of a business that outsources relevant processes to third parties (e.g., cloud hosting providers, colocation providers, managed service providers), decisions must be made as to whether the security practice controls performed by those outsourced providers should be included in the scope of the audit. Audits taking an “inclusive” approach are generally viewed as more robust and as providing a higher level of confidence / assurance than audits that take an “exclusive” or “carve-out” approach for such controls. Today different assurance programs have different expectations in this regard; for example, CMMC does not allow carve-outs while AICPA SOC2 assessments do.

Thank you again for the opportunity to provide comment as you develop the regulations necessary to implement the California Privacy Rights Act. I look forward to engaging in the process as you move forward and hope you will feel free to contact me at either [REDACTED] or [REDACTED], with any questions or requests for additional information.

Sincerely,

Donna Steward
Director, Government Affairs

From: **Howard Fienberg** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
Subject: CPPA Public Comment
Date: 11.08.2022 10:35:02 (+02:00)
Attachments: Insights-Association-comments-CPRA-8-11-22.pdf (5 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Rulemaking comments from the Insights Association attached.

Cheers,
Howard Fienberg
Senior VP, Advocacy
Insights Association

[REDACTED]
1629 K Street NW, Suite 300
Washington, DC 20006

Connect with us:

[InsightsAssociation.org](https://www.insightsassociation.org) | [Engage Community](#)
[Facebook](#) | [Twitter](#) | [LinkedIn](#) | [LinkedIn Group](#)



California Privacy Protection Agency
 Attn: Brian Soublet
 2101 Arena Blvd.
 Sacramento, CA 95834
regulations@coppa.ca.gov

August 11, 2022

Re: CPPA Public Comment of Insights Association on CPRA Rulemaking

Mr. Soublet,

The Insights Association (“Insights”) submits the following comments regarding the proposed regulations relating to the California Privacy Rights Act of 2020 (“CPRA”).

Representing more than 770 individuals and companies in California and more than 5,500 across the United States, Insights is the leading nonprofit trade association for the market research¹ and data analytics industry. We are the world’s leading producers of intelligence, analytics and insights defining the needs, attitudes and behaviors of consumers, organizations, employees, students and citizens. With that essential understanding, leaders can make intelligent decisions and deploy strategies and tactics to build trust, inspire innovation, realize the full potential of individuals and teams, and successfully create and promote products, services and ideas.

CPRA is going to have a profound impact on the business community, including the market research and data analytics industry. Small and medium-sized research firms in particular will face tremendous costs in updating and expanding on their already-extensive compliance efforts in connection with the California Consumer Privacy Act of 2018 (“CCPA”). Accordingly, and on behalf of our members, we commend your decision to seek input on the proposed regulations and are grateful for the opportunity to comment.

1. Bring CPRA in line with draft federal privacy legislation and other state laws by adding audience measurement to the list of “business purposes”

As you are aware, CPRA requires that contracts with service providers “prohibit[] the person from...[c]ombining the personal information that the service provider receives from, or on behalf

¹ Market research, as defined in model federal privacy legislation from Privacy for America, is “the collection, use, maintenance, or transfer of personal information as reasonably necessary to investigate the market for or marketing of products, services, or ideas, where the information is not: (i) integrated into any product or service; (ii) otherwise used to contact any particular individual or device; or (ii) used to advertise or market to any particular individual or device.” See Part I, Section 1, R: <https://www.privacyforamerica.com/overview/principles-for-privacy-legislation-dec-2019/>

of, the business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer,” with the exception that the service provider “may combine personal information to perform any business purpose as defined in [the] regulations.”

This restriction has implications for certain methodologies used in our industry which we believe the Agency may not have intended. Specifically, conducting audience measurement requires de-duplicating the relevant data, which in turn requires combining, at least temporarily, the relevant data from the client business with a research firm’s own internal data. Such a combination, and audience measurement more generally, is presumably not the type of activity the Agency intended to restrict. Accordingly, we request that audience measurement be added to the CPRA’s list of “business purposes.”

As you may be aware, this change by the Agency would bring CPRA in line with other privacy legislation and laws. **Draft federal legislation and extant state privacy statutes already make an accommodation for audience measurement.** For example, the American Data Privacy and Protection Act (H.R. 8152) exempts from the definition of targeted advertising “processing covered data solely for measuring or reporting advertising or content, performance, reach, or frequency, including independent measurement.”² We urge the Agency to leverage the foregoing definition, which we believe most completely captures audience measurement activities. Extant state laws in Colorado, Connecticut and Utah may also, of course, provide further guidance.³

Finally, regardless of the foregoing suggestion, we would also urge the Agency to clarify that such audience measurement activities do not constitute “cross-contextual advertising,” to avoid any ambiguity in the regulations, including if audience measurement is designated as a business purpose.

2. Limit the opt-out preference signal requirement to firms that meet one of the first two prongs of the CPRA’s “business” definition.

As the Agency is aware, there are three different ways for an organization to be defined as a “business” under the CPRA: (1) annual gross revenues in excess of \$25 million; (2) buying, selling, or sharing the personal information of at least 100,000 consumers or households; or (3) deriving 50 percent or more of its annual revenues from selling or sharing personal information.

² See American Data Privacy and Protection Act (pp. 15-16):

<https://www.insightsassociation.org/Portals/INSIGHTS/xBlog/uploads/2022/8/5/AmendmentsAdoptedbyHouseEnergyANDCommerceCommitteeDuringJuly2022MarkuptoJuly182022AINSPDF.pdf>

³ See UTAH CONSUMER PRIVACY ACT (S.B. 227), available at <https://le.utah.gov/~2022/bills/static/SB0227.html> (“‘Targeted advertising’ does not include...processing personal data solely to measure or report advertising performance, reach, or frequency”); CONNECTICUT DATA PRIVACY ACT (S.B. 6), available at <https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF> (“‘Targeted advertising’ does not include...processing personal data solely to measure or report advertising frequency, performance or reach.”); COLORADO PRIVACY ACT (SB21-190), available at https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf (“‘TARGETED ADVERTISING’...DOES NOT INCLUDE...PROCESSING PERSONAL DATA SOLELY FOR MEASURING OR REPORTING ADVERTISING PERFORMANCE, REACH, OR FREQUENCY”).

Because the third prong is not tied in any way to business size or processing volume, it includes a substantial number of small and medium-sized firms in the market research and data analytics industry. Firms who are subject to CPRA solely on the basis of this third prong should be exempt from implementing a solution to respond to opt-out preference signals.

In order to respond to these signals, firms will likely have to hire outside expertise to implement a technological solution, an expense which will be potentially significant for smaller firms. That expense may, moreover, be recurring — i.e., firms will likely have to update or at least review the technology regularly as opt-out signals evolve. Because this method for submitting an opt-out request is in addition to already-existing methods for submitting opt-out requests, we believe limiting the preference signal requirement as we propose would allow the Agency to balance the interests of small businesses without hampering the opt-out right of California consumers.

Alternatively, the Agency could limit the preference signal requirements based on smaller limits than those in the CPRA’s “business” definition (e.g., firms that do \$15 million in revenue or deal with at least 50,000 records), to protect the smallest businesses from overly onerous regulatory requirements.

3. Limit processing which presents a “significant risk” to consumers’ privacy or security to highly sensitive personal information, such as financial account information

The CPRA directs the Agency to issue regulations “requiring businesses whose processing of consumers’ personal information presents significant risk to consumers’ privacy” to perform annual cybersecurity audits and submit regular risk assessments to the Agency.

We respectfully request that processing which presents a “significant risk” be limited to processing of highly sensitive personal information, such as financial account or payment card information, social security numbers, or other personal information which, if breached, could result in immediate financial harm to consumers.

4. Limit processing which presents a “significant risk” to processing which occurs on a regular basis or a minimum number of times per year

In addition to limiting “significant risk” scenarios as described above, the Agency could also clarify that such processing must occur on a regular basis, or at least with some minimal frequency, to trigger the auditing and risk assessment requirements. It does not meaningfully further the spirit of the CPRA, and imposes particularly unnecessary burdens on small businesses, to require an audit and security assessment solely on the basis of one, two, or a handful of isolated instances of processing deemed to present a “significant risk” in a given year.

5. Limit processing which presents a “significant risk” to processing of at least 100,000 records

Alternatively, we suggest the Agency could incorporate some numerical trigger into what constitutes “significant risk” processing. For example, this number could track the figure in the

CPRA’s “business” definition of 100,000 records, or the Agency could select some lower number. In any case, the underlying statutory language of the CPRA counsels in favor of some such numerical limit. The statute contemplates “significant risk to consumers’ privacy or security,” language which connotes larger concerns of aggregate risk, not every isolated presentation of risk to any individual consumer or small group of consumers.

6. Limit the audit and risk assessment requirement to firms that meet one of the first two prongs of the CPRA’s “business” definition

We also request the Agency limit the audit and risk assessment requirements to larger firms, along the same lines as we requested for opt-out preference signals in point #2 above. These audits and risk assessments will be time consuming and expensive, and could in fact cripple small businesses who are just trying to do legitimate marketing research and data analytics work which benefits other businesses, nonprofit and educational organizations, government entities, and individual consumers.

7. Clarify that use in research results and reports of “sensitive personal information” is a “reasonably expected” use of information provided in connection with corresponding surveys and research studies

Under the CPRA, consumers have the right to request that a business “limit its use of the consumer’s sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services.” Insights is concerned that if research subjects who have provided sensitive personal information in connection with a survey or study (for example, in connection with a poll about an important political issue) submit such a request, this may compromise research results and leave market research firms in a legally unclear relationship with the research subject.

Accordingly, the regulations should stipulate that use of sensitive personal information in research results, and the continued use of those results to draw insights about consumers, is a “reasonably expected” use of sensitive personal information which was freely provided in connection with a survey or research study.

8. Exempt market research from notices of financial incentives

For our members’ research to be effective, they must ensure robust participation. This is frequently done through offering financial incentives. For example, a doctor may be offered an honorarium to answer a survey about various pharmaceuticals, or an individual may be offered a gift card to participate in a half-day focus group about the latest television shows.

Our industry has worked hard to comply with the financial incentive notice requirement under CCPA, but the notice of financial incentives requirements were not written with market research participation in mind; they inhibit research in an unintended way. Accordingly, we resubmit our request, made previously in connection with the CCPA regulations, that market research incentives and similar rewards to research subjects be exempt from notices of financial incentives requirements under the CPRA.

Most significant of all, appropriate notices of financial incentives are already provided in every legitimate market research execution. Adding parallel and/or potentially conflicting requirements will only confuse the issue for Insights members, their clients and the public at-large that participates in this research.

9. Limit the “authorized agent” concept to minors, and elderly or incapacitated individuals

Under the CPRA, a consumer may designate an authorized agent to submit opt-out requests, and requests to know and delete. There is currently no limitation on this procedure. Anyone can submit a request through an authorized agent. Increasingly, our members are receiving requests from purported authorized agents and are caught between, on one hand, wanting to honor legitimate requests and, on the other, the pervasive concern that the authorized agent mechanism invites fraud. Of course, our members take steps to verify such requests, as required by law, but those verification efforts are sometimes difficult to complete without requesting additional information, and tend to frustrate agents and/or consumers as much as they frustrate the business.

The registered agent option is unnecessary in the vast majority of cases, increases paperwork associated with the verification process, and opens the door for fraudulent requests designed to harm consumers. Except in cases where the consumer is a minor, or someone who genuinely needs an authorized agent to submit a request (such as an elderly or incapacitated individual), the purpose of the law is better served by requiring requests to be submitted by consumers themselves.

Conclusion

We hope the above comments will be useful to you and your team, and we are happy to entertain any questions or concerns you may have about the market research and data analytics industry.

Insights is also eager to discuss the concept of audience measurement, specifically, if that would be helpful.

Again, we appreciate the opportunity to comment.

Sincerely,

Howard Fienberg
Senior VP, Advocacy
Insights Association

Stuart Pardau
Counsel to Insights Association

Blake Edwards
Counsel to Insights Association

From: **Michael Geroe** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
Subject: CPPA Public Comment
Date: 11.08.2022 14:55:39 (+02:00)
Attachments: CPRA Comments (MRGLaw)(8.11.22).pdf (3 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Please see the attachment. Thank you,

Mike Geroe

--
LAW OFFICE OF MICHAEL R. GEROE, P.C.
[REDACTED]

[Calendar a Meeting](#)

NOTICE: Information contained in this transmission to the named addressee is proprietary information and is subject to attorney-client privilege and work product confidentiality. If the recipient of this transmission is not the named addressee, the recipient should immediately notify the sender and destroy the information transmitted without making any copy or distribution thereof. Thank you.

THE LAW OFFICE OF
MICHAEL R. GEROE, P.C.
8049 PASEO ARRAYAN
CARLSBAD, CA 92009

August 11, 2022

VIA ELECTRONIC MAIL
regulations@cpha.ca.gov

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

Re: CPPA Public Comment

Dear Mr. Soublet:

I am legal counsel to members of the community regulated by California privacy laws, including the California Consumer Privacy Act of 2018 (CCPA). My clients include privately held and publicly traded domestic and international businesses, generally located throughout North America and Europe. They range from businesses in banking and finance, media content and entertainment, health and beauty industries including prescription and over-the-counter drugs, nutraceuticals and cosmetics, to Internet-based service providers, including experts in marketing and advertising services. I have been advising clients on general compliance matters since 1993, and specifically on data compliance matters since 2004. Among other organizations, I am a member of the International Association of Privacy Professionals and have been certified by them since 2014 as an expert on U.S. privacy law (CIPP/US).

While the U.S. has not yet passed comprehensive federal consumer data privacy legislation, the CAN-SPAM Act of 2003 (CAN-SPAM) serves as long-standing precedent in setting standards for consumer data privacy protection in the field of general advertising. One of the standards set under CAN-SPAM was an avoidance of “magic words” required to be used by the regulated community. While the statute prohibits false or misleading email header information and requires a sender to identify commercial email as an advertisement, it does not mandate a particular method or manner to follow. It is inappropriate and counter-productive for a statute to provide for such detail, and arrogant for a legislature to presume its one method, or limited methods, will prove relevant or sufficient for all manner of use conceived of by the regulated community over time.

California should have followed an analogous approach in drafting the CCPA and subsequent legislation. The California Privacy Protection Agency (the “Agency”) should apply such standards in interpreting and enforcing the CCPA and subsequent legislation. The CCPA’s provision requiring a regulated business to have a webpage “titled ‘Do Not Sell My Personal


California Privacy Protection Agency
CPPA Public Comment
August 11, 2022
Page 3

community. Common sense and long-standing U.S. practice support the reservation of statutory magic words for specific and sensitive contexts, such as the use of controlled substances, not general consumer advertising.

For a reasonably drafted privacy policy meeting the substantive requirements of the CCPA or subsequent legislation, failure of a business to use a heading stating “Do Not Sell or Share My Personal Information” should not be grounds for enforcement action by the Agency. Where a link to the privacy policy of a business engaged in general, non-sensitive advertising is clear and conspicuous, the Agency should not take enforcement action where the link created by the business merely failed to use (the most recently amended) magic words.

The Agency’s mission and focus, as reflected in its statutory mandate, should be interpretation and enforcement of California’s privacy statutes for the protection of California residents and the California economy. Although one can understand why the legislature desires to enforce magic words in an effort to protect the public and the California economy, it is surprising to find such provisions survived the legislative process, in light of decades of relevant experience available on the public record. I hope these comments are helpful in the Agency’s consideration of how to calibrate burdens imposed on the regulated community and the intended benefits to all residents of this globally-connected and diverse State.

Sincerely,

A large black rectangular redaction box covering the signature area.

Michael R. Geroe

From: **Walsh, Kevin** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
Subject: CCPA Public Comments
Date: 15.08.2022 18:21:32 (+02:00)
Attachments: SPARK CCPA August 2022.pdf (2 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Please find attached comments from The Spark Institute, Inc. on the proposed CCPA regulations.

Regards,

Kevin Walsh

Notice: This message is intended only for use by the person or entity to which it is addressed. Because it may contain confidential information intended solely for the addressee, you are notified that any disclosing, copying, downloading, distributing, or retaining of this message, and any attached files, is prohibited and may be a violation of state or federal law. If you received this message in error, please notify the sender by reply mail, and delete the message and all attached files.



August 15, 2022

The California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd., Sacramento, CA 95834
(279) 895-6083

Re: Comments to Proposed Regulations Pursuant to California Consumer Privacy Act of 2018

Dear Acting General Counsel Soublet:

The SPARK Institute, Inc. writes to encourage you to take into account the continued needs of employers and employees when revising the proposed regulations issued on July 8, 2022, prior to their being finalized later this year (“Final Regulations”). We applaud the CCPA’s goal of providing consumers with strong protections, while still leaving employers and their service providers in a position to help employees receive health care and meet their retirement and other savings goals.

We recognize that the California Privacy Rights Act provided for an extension of certain safeguards for employers and for business to business relationships, and that the extension currently sunsets at the end of 2022. There are, however, three pending bills that would further extend – or make permanent – the current safeguards that protect the ability of employers and service providers to employers to provide employment-related benefits to California employees. These benefits are wide in scope – from retirement programs to health insurance, disability insurance, life insurance, and other similar benefits. In light of the potential for disruption, as well as the high likelihood of legislative changes prior to the end of the year, we ask that any expansion of the legal requirements related to employment-related benefits be phased in such that any revised requirements under §7012(j) take effect no earlier than July 1, 2023, with other changes taking effect sometime thereafter.

The SPARK Institute represents the interests of a broad-based cross section of retirement plan service providers and investment managers, including banks, mutual fund companies, insurance companies, third party administrators, trade clearing firms, and benefits consultants. Collectively, our members serve over 100 million employer-sponsored plan participants. Our comments reflect our unique perspective and our goal of advancing critical issues that affect plan sponsors, participants, service providers, and investment providers.

COMMENTS FROM THE SPARK INSTITUTE

A vital mission of the SPARK Institute is the promotion of employer-sponsored retirement plans, which play a critical role in helping every hardworking American retire with financial security. We worked closely with the California Attorney General's Office on the CCPA regulations to help protect privacy while ensuring that the unique employment context continues to provide employees with the benefits they expect.

We now ask that any new responsibilities imposed on employers and service providers be phased in. For example, we agree that many of the revisions to §7012(j) will likely apply to employers. We ask, though, that the regulations that would take effect by the sunset of §7012(k) be phased in so that employers have time to evaluate the changing regulatory landscape, and also have time to make employees aware of why any changes are being made. We further ask that the requirements imposed by the other regulatory sections (which requirements currently do not apply in the employment context) be delayed until January 1, 2024, again to provide employers sufficient time to better educate employees on why changes are being made to the benefit programs that they have come to expect.

It is important that the regulatory framework surrounding employer-provided benefits evolves predictably so that the legislature is able to continue to determine whether they are analogous to exempted data, such as that covered by the Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act. Rapid implementation of new privacy regulations in the employment context could prove irreversibly disruptive.

* * * * *

The SPARK Institute appreciates the opportunity to provide these comments to the California Privacy Protection Agency. If you have any questions or if you would like more information regarding this letter, please contact me or the SPARK Institute's outside counsel, David Levine and Kevin Walsh with Groom Law Group, Chartered

[REDACTED]

Sincerely,

[REDACTED]

Tim Rouse
Executive Director

From: [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 16.08.2022 01:09:02 (+02:00)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Disclaimer: I would like to remain anonymous from all public records and publications. However, I sign with my full name and please feel free to write me back.

To whom it may concern,

As a victim of two kidnapping situations I am utterly agreed on a privacy act. I am not comfortable with my private information including date of birth and private residence address being public anywhere on the internet and even "people finder" websites. I don't feel safe. I suffered a lot and everytime I see anything private getting public I feel unsafe and triggers my PTSD. That's my personal experience as a consumer and as a person.

As for the rest of people I think we all have the same right to privacy and I don't think that any personal information should be public. If we continue to allow this, we only feed the ID theft, kidnappings, robberies and more crimes.

We really need to stop this 'privacy exposure'.

Thank you for reading me.

My best regards,
[REDACTED]

P.S. I think that the US Gov is always achieving a good job regardless of the parties or external circumstances. I really thank you for everything.

Get [Outlook for iOS](#)

From: [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
CC: [REDACTED]
Subject: CPPA Public Comment | Washington Legal Foundation Comment to Proposed CPRA Regulations
Date: 17.08.2022 22:18:10 (+02:00)
Attachments: WLF Comment to CPPA Regarding Proposed Regulations 17 Aug. 2022.pdf (65 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Mr. Soublet,

The law firm of Greenberg Traurig LLP is pleased to submit the attached comment on behalf of the Washington Legal Foundation concerning the California Privacy Protection Agency's proposed regulations implementing the CPRA.

Kind Regards,

-David

David Zetoony

Shareholder

Co-Chair U.S. Data Privacy and Cybersecurity Practice

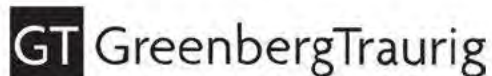
Greenberg Traurig, LLP

1144 15th Street, Suite 3300 | Denver, Colorado 80202

[REDACTED] | www.gtlaw.com | [View GT Biography](#)

GT GreenbergTraurig

If you are not an intended recipient of confidential and privileged information in this email, please delete it, notify us immediately at postmaster@gtlaw.com, and do not use or disseminate the information.



David A. Zetoony
[REDACTED]

August 17, 2022

VIA EMAIL (regulations@coppa.ca.gov)

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

Re: Washington Legal Foundation's comment on CPPA Rulemaking /
CPPA Public Comment

The law firm of Greenberg Traurig LLP is pleased to submit this comment on behalf of the Washington Legal Foundation ("WLF") concerning the economic analysis submitted by the California Privacy Protection Agency ("CPPA") along with its proposals for regulations (the "Proposed Regulations") implementing the California Privacy Rights Act ("CPRA").

Founded in 1977, WLF is a nonprofit, public-interest law firm and policy center with supporters nationwide, including many in California. WLF promotes free enterprise, individual rights, limited government, and the rule of law. To that end, WLF often appears as amicus curiae in important administrative law cases. Additionally, WLF's Legal Studies division regularly publishes papers by outside experts on state and federal regulatory overreach.

As detailed below, the CPPA did not complete a full or accurate economic analysis of the Proposed Regulations as is required by the California Administrative Procedure Act ("APA"). Instead, it submitted a shorthand Economic Impact Statement ("EIS") that grossly underestimates the full economic impact of the Proposed Regulations on California businesses.¹ Not only did this underestimation result in an incorrect public disclosure that is being relied on by consumers and businesses in their consideration of the Proposed Regulations, it also led to the CPPA incorrectly treating the Proposed Regulations as a non-major regulation – effectively denying a proper review by the Department of Finance ("DOF") and the Office of Administrative Law ("OAL").

Although the EIS is vulnerable to several criticisms,² this comment focuses on the CPPA's insufficient analysis of new requirements imposed on businesses by the Proposed Regulations. The

¹ The APA uses the term "Economic Impact Assessment" whereas the CPPA uses the term "Economic Impact Statement." We use the term Economic Impact Statement and the acronym EIS throughout this comment for consistency.

² For example, the EIS states that the CPPA does not expect a significant direct negative impact on investment in California. Studies conducted on jurisdictions that passed similarly comprehensive privacy laws and regulations (like the European GDPR) found significant negative impacts on investment. *See e.g.,* Mical S. Gal & Oshrit Aviv, *The Competitive Effects of the GDPR*, 2020 J. COMPET. L. & ECON. 1, 6, <https://ssrn.com/abstract=3548444> (finding that the GDPR negatively impacted the number of venture deals in the

Attn: Brian Soublet

August 17, 2022

Page 2

CPPA concluded that the **66 pages** of revisions and amendments to the current privacy regulations would only lead to three new compliance obligations, which businesses could purportedly satisfy with de minimis time and resources: 1.5 hours of compliance effort — less than \$200 per business. Indeed, the 1.5 hours of time contemplated by the CPPA would be insufficient for companies to even read the 66 pages of privacy regulations, let alone implement them. In actuality, the Proposed Regulations **include over 45 new compliance requirements that were not evaluated by the CPPA**. When those 45 compliance obligations are included, it becomes clear that what the CPPA is proposing will have a much larger economic impact on businesses, and that the Proposed Regulations are a “major regulation” under the APA requiring enhanced review by the OAL and the DOF.

For the reasons stated above, the Proposed Regulations should be returned to the CPPA for the preparation of a Standard Regulatory Impact Analysis (“SRIA”) as is required for major regulations, and should be resubmitted to the DOF and the OAL as part of a new notice-and-comment period. The resubmission of a full economic analysis using the SRIA process is needed to ensure that the public has a chance to review and comment on the Proposed Regulations *within the context* of the actual economic impact that the Proposed Regulations are likely to have.

1. The Rulemaking Process

The APA governs how state agencies, such as the CPPA, may issue regulations. The rulemaking procedures and standards of the APA “are designed to provide the public with a meaningful opportunity to participate in the adoption of regulations or rules that have the force of law by California state agencies and to ensure the creation of an adequate record for the OAL and judicial review.”³ In other words, proper rulemaking procedures allow the public to understand and engage with regulations that would affect them directly, and ensure that future judicial and administrative reviews are accessible and fair.

The APA divides regulations into two categories: major regulations and non-major regulations. A major regulation is defined as a proposed regulation that may have an “economic impact on California business enterprises and individuals in an amount exceeding fifty million dollars (\$50,000,000), as estimated by the agency.”⁴ Proposals that will have an impact of less than \$50 million are considered non-major regulations.

Proposals that are considered non-major regulations are subject to reduced analysis obligations and oversight. Specifically, if an agency intends to propose a non-major regulation, it only needs to file an EIS, which will be reviewed by the OAL for facial consistency (for example, whether

EU, the size of the deals, and the overall amount of dollars invested). The CPPA does not discuss or address these studies, let alone conduct an analysis as to whether California may experience similar negative impacts. This gap is particularly ironic given that the CPPA’s consultant expressly compares the Proposed Regulations to the requirements of the GDPR. *See* BERKELEY ECON. ADVISING & RSCH., CALIFORNIA CONSUMER PRIVACY AGENCY NOTES ON ECONOMIC IMPACT ESTIMATES FOR FORM 399, at 8-9 (2022) https://cppa.ca.gov/regulations/pdf/std_399_attachment.pdf [hereinafter BEAR Report].

³ *Rulemaking Process*, OFF. OF ADMIN. L., https://oal.ca.gov/rulemaking_process/ (last visited July 29, 2022).

⁴ CAL. GOV’T. CODE § 11342.548 (West 2022).

Attn: Brian Soublet

August 17, 2022

Page 3

the EIS was completed and was included within the rulemaking file) and published for notice and comment.⁵

In contrast, an agency that intends to propose a major regulation must submit a SRIA, which is far more comprehensive than a regular EIS and subject to heightened scrutiny by the DOF and OAL. The following summarizes the practical impact of a proposed regulation that is classified as a major regulation:

1. Advance notice to the DOF by February 1st. Any agency that intends to propose a major regulation must notify the DOF of its intention by February 1st through the submission of a form DF-130.⁶
2. The DOF Publishes Notice of the Major Regulation. The DOF must independently publish a notice of the proposed major regulation.⁷
3. Creation of SRIA. The agency must prepare a SRIA⁸ which must address, among other things, the “competitive advantages or disadvantages for businesses currently doing business within the state”⁹ and “each regulatory alternative for addressing the stated need for the proposed major regulation, including each alternative that was provided by the public or another governmental agency and each alternative that the agency considered; all costs and all benefits of each regulatory alternative considered; and the reasons for rejecting each alternative;”¹⁰
4. SRIA Submitted 60 - 90 days prior to Notice of Proposed Rulemaking. The agency must submit a SRIA to the DOF “[n]ot less than 60 days prior to filing a notice of proposed action with OAL” or “[n]ot less than 90 days prior to filing a notice of proposed action with OAL if the agency has not notified the department of the proposed major regulation” by February 1.¹¹
5. Public Notice of the SRIA before the Notice of Proposed Rulemaking. Within 10 days of receiving the SRIA, the DOF must post a copy of the SRIA online and send a copy directly to all relevant government agencies.¹²

⁵ CAL. GOV’T. CODE § 11346.3(b) (West 2022). *See also* CAL. GOV’T. CODE § 11349.1(d)(2) (West 2022) (stating that OAL should return any regulation that has not complied with the obligation under Cal. Gov’t. Code § 11346.3 (West 2022) to complete an EIS and to include the EIS within the rulemaking file).

⁶ CAL. CODE. REGS. tit. 1, § 2001(a)(1) (2022). If notification is not possible by February 1st, the Propounding Agency must submit its notice “as soon as possible but in no event later than 60 days prior to filing a notice of proposed action with the OAL [Office of Administrative Law].” CAL. CODE. REGS. tit. 1, § 2001(a)(2) (2022).

⁷ CAL. CODE. REGS. tit. 1, § 2001(a)(c) (2022).

⁸ CAL. GOV’T. CODE § 11346.3(c)(1) (West 2022).

⁹ CAL. GOV’T. CODE § 11346.3(c)(1)(C) (West 2022).

¹⁰ CAL. CODE. REGS. tit. 1, § 2002(c)(8) (2022).

¹¹ CAL. CODE. REGS. tit. 1, § 2002(a)(1), (2) (2022).

¹² CAL. CODE. REGS. tit. 1, § 2002(d), (e) (2022).

Attn: Brian Soublet
 August 17, 2022
 Page 4

6. Independent Review and Evaluation. The DOF must then independently evaluate whether the SRIA adheres to the requirements of the APA.¹³
7. Comments from DOF. After conducting its analysis, the DOF must transmit its independent and objective comments to the agency within 30 days.¹⁴
8. Consideration by Propounding Agency. The propounding agency must respond to the DOF comments and issue a “statement of the results of the updated analysis.”¹⁵
9. Submission to the Public. Only after all of the above occurs may the agency publish the regulation for notice and comment.¹⁶

The requirement for agencies to exhaustively document the full economic impact of a major regulation through a SRIA is a core feature of the regulatory process. A complete, thorough, and accurate impact of a proposed regulation is necessary for the propounding agency to “provide [other] agencies and the public with tools to determine whether the regulatory proposal is an efficient and effective means of implementing the policy decisions enacted in statute.”¹⁷ Only by “inform[ing] the agencies and the public of the economic consequences of regulatory choices” can the public fully participate in the rulemaking process. Without such information, the public and impacted businesses are not fairly put on notice of the impact a proposed regulation may have on them and thus cannot meaningfully decide whether to invest the time and resources needed to participate in the comment process.¹⁸

Additionally, the major regulation process is crucial to the propounding agency’s ability to solicit and consider regulatory alternatives and ensure that the “proposed action is the most effective, or equally effective and less burdensome, alternative in carrying out the purpose for which the action is proposed, or the most cost-effective alternative to the economy and to affected private persons that would be equally effective in implementing the statutory policy or other provision of law.”¹⁹ Without taking the necessary steps to identify all alternatives that are just as effective but potentially less costly, the potential for overly burdensome and unnecessary regulations grows.

In any event, California courts have held that a failure to follow the process for submitting major regulations can invalidate final regulations in their entirety, rendering them unenforceable.²⁰

¹³ CAL. GOV’T. CODE § 11346.3(f) (West 2022).

¹⁴ CAL. GOV’T. CODE § 11346.3(f) (West 2022).

¹⁵ CAL. GOV’T. CODE § 11346.3(f) (West 2022).

¹⁶ CAL. GOV’T. CODE § 11346.5(a)(10) (West 2022) (stating that an agency’s notice of proposed rulemaking must include a summary of the comments provided to the agency by the DOF pursuant to Cal. Civ. Code § 11346.3(f) (West 2022)).

¹⁷ CAL. GOV’T. CODE § 11346.3(e) (West 2022).

¹⁸ CAL. GOV’T. CODE § 11346.3(e) (West 2022).

¹⁹ CAL. GOV’T. CODE § 11346.36(b)(2) (West 2022).

²⁰ CAL. GOV’T. CODE § 11350(a), (b)(1) (West 2022) (stating that a regulation “may be declared to be invalid

Attn: Brian Soublet
 August 17, 2022
 Page 5

2. The CPPA Did Not Comply with the Process for Submitting a Major Regulation.

On January 28, 2022, the CPPA transmitted form DF-130 to the DOF indicating that the CPPA anticipated creating a major regulation.²¹ The DOF subsequently published a notice that the CPPA intended to issue a major regulation.²² These actions appear to have satisfied requirements (1) and (2) of the major regulation process described above. The CPPA did not complete steps (3) through (8) of the major rulemaking process. Instead, and without providing notice to the public, on June 28, 2022, the CPPA submitted the Proposed Regulations to the OAL for publication in the California Register. As part of its submission, the CPPA provided the OAL with an EIS which concluded that the Proposed Regulation would have a “small cost per business (\$127.60).”²³ The EIS included a report prepared by Berkeley Economic Advising and Research (the “BEAR Report”) titled “California Consumer Privacy Agency Notes on Economic Impact Estimates for Form 399.” Notably, because the CPPA incorrectly determined that the Proposed Regulations would have a small cost per business, the Proposed Regulations were treated like a non-major regulation. The CPPA did not provide an SRIA to the DOF 60 – 90 days before submitting the Proposed Regulations (or, indeed, at any time).

The estimate that the Proposed Regulations would have a de minimis impact on business, and the ultimate conclusion that the Proposed Regulations should be treated as a non-major regulation, was surprising. For context, when the Office of the California Attorney General had proposed the 28 pages of CCPA Regulations three years prior it identified those regulations as imposing an initial cost of \$75,000 per business, with an annual ongoing cost of \$2,500 per business every year for 10 years – in other words a total cost of \$100,000 per business. The overall statewide impact was estimated at \$467 million to \$16 billion.²⁴

As detailed below, the actual impact on businesses is far greater than disclosed by the CPPA. The EIS failed to identify all of the obligations imposed on businesses by the Proposed Regulations and thus did not calculate the economic impact associated with such obligations. The costs arising from the unanalyzed obligations alone (not to mention those costs that were not accounted for due to other methodological errors)²⁵ easily exceed \$50 million. For this reason, the CPPA was required to follow the APA’s major-regulation procedures.

for a substantial failure to comply with [the APA.]”); *Sims v. Dep’t of Corrs. & Rehab.*, 216 Cal. App. 4th 1059, 1067, 1081 – 82 (2013) (finding that regulations promulgated by an agency that failed to complete a fiscal impact assessment were invalid and unenforceable).

²¹ Response to Public Records Act Request from CPPA (Aug. 10, 2022) (Attached as Exhibit B).

²² See *2022 Major Regulations Rulemaking Calendar*, DEP’T OF FIN., <https://dof.ca.gov/wcontent/uploads/Forecasting/Economics/Documents/2022-MajorRegsCalendar.pdf> (last visited Aug. 15, 2022).

²³ CAL. PRIV. PROT. AGENCY, STD. 399 ECONOMIC AND FISCAL IMPACT STATEMENT 1 (in conjunction with the California Consumer Privacy Act (CCPA) Regulations, signed June 28, 2022), https://cppa.ca.gov/regulations/pdf/std_399.pdf. The EIS extrapolated that the \$127.60 per business cost might have an aggregate impact of \$8,424,690.

²⁴ *Id.* at 2.

²⁵ See *supra* note 2.

Attn: Brian Soublet
 August 17, 2022
 Page 6

3. The Economic Analysis Submitted by the CPPA with the Proposed Regulations Is Foundationally Deficient

The BEAR Report, intended to clarify and support the economic impact asserted in the EIS, begins by stating the assumptions and criteria BEAR used in its analysis. BEAR explains that it “assessed whether each section [of the Proposed Regulations] created obligations that were not found in existing law,” existing law being loosely defined as the existing CCPA regulations and the CPRA amendments. Upon reading the existing CCPA regulations, CPRA amendments, and the Proposed Regulations, BEAR concluded in its initial analysis that the “new proposed draft regulations initially appear **significant** in scope” and that, “[**in many sections**, [BEAR] initially believed that there could be a **regulatory impact**.”²⁶ Attached as an Appendix 2 to the BEAR Report is a list of “selected sections” of the Proposed Regulations where BEAR “initially assessed there may be regulatory deltas.”²⁷ Presumably these initial conclusions were based on an independent and unbiased reading of the existing law and Proposed Regulation, and would have supported the classifying the Proposed Regulations as a “major regulation” necessitating a full SRIA.

The BEAR Report then alludes to a “discussion” between BEAR and unidentified CPPA “supporting staff.” During this discussion, the unidentified staff apparently argued that “most of the potential regulatory ‘deltas’” that BEAR had identified “were reiterated [in] the existing CPRA amendments or existing regulations from the CCPA.” They urged BEAR not to identify these sections as imposing new obligations upon businesses and instructed BEAR not to analyze these sections for their economic impact.²⁸ Tellingly, Appendix 2 of the Report fails to fully discuss where in the existing law each identified delta is, in fact, addressed. Instead, Appendix 2 provides a generalized statement that is not only inadequate, but in many cases false.²⁹

Ultimately, based on the assertions of unidentified staff, BEAR assumed that the Proposed Regulations would impose only “three” new requirements on businesses, rather than the 10 requirements first listed by BEAR, or the 45 requirements identified by WLF in the chart below.

To better understand the directions and assumptions provided to BEAR, and to view a copy of BEAR’s initial assessment, WLF submitted separate Public Records Act requests to the California AG and the CPPA requesting a copy of any transcripts or notes from the discussions between the unidentified CPPA staff and BEAR. The Office of the California Attorney General responded that it is unaware of any notes or transcripts from the meeting, but that if any records exist they “may be subject to exemptions from disclosure” (no explanation was provided as to what exemptions might apply).³⁰ The CPPA refused to say whether any notes and transcripts existed, but asserted that if such documents exist they are shielded from public disclosure under “the confidentiality

²⁶ BEAR Report at 1.

²⁷ As BEAR refers to these as “selected sections” presumably they were not intended to be an exhaustive list of all the areas in which BEAR believed there to be a regulatory delta. BEAR Report at 19.

²⁸ BEAR Report at 1-2.

²⁹ See e.g., Row 31 in the table below (discussing how §7051(a)(2) has in fact not been addressed by the CPRA despite the statement provided for in the BEAR Report at 20).

³⁰ Response to Public Records Act Request from Amos E. Hartston, Deputy Att’y Gen. (July 26, 2022) (Attached as Exhibit A).

Attn: Brian Soublet
 August 17, 2022
 Page 7

privileges set forth in California law, including the attorney-client privilege contained in Evidence Code section 954, which are expressly incorporated into the Public Records Act and the public interest is served in supporting Agency counsel's ability to provide confidential advice and counsel to the Agency."³¹ While beyond the scope of this comment, it is significant to note that the CPPA offered no support for its assertion that Cal. Evid. Code §954 is appropriate to shield the BEAR notes and transcripts from disclosure.³²

The CPPA did, however, provide a copy of the contract between BEAR and the CPPA, which states that if BEAR's "initial analysis concludes that the regulatory assumption provided by the Agency will have an impact of more than \$50 million, contractor shall prepare the necessary Standardized Regulatory Impact Assessments (SRIA) required by Government Code Sections 11346.2(b)(2)(B) and 11346.3(c)."³³ Unfortunately, the CPPA did not provide a copy of the "initial assessment" that was update per the "discussion" between BEAR and unidentified CPPA "supporting staff," so it is unclear whether this contractual provision was triggered by BEAR's initial findings.

Contrary to the assertion of the unidentified staff, the Proposed Regulations impose far greater than three new obligations on businesses. The following table identifies **more than 45** significant new obligations that the Proposed Regulations would impose on businesses. None of these new obligations were accounted for within the BEAR Report's analysis or the EIS's calculations. WLF believes that an objective analysis of the new obligations would undoubtedly classify the Proposed Regulations as a "major regulation" for which a SRIA was required.

(See following page)

³¹ Response to Public Records Act Request from CPPA (no sender identified) (Aug. 10, 2022) (Attached as Exhibit B).

³² Cal. Evid. Code §954 covers "confidential communications" between a "client" and that client's "lawyer" (all terms further defined in Chapter 3 of the Evidence Code). The assertion of attorney-client privilege requires a party to identify an attorney, a communication where a "legal opinion [is] formed" by a lawyer, and ensure that the communication remains confidential and is not waived. Cal. Evid. Code 952. In this case, the CPPA did not identify a lawyer, did not identify specific communications, and provided no basis for believing that any communication that might have occurred between an attorney for the CPPA and BEAR (an independent third party) had any expectation of confidentiality. Indeed, even if an attorney-client privilege could have existed it would have been waived when BEAR (and the CPPA) expressly relied upon the purported statements of the attorney as the foundation of the BEAR report. Attempting to shield an agency's analysis of the impact of a proposed regulation from the public by the assertion of attorney-client privilege when the agency is statutorily mandated to disclose the regulatory impact is extremely unusual (and indeed may be unprecedented) and raises severe concerns regarding the transparency of the CPPA and their commitment to the regulatory process.

³³ California Privacy Protection Agency Economic Analysis Consulting Services Contract at 2 (received Aug. 10, 2022) (Attached as Exhibit B).

Attn: Brian Soublet
 August 17, 2022
 Page 8

New Compliance Obligations Imposed by the Proposed Regulations and Not Accounted for within the EIS or BEAR Report

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CPPA / BEAR within the EIS
1.	§ 7001(c)	<u>Expansion of authorized agents.</u> The Proposed Regulation would change the definition of "Authorized Agent" to remove the requirement that such entities be registered with the California Secretary of State.	The current CCPA Regulations require that all authorized agents be "registered with the Secretary of State to conduct business in California." ³⁴	<ul style="list-style-type: none"> Businesses would need to begin responding to "authorized agent" requests submitted by companies that are not registered with the Secretary of State. The increased volume of authorized agent requests may require additional resources to track, process, and respond to data subject requests. 	Not accounted for by BEAR / 0 hours and \$0 assigned
2.	§ 7003(c)	<u>Size and color of links.</u> The Proposed Regulation would mandate that all links required under the CCPA be in the same "font size and color" as "other links used by the business on its homepage."	The CCPA, CPRA, and current CCPA Regulations do <u>not</u> mandate that businesses verify that the size and color of all links mandated by the CCPA are of the same approximate size or color as other links on the homepage. The CPRA only requires that "a link to a web page that enables the consumer to consent to the business ignoring the opt-out preference signal" have "a similar look, feel, and size relative to other links on the same web page." ³⁵	<ul style="list-style-type: none"> Businesses would need to visually inspect each website under their control to verify the size and color of CCPA/CPRA mandated links. For businesses that maintain multiple websites, each website would need to be inspected. Any website that is identified as utilizing a different font size and/or color would need to be modified. 	Not accounted for by BEAR / 0 hours and \$0 assigned
3.	§ 7003(d)	<u>Links within mobile applications.</u> The Proposed Regulation would mandate that in mobile applications a "conspicuous link <u>shall be</u> accessible within the application, such as through the application's settings menu." This would be in addition to the inclusion of conspicuous links within privacy notices.	The current CCPA Regulations do <u>not</u> mandate that a mobile application make links accessible within the application, but rather allows companies to decide whether to include links in such location. Specifically <ul style="list-style-type: none"> the current CCPA Regulations state that a Notice at Collection "<u>may</u>" be provided "within the application, such as through the application's settings menu,"³⁶ and the current CCPA Regulations state that a business "<u>may</u>" choose to provide a DNSMPI link "within the application, 	<ul style="list-style-type: none"> Businesses would need to visually review each mobile application under their control to verify that all "conspicuous links" required by the CPRA (including privacy notice, DNSOSMPI, Limit Use, etc.) are accessible within an Application's settings menu. Businesses would need to ensure the display of multiple links does not interfere with user experience or violate third party UX requirements (such as Apple's Human Interface Guidelines³⁹). For businesses that maintain multiple mobile applications (dozens or hundreds) each mobile application would need to be inspected. 	Not accounted for by BEAR / 0 hours and \$0 assigned

³⁴ CAL. CODE REGS. tit. 11, § 7001(c) (2022).

³⁶ CAL. CODE REGS. tit. 11, § 7012(a)(3)(B) (2022) (emphasis added).

³⁹ *Human Interface Guidelines*, APPLE INC., <https://developer.apple.com/design/human-interface-guidelines/guidelines/overview/> (last visited Aug. 4, 2022).

Attn: Brian Soublet
 August 17, 2022
 Page 9

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CCPA / BEAR within the EIS
			<p>such as through the application's settings menu" in addition to the mandatory placement of the link on the Business's homepage.³⁷</p> <ul style="list-style-type: none"> The current CCPA Regulations state that a business "may include a link to the privacy policy in the application's settings menu" in addition to the mandatory placement of the link on the download or landing page of the mobile application.³⁸ 	<ul style="list-style-type: none"> Any mobile application that does not contain such links would need to be modified. Note that for businesses that did not develop or do not maintain their own mobile applications, this may necessitate engaging third party mobile application development companies. 	
4.	§ 7004(a)(2)	<p>Review cookie banner verbiage. The Proposed Regulation is ambiguous as to its scope. It is unclear whether the example refers to a website banner that a consumer might see <i>after</i> opting-out of a sale or sharing (a banner resoliciting consent) or website banners that a consumer might see asking for the consumer to provide a use or direction for the business to disclose personal information in the first instance (an action that would remove the data transfer from the sale of personal information per 1798.140(ad)(2)(A)). For whatever banner the example was intended to impact it would mandate that businesses review and/or update the verbiage to include both an "accept all" and "decline all" option, instead of "accept all" and "preferences."</p>	<p>The current CCPA Regulations discuss parity of methods for submitting requests to (a) "opt-out," or (b) opt-in "<i>after</i> having previously opted out" (resolicitation). Only in the context of the latter situation do the current CCPA Regulations require a parity of "steps" between an opt-out mechanism <i>as compared to</i> the mechanism for requesting to "opt-in to the sale of personal information <i>after</i> having previously opted out."⁴⁰</p> <p>The CPRA and the current CCPA Regulations do <u>not</u> regulate <i>opt-in</i> banners that do not involve resolicitation (that is, requests for a consumer to consent in the first instance to the use of AdTech cookies before such cookies are deployed).</p> <p>If the Proposed Regulation is intended to govern opt-in banners (as opposed to resolicitation banners) by interpreting certain opt-in banners as constituting "dark patterns" the regulation would be</p>	<p>If the Proposed Regulation is intended to govern opt-in banners (as opposed to resolicitation banners):</p> <ul style="list-style-type: none"> Businesses would need to review their websites for any opt-in cookie consent banners. For businesses that identify opt-in consent banners, the business would have to review the terminology and consent structure to identify whether an "accept all" and "decline all" button exists. If a "decline all" button does not exist, the business would need to modify the cookie banner. Note that for businesses that did not develop and/or do not maintain their own cookie banners, the new requirement may necessitate resources of third party support companies (e.g., cookie banner providers). 	<p>Not accounted for by BEAR / 0 hours and \$0 assigned.</p>

³⁷ CAL. CODE REGS. tit. 11, § 7013(b)(1) (2022) (emphasis added).

³⁸ CAL. CODE REGS. tit. 11, § 7011(b) (2022).

⁴⁰ CAL. CODE REGS. tit. 11, § 7026(h)(1) (2022) (emphasis added).

Attn: Brian Soublet
 August 17, 2022
 Page 10

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CPPA / BEAR within the EIS
			substantively new and should be analyzed for its economic impact.		
5.	§ 7004(a)(2)(D)	<u>Review opt-in cookie banner font size and color.</u> The Proposed Regulation would mandate that all businesses that use opt-in cookie banners review the font size and color of the "yes" button to ensure that it is no larger or "more eye-catching" than the "no button."	The CPRA and the current CCPA Regulations do <u>not</u> regulate <i>opt-in</i> consent banners (requests for a consumer to consent to the use of AdTech cookies before such cookies are deployed). The CPRA and the CCPA only discuss (1) opt-out mechanisms (giving consumers the right to stop the selling or sharing of personal data that would otherwise occur if the consumer takes no action), and (2) opt-in mechanisms <i>after</i> the consumer has previously opted out. ⁴¹	If the Proposed Regulation is intended to govern opt-in banners (as opposed to resolicitation banners): <ul style="list-style-type: none"> • Businesses would need to review their websites for any opt-in cookie consent banners. • For businesses that identify opt-in consent banners, the business would have to review the font size, color, and prominence of the options displayed. • If a "yes" button is larger or of a more "eye-catching color" the business would need to modify the cookie banner. Note that for businesses that did not develop or do not maintain their own cookie banners, the new requirement may necessitate resources of third party support companies (e.g., cookie banner providers). 	Not accounted for by BEAR / 0 hours and \$0 assigned
6.	§ 7004(a)(4)(A)	<u>Review verbiage of financial incentive choices.</u> The Proposed Regulation would mandate that businesses that offer financial incentive programs review the terminology of their consent mechanism to avoid statements such as "No, I don't want to save money."	The CPRA and the current CCPA Regulations do <u>not</u> contain any requirements regarding the terminology that should be used when soliciting consent for a financial incentive program.	<ul style="list-style-type: none"> • Businesses would need to review their practices to identify all instances in which consumers are asked to join a financial incentive program. • In each instance in which a business solicits participation in a financial incentive program, the business would need to review the consent structure and the verbiage surrounding options open to the consumer for conformance to the Proposed Regulation. • If the current terminology does not conform to the Proposed Regulation, the business would need to modify the terminology. For website-based financial incentive program requests, such a change would necessitate website development time. For paper-based financial incentive program requests, such a change would necessitate creating and printing new forms and/or signage. 	Not accounted for by BEAR / 0 hours and \$0 assigned

⁴¹ CAL. CODE REGS. tit. 11, § 7026(h)(1) (2022).

Attn: Brian Soublet
 August 17, 2022
 Page 11

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CPPA / BEAR within the EIS
7.	§ 7004(a)(4)(C)	<u>Create separate consent pathways.</u> The Proposed Regulation would prohibit businesses from "bundling" a request for consent to use personal information for one purpose with a request for consent to use personal information for an unrelated purpose.	The CPRA prohibits a business from collecting information for one purpose, and then using the information for an "incompatible purpose" that was not disclosed to the consumer. ⁴² The CPRA and the current CCPA Regulations do <u>not</u> prohibit a business from using personal information for an incompatible purpose so long as the consumer is provided "with notice" of the additional purpose, nor does the CPRA (or the current CCPA Regulations) prohibit a business from asking a consumer to consent to two different purposes simultaneously.	<ul style="list-style-type: none"> Businesses would need to review their practices to identify all instances in which consumers are asked to consent to the use of their personal information. In each instance in which a business solicits consent, the business would need to review the consent structure to identify whether the business is requesting consent for multiple uses of the personal information that might be considered by the CPPA to be "unexpected or incompatible." In each instance where a bundled consent is identified, the business would need to modify its consent structure to present the consumer with separate consent options for each of the business's use of personal information. Where bundled consent has already been obtained by the consumer, the business may need to consider the feasibility of resoliciting consent using an unbundled consent structure (i.e., contacting the consumer and asking them to verify their previous choices). 	Not accounted for by BEAR / 0 hours and \$0 assigned
8.	§ 7012(g)(1), (2), (4)(A).	<u>AdTech and/or analytics providers must provide notices at collection.</u> The Proposed Regulations would require that a notice of collection be provided by "both" a business that provides a website as well as a "third party controlling the collection of personal information."	The current CCPA Regulations only require that a business provide a notice at collection if the business collects personal information "from the consumer." ⁴³ In situations in which a business collects personal information <i>about</i> a consumer, but collects such personal information from or through a third party (i.e., from a third party that initially collected the personal information), the regulations implementing the CCPA make clear that the business "does not need to provide a notice at collection" so long as the business does not intend to sell the personal information. ⁴⁴ If the business intends to sell the personal information, a notice at collection is still	<ul style="list-style-type: none"> Publishers may need to audit each website that they maintain to determine which third parties are collecting personal information from those websites. Publishers may need to review their contracts with each identified third party to identify each contractual requirement to display the third party partner's notice at collection within the first party's notice at collection. Publishers may need to modify their notice at collection to include the notice at collection of any third party partner that has contractually obligated the publisher to display the third party's notice at collection. Publishers may need to design an internal process by which the addition, or subtraction, of third parties that are allowed to collect 	Not accounted for by BEAR / 0 hours and \$0 assigned

⁴² CAL. CIV. CODE §1798.100(a)(1) (West 2022).

⁴³ CAL. CODE REGS. tit. 11, § 7001(l) (2022); CAL. CODE REGS. tit. 11, § 7010(b) (2022) (emphasis added).

⁴⁴ CAL. CODE REGS. tit. 11, § 7012(d) (2022).

Attn: Brian Soublet
 August 17, 2022
 Page 12

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CPPA / BEAR within the EIS
			not required if the business complies with California's rules regulating data brokers. ⁴⁵	<p>personal information from websites triggers a process by which the third party's notice at collection is removed from or added to the first party's notice at collection as needed.</p> <ul style="list-style-type: none"> • Publishers may need to design an external process through which third party partners could notify the first party if the third party's notice at collection has changed (thus requiring the first party to modify the sections in its own privacy notice/notice at collection that refer to the third party's practices). 	
9.	§ 7013(c)	<u>DNSOSMPI link must be in header or footer.</u> The Proposed Regulation would require that businesses that are required to publish a "Do Not Sell or Share My Personal Information" link locate that link in either the header or the footer of the homepage.	<p>The CPRA only requires that businesses that are required to include the DNSOSMPI link make the link "clear and conspicuous."</p> <p>The current CCPA regulations only require that businesses that are required to include the DNSOSMPI link make the link available on the website homepage.</p> <p>Neither the CPRA nor the current CCPA Regulations mandate that the link be located within the header or the footer of the website.</p>	<ul style="list-style-type: none"> • Businesses would need to review each website under their control that includes a DNSOSMPI link and verify that the link is located within the website's header or within the website's footer. • Any website that is identified where the DNSOSMPI link is located in a different location (e.g., the body of the homepage, a sidebar, a pop-up window, or a pop-up notice) would need to be modified. 	Not accounted for by BEAR / 0 hours and \$0 assigned
10.	§ 7013(e)(3)(C)	<u>DNSOSMPI info must be included in telephone scripts.</u> The Proposed Regulation would require that businesses that sell or share personal information collected over the telephone "shall" provide notice orally of how the consumer can opt-out of the sale.	The current CCPA Regulations state only that a business that collects personal information over the phone "may" provide notice orally of how the consumer can opt-out of the sale. ⁴⁶	<ul style="list-style-type: none"> • Businesses would need to determine whether any information that is collected over the telephone is sold or shared. • Businesses that engage in outbound direct marketing would need to review outbound call scripts and/or interactive voice response ("IVR") scripts. • To the extent that the current outbound call script and/or IVR script does not include information on how a consumer can opt-out of the sale of personal information, the outbound call script would need to be modified and/or the IVR script would need to be reprogrammed. 	Not accounted for by BEAR / 0 hours and \$0 assigned

⁴⁵ CAL. CODE REGS. tit. 11, § 7012(e) (2022). *See also* CAL. CIV. CODE § 1798.99.80 et seq. (West 2022) (regulating data brokers).

⁴⁶ CAL. CODE REGS. tit. 11, § 7013(b)(3)(B) (2022).

Attn: Brian Soublet
 August 17, 2022
 Page 13

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CPPA / BEAR within the EIS
				<ul style="list-style-type: none"> Businesses that accept inbound telephone calls would need to review inbound call scripts and/or IVR scripts. To the extent that the current inbound call script and/or IVR script does not include information on how a consumer can opt-out of the sale of personal information, the inbound call script would need to be modified and/or the IVR script would need to be reprogrammed. 	
11.	§ 7014(e)(3)(A)	<u>Limit the use of sensitive information notice must be provided offline.</u> The Proposed Regulation would require that businesses that are required to provide an option for consumers to limit the use of sensitive personal information, and that collect such information offline (e.g., brick-and-mortar stores), provide a notice "through an offline method" of the consumer's right to limit the use of their sensitive personal information.	<p>The CPRA does <u>not</u> require that information regarding how consumers can limit the use of sensitive personal information be provided in notices at collection.⁴⁷</p> <p>The CPRA only requires that a business that is required to provide an option for consumers to limit the use of sensitive personal information include a "clear and conspicuous link on the business's internet homepages, titled 'Limit the Use of My Sensitive Personal Information'"⁴⁸</p>	<ul style="list-style-type: none"> Businesses will need to review their in-store collection practices to verify whether they do, or do not, collect sensitive personal information within brick-and-mortar stores. If the business is required to provide the ability to limit the use of sensitive personal information, the business will need to design, print, distribute, and post offline signage in such stores and/or update any paper forms that collect sensitive personal information. Businesses may have to monitor brick-and-mortar locations to verify that any in-store signage has not been removed, replaced, or obscured. 	Not accounted for by BEAR / 0 hours and \$0 assigned
12.	§ 7014(e)(3)(B)	<u>Limit the use of sensitive information notice must be provided over the phone.</u> The Proposed Regulation would require that businesses that (1) are required to provide an option for consumers to limit the use of sensitive personal information and (2) collect such information over the phone, "provide notice orally during the call when the sensitive personal information is collected."	<p>The CPRA does <u>not</u> require that information regarding how consumers can limit the use of sensitive personal information be provided in notices at collection.⁴⁹</p> <p>The CPRA only requires that a business that is required to provide an option for consumers to limit the use of sensitive personal information include a "clear and conspicuous link on the business's internet homepages, titled 'Limit the Use of My Sensitive Personal Information'"⁵⁰</p>	<ul style="list-style-type: none"> Businesses will need to review their telephone collection practices to verify whether they do, or do not, collect sensitive personal information over the telephone. If the business is required to provide the ability to limit the use of sensitive personal information, the business will need to create a call script and/or reprogram the IVR script to notify consumers that they can limit the use of their sensitive personal information. Businesses may need to train customer service agents to provide the required notice. 	Not accounted for by BEAR / 0 hours and \$0 assigned

⁴⁷ See CAL. CIV. CODE § 1798.100(a) (West 2022).

⁴⁸ CAL. CIV. CODE § 1798.121(a), 135(a)(2) (West 2022).

⁴⁹ See CAL. CIV. CODE § 1798.100(a) (West 2022).

⁵⁰ CAL. CIV. CODE § 1798.121(a), 135(a)(2) (West 2022).

Attn: Brian Soublet
 August 17, 2022
 Page 14

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CCPA / BEAR within the EIS
				<ul style="list-style-type: none"> Businesses may have an ongoing obligation to monitor telephone interactions to ensure that customer service agents are providing the required notice. 	
13.	§ 7014(e)(3)(C)	<p><u>Limit the use of sensitive information notice must be provided as part of a connected device.</u> The Proposed Regulation would require that businesses that (1) are required to provide an option for consumers to limit the use of sensitive personal information and (2) collect such information through a connected device "provide notice in a manner that ensures that the consumer will encounter the notice while using the device."</p>	<p>The CPRA does <u>not</u> require that information regarding how consumers can limit the use of sensitive personal information be provided in notices at collection.⁵¹</p> <p>The CPRA only requires that a business that is required to provide an option for consumers to limit the use of sensitive personal information include a "clear and conspicuous link on the business's internet homepages, titled 'Limit the Use of My Sensitive Personal Information'"⁵²</p>	<ul style="list-style-type: none"> Businesses will need to review their connected devices to verify whether they do, or do not, collect sensitive personal information. If the business is required to provide the ability to limit the use of sensitive personal information, the business will need to design a mechanism through which consumers can be notified of their ability to limit the use of such information. 	Not accounted for by BEAR / 0 hours and \$0 assigned
14.	§ 7014(e)(3)(D)	<p><u>Limit the use of sensitive information notice must be provided as part of a virtual reality experience.</u> The Proposed Regulation would require that businesses that (1) are required to provide an option for consumers to limit the use of sensitive personal information and (2) collect such information through augmented or virtual reality "provide notice in a manner that ensures that the consumer will encounter the notice while in the augmented or virtual reality environment."</p>	<p>The CPRA does <u>not</u> require that information regarding how consumers can limit the use of sensitive personal information be provided in notices at collection.⁵³</p> <p>The CPRA only requires that a business that is required to provide an option for consumers to limit the use of sensitive personal information include a "clear and conspicuous link on the business's internet homepages, titled 'Limit the Use of My Sensitive Personal Information'"⁵⁴</p>	<ul style="list-style-type: none"> Businesses will need to review any augmented or virtual reality environments that they offer (e.g., gaming environments) to verify whether they do, or do not, collect sensitive personal information. If the business is required to provide the ability to limit the use of sensitive personal information, the business will need to design a mechanism through which consumers can be notified of their ability to limit the use of such information. 	Not accounted for by BEAR / 0 hours and \$0 assigned
15.	§ 7021(a)	<p><u>Confirm receipt of requests to correct within 10 business days.</u> The Proposed Regulation would require that a business confirm receipt of a request to correct within 10 business days.</p>	<p>The CPRA does <u>not</u> require that a business confirm receipt of a request to correct.</p> <p>The current CCPA Regulations only require that a business confirm receipt of a request to know or a request to delete.</p>	<ul style="list-style-type: none"> Businesses will need to review and revise their data subject request policies, procedures, or protocols to include a process by which requests to correct will be acknowledged within 10 business days. 	Not accounted for by BEAR / 0 hours and \$0 assigned

⁵¹ See CAL. CIV. CODE § 1798.100(a) (West 2022).

⁵² CAL. CIV. CODE § 1798.121(a), 135(a)(2) (West 2022).

⁵³ See CAL. CIV. CODE § 1798.100(a) (West 2022).

⁵⁴ CAL. CIV. CODE § 1798.121(a), 135(a)(2) (West 2022).

Attn: Brian Soublet
 August 17, 2022
 Page 15

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CPPA / BEAR within the EIS
			They do <u>not</u> require that a business confirm receipt of a request to correct.		
16.	§ 7022(b)(3)	<u>Flowing down requests to delete to third parties.</u> The Proposed Regulation would require that a business notify "all third parties to whom the business has sold or shared the personal information" after a request to delete has been received.	The CPRA and current CCPA Regulations only require that businesses flow down deletion requests to service providers and contractors; they do <u>not</u> require that a business flow down deletion requests to third parties to whom the information was sold prior to receiving a deletion request.	<ul style="list-style-type: none"> • Businesses may need to keep records of all third parties to whom a particular consumer's personal information had been sold. • Businesses may have to establish a communications channel to those third parties with whom the business currently has a relationship through which deletion requests could be transmitted. • Businesses may have to maintain a communications channel to those third parties with whom the business formerly had a relationship (but does not have a current relationship) through which deletion requests could be transmitted. • Businesses may have to flow-down deletion requests to all current and former third party data recipients. • In the event that a third party with whom the business currently has a relationship, or with whom the business formerly had a relationship, is unable to receive flow down requests in an efficient manner, the business may need to document the effort involved with attempting to contact the third party and convey that information to the consumer. 	Not accounted for by BEAR / 0 hours and \$0 assigned
17.	§ 7023(c)	<u>Ensure that personal information subject to a correction request remains corrected.</u> The Proposed Regulation would require that a business that is required to comply with a request to collect personal information "implement measures to ensure that the information remains corrected."	<p>The CPRA only requires that a business correct inaccurate personal information that it holds within its system at the time that a correction request is made.⁵⁵</p> <p>The CPRA does <u>not</u> obligate a business to continue to ensure that corrected personal information remains accurate indefinitely.</p>	<ul style="list-style-type: none"> • Businesses may need to implement a mechanism that puts a permanent system-wide tag on corrected data. • Businesses may need to design a mechanism through which it can flag any new data that enters the system, check it against the corrected information, and ensure that conflicting information does not overwrite the corrected information. • Businesses may need to implement a system through which it can contact the individual in the event conflicting information is entered into the system to ascertain whether the new information is now the correct information (e.g., a new address is provided by the individual after the individual has made a 	Not accounted for by BEAR / 0 hours and \$0 assigned

⁵⁵ CAL. CIV. CODE § 1798.106(a)-(c) (West 2022).

Attn: Brian Soublet
 August 17, 2022
 Page 16

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CPPA / BEAR within the EIS
				correction request with respect to the current address in the system).	
18.	§ 7023(f)(4)	<u>Create process for consumers to submit 250 word statements regarding health-data inaccuracy.</u> The Proposed Regulation would require that a business that collects health information create a process through which a consumer could submit a 250-word statement regarding any alleged inaccurate health-related fact. The business would be required to maintain the consumer's submission (indefinitely) and make it available to any person (presumably a service provider or a third party) with whom the business shares such information.	<p>The CPRA does not impose any <i>direct</i> obligation upon a business to permit consumers to submit 250 word challenges to allegedly inaccurate health information.</p> <p>While the CPRA directs that the CPPA adopt regulations that would permit such 250 word challenges,⁵⁶ pursuant to the APA such regulations should be evaluated for their economic impact. Furthermore, the CPRA in its description of the regulations that should be adopted does not contemplate that a business would be required to transmit the consumer's statement to third parties such as other businesses to which the information had been historically sold.</p>	<ul style="list-style-type: none"> Businesses may need to develop a system through which a consumer could submit a 250-word statement. Businesses may need to develop a system to record and store such statements. As such statements are likely to contain sensitive category data (i.e., health information), business may need to investigate the adequacy of any security measures utilized for such systems. Businesses may need to develop a mechanism to communicate consumer submitted statements to third parties to whom the business intends to share or sell the consumer's health data in the future. Business may need to maintain a comprehensive list of all third parties to whom the business has sold or shared the consumer's health data. Businesses may need to develop a process to retroactively determine whether the data fields that may have been historically shared or sold with third parties include the specific data field that the consumer has alleged is inaccurate. Businesses may need to develop a mechanism to communicate consumer submitted statements to third parties with whom the business shared or sold such health data in the past. 	Not accounted for by BEAR / 0 hours and \$0 assigned
19.	§ 7023(i)	<u>Provide consumers with the name of the source of inaccurate information.</u> The Proposed Regulation would require that a business provide consumers with the name of the source of allegedly inaccurate information.	The CPRA does <u>not</u> require that a business provide the source of inaccurate information following the receipt of a request to correct.	<ul style="list-style-type: none"> Businesses may need to track and record the source of each individual piece of information on a going forward basis. Businesses may need to review information currently in their possession and determine (e.g., investigate) the source of such information. Businesses may need to review their contracts with third party data providers (e.g., service providers that collect information on a business's behalf, data brokers, data sellers, 	Not accounted for by BEAR / 0 hours and \$0 assigned

⁵⁶ CAL. CIV. CODE § 1798.185(a)(8)(D) (West 2022).

Attn: Brian Soublet
 August 17, 2022
 Page 17

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CCPA / BEAR within the EIS
				<p>etc.) to determine whether such contracts (a) prohibit identification of the third party, or (b) mandate that the business notify the third party prior to identifying the third party to a data subject.</p> <ul style="list-style-type: none"> If a contract with a data broker requires that the business notify the data broker prior to identifying the data broker by name to a data subject, the business may need to design a process and system for notifying the data broker within the time period mandated by the contract. 	
20.	§ 7023(j)	<u>Disclose information to allow consumers to confirm correction.</u> The Proposed Regulation would require a business to disclose all specific information maintained on a consumer to allow the consumer to confirm that the business corrected inaccurate information contained in a request to correct. This would not be considered a response to a request to know, nor would it count as one of the two requests to know that a consumer is allowed to submit in a 12-month time period.	The CPRA does <u>not</u> require a business to disclose all specific information on a consumer following a request to correct unless the business has received a separate request to know.	<ul style="list-style-type: none"> Businesses may need to modify their existing data subject request procedures to allow data subjects that had submitted a request to correct to ask for access to their personal information without converting such a request into a "request to know." Businesses may need to ensure the response to these requests was recorded separately from responses to requests to know, and that the business does not count the request as one of the two requests to know permitted within a 12 month period. 	Not accounted for by BEAR / 0 hours and \$0 assigned
21.	§ 7025(b), (c), (e); 7026(a)(1)	<u>Businesses are required to process an opt-out preference signal (even if they have a DNSOSMPI link).</u> The Proposed Regulations would require that any business which sells or shares personal information detect and honor an opt-out preference signal. The Proposed Regulations would specifically "not give the business the choice between posting the above-referenced links or honoring opt-out preference signals."	Although the current CCPA Regulations indicate that a business may need to treat "user-enabled global privacy controls" as a valid request to opt-out, ⁵⁷ the CCPA Regulations were superseded by the passage of the CPRA which indicates that a business may choose to recognize the opt-out preference signal as an alternative to posting a "do not sell or share my personal information" link on their homepage. ⁵⁸ Neither the current CCPA Regulations nor the CPRA state that a business <u>must</u> honor an opt-out preference signal.	<ul style="list-style-type: none"> Businesses that sell or share personal information may need to adapt their websites to identify an opt-out preference signal. If the opt-out preference signal is detected, businesses may need to stop the sale/sharing of personal information. If the consumer has authenticated (i.e., is a known consumer), businesses may need to record the opt-out preference within the consumer's profile in order for the preference to apply the next time that the consumer authenticates (i.e., logs-in). Businesses may need to monitor for new standards and methods of transmitting an opt-out preference signal. If a new standard or method of transmitting an opt-out preference signal is developed, a 	Not accounted for by BEAR / 0 hours and \$0 assigned

⁵⁷ CAL. CODE REGS. tit. 11, § 7026(c) (2022).

⁵⁸ CAL. CIV. CODE § 1798.135(b)(1) (West 2022).

Attn: Brian Soublet
 August 17, 2022
 Page 18

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CPPA / BEAR within the EIS
				business may need to adjust its own technology to detect, and respond to, the signal.	
22.	§7025(c)(1), (7)(B), (7)(C)	<u>Create persistence mechanism for opt-out preference signal for known consumers.</u> The Proposed Regulations would require businesses create a persistence mechanism so that if (1) an opt-out preference signal is detected on Day 1, (2) the consumer authenticates into the website (e.g., she logs in), (3) the consumer visits the website on Day 2 while not broadcasting an opt-out preference signal, and (4) the consumer authenticates into the website (e.g., she logs in), then the business would continue to apply an opt-out preference.	While the CPRA directs that the CPPA adopt regulations that would govern how a business responds to opt-out preference signals, ⁵⁹ pursuant to the APA such regulations should be evaluated for their economic impact. Furthermore, the CPRA in its description of the regulations that should be adopted does <u>not</u> contemplate that a business would be <u>required</u> (i.e., mandated) to treat opt-out preference signals as a request to opt-out of sale/sharing or that the signal be connected to the device and the consumer.	<ul style="list-style-type: none"> Businesses may need to create a system to detect whether an opt-out preference signal has been broadcast. Businesses may need to create a system to record an opt-out preference in a manner that can be recognized and applied the next time a known consumer authenticates (i.e., logs-in). 	Not accounted for by BEAR / 0 hours and \$0 assigned
23.	§ 7025(c)(5)	<u>Create persistence mechanism for known browsers (but not known consumers) such that initial opt-out preference signal continues to be treated as an "opt out" even if the consumer chooses to stop broadcasting the signal.</u> The Proposed Regulations would prohibit businesses from interpreting the absence of an opt-out preference signal after a consumer previously set an opt-out preference signal as consent to opt-in to the sale or sharing of personal information. As a result, if a consumer broadcast an opt-out preference signal (e.g., it broadcast by default from the consumer's browser) on Day 1, and a consumer (either the same consumer or a different consumer) manually disabled the opt-out preference signal to reflect their choice that data could be shared on Day 2, the business would be required to continue to treat the browser as opted-out despite the consumer's action to disable the signal.	The CPRA does <u>not</u> contain any requirements for the treatment of information when a previously communicated opt-out preference signal is absent. The CPRA allows, but does not require, businesses to "provide a link to a web page that enables the consumer to consent to the business ignoring the opt-out preference signal." ⁶⁰	<ul style="list-style-type: none"> Businesses may need to create a system to record an opt-out preference signal, so that the next time that the browser/device visits the businesses website data is not sold/shared regardless of whether the browser/device continues to be broadcasting the opt-out preference signal. 	Not accounted for by BEAR / 0 hours and \$0 assigned
24.	§7025(c)(6)	<u>Display whether opt-out preference signal has been processed.</u> The Proposed Regulation would require a business to display whether a	The CPRA does <u>not</u> contain any requirement for communicating whether an opt-out preference signal has been processed.	<ul style="list-style-type: none"> Businesses may need to create a process to determine whether or not opt-out preference signals have been processed. 	Not accounted for by BEAR / 0 hours and \$0 assigned

⁵⁹ CAL. CIV. CODE § 1798.185(a)(20) (West 2022).

⁶⁰ CAL. CIV. CODE § 1798.135(b)(2) (West 2022).

Attn: Brian Soublet
 August 17, 2022
 Page 19

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CPPA / BEAR within the EIS
		consumer's opt-out preference signal has been processed.		<ul style="list-style-type: none"> Businesses may need to modify webpages to display notifications when opt-out preference signals have been received. 	
25.	§7025(c)(6), (c)(4)	<u>Display whether opt-out preference signal conflicts with a financial incentive enrollment.</u> The Proposed Regulation would require that if (1) a consumer broadcasts an opt-out preference signal, and (2) a consumer chooses to remain enrolled in a financial incentive program, then the business must "display in a conspicuous manner" the status of the "consumer's choice."	The CPRA does <u>not</u> contain any requirement for communicating the status of the consumer's opt-out and/or financial incentive enrollment.	<ul style="list-style-type: none"> In addition to the compliance burdens identified with respect to 7025(c)(6), a business may need to modify webpages to display the consumer's status regarding enrollment in a financial incentive program. 	Not accounted for by BEAR / 0 hours and \$0 assigned
26.	§7026(a)(4)	<u>DNSOSMPI link cannot be within a cookie banner.</u> The Proposed Regulation appear to state that a "cookie banner or cookie controls" cannot be used as an acceptable method for submitting DNSOSMPI requests.	The CPRA does <u>not</u> prohibit a business from placing a DNSOSMPI option within a cookie banner or notice.	<ul style="list-style-type: none"> Businesses may need to review their websites for cookie banners that include DNSOSMPI links or terminology. To the extent that the business utilizes a cookie banner to display the DNSOSMPI option, the business may need to create an alternative method for submitting a DNSOSMPI request. 	Not accounted for by BEAR / 0 hours and \$0 assigned
27.	§ 7026(f)(3)	<u>Flowing down requests to opt-out of sale or sharing to third parties.</u> The Proposed Regulation appears to require that a business that has received a request to opt-out of sale or sharing "notify all third parties to whom the business makes personal information available, including businesses authorized to collect personal information or controlling the collection of personal information on the business's premises." The business must then direct them to "1) comply with the consumer's request and 2) to forward the request to any other person with whom the third party has disclosed or shared the personal information." Third parties would, in turn, be prohibited from "retain[ing], us[ing], or disclos[ing] the personal information" unless they became a service provider.	<p>The CPRA gives businesses the opportunity to communicate consumers' requests to "any person authorized by the business to collect personal information," but does <u>not</u> require it.⁶¹</p> <p>Further note that if a business chooses to communicate a consumer's opt-out request, the third party is <u>not</u> required to delete the personal information or sign a service provider agreement; they are, however, prohibited from using, sharing, retaining, or disclosing the personal information if such activities are not in-line with the services that they are providing.⁶²</p>	<ul style="list-style-type: none"> Businesses may need to keep records of all third parties to whom a consumer's personal information has been made available. Businesses may need to keep records of all third parties it authorizes to collect personal information. Businesses may need to keep records of all third parties controlling the collection of personal information on the business' premises. Businesses may have to establish a communications channel to such third parties with whom the business currently has a relationship through which opt-out requests could be transmitted. Businesses may have to maintain a communications channel to such third parties with whom the business formerly had a relationship (but does not have a current relationship) through which opt-out of sale/sharing requests could be transmitted. 	Not accounted for by BEAR / 0 hours and \$0 assigned

⁶¹ CAL. CIV. CODE § 1798.135(f) (West 2022).

⁶² CAL. CIV. CODE § 1798.135(f) (West 2022).

Attn: Brian Soublet
 August 17, 2022
 Page 20

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CCPA / BEAR within the EIS
				<ul style="list-style-type: none"> Businesses may have to flow-down opt-out requests to all current and former third party data recipients. Businesses may have to create a notification and instruction processes to direct third party data recipients to comply with the consumer request and to forward the request to any other persons the third party had shared the information with. 	
28.	§ 7026(i)	<u>Exempt requests made through opt-out preference signals from written authorization requirement for agents.</u> The Proposed Regulation would allow an authorized agent to submit a request to opt-out of sale/sharing via the opt-out preference signal without obtaining and providing written permission from the consumer.	<p>The CPRA does <u>not</u> allow agents to submit opt-out requests through opt-out signal preferences or without written authorization from the consumer.</p> <p>Furthermore the current CCPA Regulations stated that a "[u]ser-enabled global privacy control . . . shall be considered a request directly from the consumer, not through an authorized agent."⁶³</p>	<ul style="list-style-type: none"> Businesses may need to create a process for authorized agents to indicate the consumer for whom they are communicating the opt-out preference signal. Businesses may need to revise processes for authorized agents to accept opt-out preference signals without written permission. Businesses may need to create a system to record opt-out preference signals from agents and connect such requests to consumer data. Businesses may need to create processes to identify and prevent unauthorized requests made by unauthorized third parties. 	Not accounted for by BEAR / 0 hours and \$0 assigned
29.	§ 7027(g)(3)	<u>Flowing down requests to limit use of sensitive information to previously engaged third parties.</u> The Proposed Regulation would require that a business "notify all third parties to whom the business has disclosed or made available the consumer's sensitive personal information" after receiving a request limit and direct them to "1) comply with the consumer's request and 2) to forward the request to any other person with whom the third party has disclosed or shared the sensitive personal information."	The CPRA does not require that businesses flow down requests to limit use and disclosure of sensitive personal information to third parties.	<ul style="list-style-type: none"> Businesses may need to keep records of all third parties to whom a consumer's sensitive personal information had been disclosed or made available. Business may have to establish a communications channel to such third parties with whom the business currently has a relationship through which limiting requests could be transmitted. Businesses may have to maintain a communications channel to such third parties with whom the business formerly had a relationship (but does not have a current relationship) through which limiting requests could be transmitted. Businesses may have to flow-down limiting requests to all current and former third party data recipients. Businesses may have to create a notification and instruction process to direct third party 	Not accounted for by BEAR / 0 hours and \$0 assigned

⁶³ CAL. CODE REGS. tit. 11, § 7026(f) (2022).

Attn: Brian Soublet
 August 17, 2022
 Page 21

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CPPA / BEAR within the EIS
				data recipients to comply with the consumer request and to forward the request to any other person the third party had shared the sensitive information with.	
30.	§ 7027(g)(4)	<p><u>Flowing down requests to limit use of sensitive information to currently engaged third parties.</u> The Proposed Regulation would require that a business "notify all third parties to whom the business has disclosed or made available the consumer's sensitive personal information," including businesses authorized to collect personal information or controlling the collection of personal information on the business's premises" after receiving a request to limit and direct them to "1) comply with the consumer's request and 2) to forward the request to any other person with whom the third party has disclosed or shared the sensitive personal information."</p>	The CPRA does <u>not</u> require that businesses flow down requests to limit use and disclosure of sensitive personal information to third parties.	<ul style="list-style-type: none"> • Businesses may need to keep records of all third parties to whom a consumer's sensitive personal information has been disclosed or made available. • Businesses may need to keep records of all third parties it authorizes to collect sensitive personal information. • Businesses may need to keep records of all third parties controlling the collection of sensitive personal information on their premises. • Business may have to establish a communications channel to such third parties with whom the business currently has a relationship through which limiting requests could be transmitted. • Businesses may have to maintain a communications channel to such third parties with whom the business formerly had a relationship (but does not have a current relationship) through which limiting requests could be transmitted. • Businesses may have to flow-down limiting requests to all current and former third party data recipients. • Businesses may have to create a notification and instruction processes through which it can direct third party data recipients to comply with the consumer request and to forward the request to any other persons the third party had shared the sensitive information with. 	Not accounted for by BEAR / 0 hours and \$0 assigned
31.	§7027(g)(5)	<p><u>Confirm whether request to limit has been processed.</u> The Proposed Regulation would require a business to provide a means by which the consumer can confirm that their request to limit has been processed, such as by displaying a toggle or radio button.</p>	The CPRA does <u>not</u> contain any requirement for communicating whether a request to limit has been processed.	<ul style="list-style-type: none"> • Businesses may need to create a process to determine whether or not requests to limit have been processed. • Businesses may either need to (1) modify webpages to display notifications when requests to limit have been processed, or (2) modify data subject request submissions and processes to allow consumers to request separate confirmation of the right to limit. 	Not accounted for by BEAR / 0 hours and \$0 assigned

Attn: Brian Soublet
 August 17, 2022
 Page 22

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CPPA / BEAR within the EIS
32.	§ 7028(a)	<u>Two-step consent process for opting-in to the sharing or sale of personal information and/or the use and disclosure of sensitive personal information.</u> The Proposed Regulation would require requests to opt-in to the sharing or selling of personal information and/or the use and disclosure of sensitive personal information to use a two-step opt-in process.	<p>The CPRA does <u>not</u> require specific opt-in procedures for the use and disclosure of sensitive personal information.</p> <p>The CPRA does <u>not</u> require specific procedures to obtain consumer's intentional use or direction to share or disclose personal information to third parties.</p>	<ul style="list-style-type: none"> Businesses may need to review current opt-in procedures for use and disclosure of sensitive personal information. Businesses may need to revise current procedures or implement new procedures for requests to opt-in to the use and disclosure of sensitive personal information. Businesses may need to develop processes to separately confirm all opt-in requests. Businesses may need to track consumers who only complete half of the opt-in process to ensure that those requests are not treated as a full opt-in. Business may need to review how they are currently obtaining indications by consumers that the consumer intends for his/her personal information to be used or disclosed to third parties to determine whether the consumer's indication is enough to satisfy the Proposed Regulation's double-opt-in requirement. If current systems to obtain intentional use or direction do not conform to the Proposed Regulation's standard, businesses may need to consider modifying their process for obtaining and documenting intentional use or disclosure to third parties. 	Not accounted for by BEAR / 0 hours and \$0 assigned
33.	§ 7050(c)(1)	<u>Prohibit classifying cross-contextual behavioral advertising companies as service providers or contractors.</u> The Proposed Regulation would prohibit businesses from contracting with service providers or contractors for cross-contextual behavioral advertising services.	The CPRA does <u>not</u> prohibit contracting service providers or contractors to provide cross-contextual behavioral advertising services.	<ul style="list-style-type: none"> Businesses would need to review their contracts with cross-context behavioral advertisers to identify whether those contracts classified the advertiser as either a service provider or a contractor. If a contract did classify a cross-context behavioral advertiser as a service provider or contractor, the business may need to renegotiate the contract and/or reassess whether personal information can continue to be provided to such companies consistent with the business's overall strategy regarding the sharing of personal information with non-service providers. 	Not accounted for by BEAR / 0 hours and \$0 assigned
34.	§ 7051(a)(2)	<u>Requires contracts with service providers and contractors to identify business purposes and services for processing personal information.</u> The Proposed Regulation would require that	The CPRA does <u>not</u> require that the contract include a statement of the business purposes, nor does it prohibit the described	<ul style="list-style-type: none"> Businesses might have to review each contract they have with service providers and contractors to ensure that the contract specifically identifies the business purposes 	Not accounted for by BEAR / 0 hours and \$0 assigned

Attn: Brian Soublet
 August 17, 2022
 Page 23

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CPPA / BEAR within the EIS
		contracts between a business and a service provider or contractor specify the business purposes and services for which the service provider or contractor is processing personal information, and specify that the business is disclosing personal information for that limited and specific purpose. The description of the business purposes <u>cannot</u> be generic.	business purposes from being general or generally referring to the entire contract. ⁶⁴	<p>for which the service provider/contractor is processing personal information.</p> <ul style="list-style-type: none"> Businesses would need to revise any contracts that only describe the business purposes by (1) providing a general business purpose or (2) referencing an overarching agreement (such as a master services agreements). 	
35.	§ 7051(a)(8)	<u>Requires agreements with service providers or contractors to include a 5-day notice provision of non-compliance.</u> The Proposed Regulation would require that agreements between a business and a service provider or contractor require the service provider or contractor to notify the business "no later than five business days after it makes a determination" that it can no longer meet its obligations under the CCPA or the Proposed Regulations.	The CPRA requires that a contract with a service provider or contractor obligate the service provider or contractor to "notify the business if it makes a determination" that it can no longer meet its obligations under the CPRA. ⁶⁵ The CPRA does <u>not</u> require that the contract specify that the notification must occur within five business days.	<ul style="list-style-type: none"> Each contract with a service provider or contractor may need to be reviewed to determine whether the notification provision specified a five-day time period for notice. If a contract did not specify a time period, or if it specified a time period that was longer than five business days, the business would need to contact the service provider or contractor, propose an amendment to the contract to comply with the Proposed Regulation, and enter into renegotiation discussions to bring the contract into compliance. If the service provider or contractor is unwilling, or unable, to agree to the five-day time period, the business may need to consider whether termination of the contract is warranted. 	Not accounted for by BEAR / 0 hours and \$0 assigned
36.	§ 7051(e)	<u>Due diligence of service providers or contractors.</u> The Proposed Regulation states that if a business does not conduct "due diligence of its service providers or contractors" that fact may factor into whether the business has a reason to believe that the service provider or contractor is using information in violation of the CCPA.	The CPRA provides a safe harbor from vicarious liability (i.e., a business "shall not be liable") if the business communicates a consumer's opt-out requests to a "person" and that person violates the CPRA so long as the business does "not have actual knowledge, or reason to believe, that the person intends to commit such a violation." ⁶⁶ The CPRA does <u>not</u> require a business to conduct due diligence, or impose a duty upon the business to investigate or inquire about the privacy	<ul style="list-style-type: none"> Businesses may need to design a program to conduct due diligence on all service providers or contractors privacy practices (e.g., auditing, contract review, questionnaires, and/or other forms of monitoring). Such a program may need to be in addition to any existing due diligence activities that are focused on other compliance-related concerns (e.g., data security). Businesses may need to allocate sufficient staff and resources to implement the due diligence program on an ongoing basis. 	Not accounted for by BEAR / 0 hours and \$0 assigned

⁶⁴ CAL. CIV. CODE § 1798.100(d) (West 2022).

⁶⁵ CAL. CIV. CODE § 1798.100(d)(4) (West 2022).

⁶⁶ CAL. CIV. CODE § 1798.135(g) (West 2022).

Attn: Brian Soublet
 August 17, 2022
 Page 24

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CPPA / BEAR within the EIS
			practices of a service provider or contractor.		
37.	§ 7052(a)	<u>Third parties must comply with forwarded deletion or opt-out requests.</u> The Proposed Regulation would require a third party to comply with a consumer's "request to delete or request to opt-out of sale/sharing forwarded to them from a business" that initially provided the consumer's data to the third party.	<p>The CPRA contains a requirement that company B must honor opt-out of sale/sharing requests that have been communicated to it by business A, but only where company B is a "person authorized by the business [A] to collect personal information."⁶⁷</p> <p>The CPRA does <u>not</u> impose any requirement for business A to communicate a <i>deletion</i> request to third parties, or for third parties to honor <i>deletion</i> requests that have been forwarded to them by businesses.</p>	<ul style="list-style-type: none"> • Third parties may need to design a process through which they could receive opt-out communications from businesses that currently provide (or previously provided) them with personal information. • Third parties may need to communicate that process to those businesses that provide/provided them with personal information. • Businesses may need to design a process through which it could transmit opt-out communications to multiple third parties that may each have different communication processes (e.g., email, XLS, API, etc.). • Third parties may need to design a process through which they could receive deletion communications from businesses that currently provide (or previously provided) them with personal information. • Third parties may need to communicate that process to businesses that provide them with personal information. • Businesses may need to design a process through which it could transmit deletion communications to multiple third parties that may each have different communication processes (e.g., email, XLS, API, etc.). 	Not accounted for by BEAR / 0 hours and \$0 assigned
38.	§ 7052(b)	<u>Third parties must comply with forwarded limit the use of sensitive information requests.</u> The Proposed Regulation would require a third party to comply with a "consumer's request to limit forwarded to them from a business that provided, made available, or authorized the collection of the consumer's sensitive personal information"	<p>The CPRA contains a requirement that company B must honor opt-out of sale/sharing requests that have been communicated to it by business A, but only where company B is a "person authorized by the business [A] to collect personal information."⁶⁸</p> <p>The CPRA does <u>not</u> impose any requirement for business A to communicate</p>	<ul style="list-style-type: none"> • Third parties may need to design a process through which it could receive limit the use requests from businesses that provide the third party with personal information. • Third parties may need to communicate that process to businesses that provide (or provided) them with personal information. • Businesses may need to design a process through which it could transmit limit the use 	Not accounted for by BEAR / 0 hours and \$0 assigned

⁶⁷ CAL. CIV. CODE § 1798.135(f) (West 2022).

⁶⁸ CAL. CIV. CODE § 1798.135(f) (West 2022).

Attn: Brian Soublet
 August 17, 2022
 Page 25

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CCPA / BEAR within the EIS
			a <i>limit the use</i> request to third parties, or for third parties to honor a limit the use request that has been forwarded to them by a business.	requests to multiple third parties that may each have different communication processes (e.g., email, XLS, API, etc.).	
39.	§ 7052(c)	<u>Third parties that collect personal information online must honor opt-out preference signals.</u> The Proposed Regulation would require that a third party that collects personal information from a consumer online (e.g., through a first party's website) recognize and honor an opt-out preference signal received by the first party website.	Although the current CCPA Regulations indicate that a business may need to treat "user-enabled global privacy controls" as a valid request to opt-out, ⁶⁹ the CCPA Regulations were superseded by the passage of the CPRA which indicates that a business may choose to recognize the opt-out preference signal as an alternative to posting a "do not sell or share my personal information" link on their homepage. ⁷⁰ Neither the current CCPA Regulations nor the CPRA state that a third party that collects personal information online must honor an opt-out preference signal received by a first party's website.	<ul style="list-style-type: none"> • Third parties that collect personal information online may need to design systems and technology capable of detecting opt-out preference signals received by first party websites. • Third parties that collect personal information from multiple websites may need to design systems and technology capable of opting a consumer out of the sale/sharing of personal information from one website, but not another. 	Not accounted for by BEAR / 0 hours and \$0 assigned
40.	§ 7053(a)(6)	<u>Requires agreements with third parties to include a 5-day notice provision of non-compliance.</u> The Proposed Regulation would require that agreements between a business and a third party require the third party to notify the business "no later than five business days after it makes a determination" that it can no longer meet its obligations under the CCPA or the Proposed Regulations.	The CPRA requires that a contract with a third party obligate the third party to "notify the business if it makes a determination" that it can no longer meet its obligations under the CPRA. ⁷¹ The CPRA does <u>not</u> require that the contract specify that the notification must occur within five business days.	<ul style="list-style-type: none"> • Each contract with a third parties may need to be reviewed to determine whether the notification provision specified five-day non-compliance notification. • If a contract did not specify a time period, or if it specified a time period that was longer than five business days, the business may need to contact the third party, propose an amendment to the contract to comply with the Proposed Regulation, and enter into renegotiation discussions to bring the contract into compliance. • If the third party is unwilling, or unable, to agree to the five-day time period, the business may need to consider whether termination of the contract is warranted. 	Not accounted for by BEAR / 0 hours and \$0 assigned

⁶⁹ CAL. CODE REGS. tit. 11, § 7026(c) (2022).

⁷⁰ CAL. CIV. CODE § 1798.135(b)(1) (West 2022).

⁷¹ CAL. CIV. CODE § 1798.100(d)(4) (West 2022).

Attn: Brian Soublet
 August 17, 2022
 Page 26

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CCPA / BEAR within the EIS
41.	§ 7053(b)	<u>Requires agreements with third parties to obligate the third party to check for opt-out signals.</u> The Proposed Regulation would require businesses that sell or share personal information with third parties to contractually require the third party to "check for and comply with" a consumer's opt-out preference signal unless the business confirms that the consumer consented in the first instance to the sale or sharing.	The CPRA does <u>not</u> require that a contract with a third party obligate the third party (i.e., a company that is not a service provider) to check for and comply with a consumer's opt-out preference signal.	<ul style="list-style-type: none"> Businesses that sell or share personal information may need to review each contract that they have with third parties to determine whether the contract contains a requirement that third party check for and comply with a consumer's opt-out preference signal. If a contract did not contain such a provision, the business may need to contact the third party, propose an amendment to comply with the Proposed Regulation, and enter into renegotiation discussions to bring the contract into compliance. If the third party is unwilling, or unable, to agree to check for and comply with consumer opt-out preference signals the business may need to consider whether termination of the contract was warranted. 	Not accounted for by BEAR / 0 hours and \$0 assigned
42.	§ 7053(e)	<u>Due diligence of third parties.</u> The Proposed Regulation state that if a business does not conduct "due diligence of third part[ies]," that fact may factor into whether the business has a reason to believe that the third party is using information in violation of the CCPA.	The CPRA provides a safe harbor from vicarious liability (i.e., a business "shall not be liable") if the business communicates a consumer's opt-out requests to a "person" and that person violates the CPRA so long as the business does "not have actual knowledge, or reason to believe, that the person intends to commit such a violation." ⁷² The CPRA does <u>not</u> require a business to conduct due diligence, or impose a duty upon the business to investigate or inquire about the privacy practices of a third party.	<ul style="list-style-type: none"> Businesses may need to design a program to conduct due diligence on all third party data recipients (e.g., auditing, contract review, questionnaires, and/or other forms of monitoring). Such a program may need to be in addition to any existing due diligence activities that are focused on other compliance-related concerns (e.g., data security). Businesses may need to allocate sufficient staff and resources to implement the due diligence program on an ongoing basis. 	Not accounted for by BEAR / 0 hours and \$0 assigned
43.	§ 7102(a)(1)(B)	<u>Report quantity of correction requests received.</u> The Proposed Regulation would require businesses that process personal information regarding more than 10 million Californians to compile the quantity of correction requests received each calendar year	<p>The CPRA does <u>not</u> require businesses to publish metrics regarding correction requests.</p> <p>The current CCPA Regulations require that a business that collects personal information of more than 10 million Californians publish metrics regarding access, deletion, and opt-out requests; it does <u>not</u> require that such metrics be published regarding correction requests.</p>	<ul style="list-style-type: none"> Impacted businesses would be required to compile and review the quantity of correction requests received each calendar year. For businesses that don't keep correction requests in an automated database, that requirement may necessitate a manual review of correction requests received via multiple channels (e.g., offline, online) and multiple business personnel (e.g., data privacy officer, human resources, customer service, etc.). Note that for businesses that have routinely handled correction-like requests prior to the CPRA (e.g., as a matter of course through 	Not accounted for by BEAR / 0 hours and \$0 assigned

⁷² CAL. CIV. CODE § 1798.135(g) (West 2022).

Attn: Brian Soublet
 August 17, 2022
 Page 27

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CPPA / BEAR within the EIS
				customer service), the Proposed Regulation may require such requests to be centralized, managed, and tracked in a manner that facilitates reporting separate and apart from the manner in which they are currently handled.	
44.	§ 7102(a)(1)(E)	<u>Report quantity of requests to limit the use of sensitive personal information.</u> The Proposed Regulation would require businesses that process personal information regarding more than 10 million Californians to compile and publish statistics regarding the quantity of "requests to limit" that the business received.	<p>The CPRA does <u>not</u> require businesses to publish metrics regarding requests to limit the use of sensitive information.</p> <p>The current CCPA Regulations require that a business that collects personal information of more than 10 million Californians publish metrics regarding access, deletion, and opt-out requests; it does <u>not</u> require that such metrics be published regarding limit the use of sensitive information requests.</p>	<ul style="list-style-type: none"> Businesses would be required to compile and review the quantity of limit the use requests received each calendar year. For businesses that don't keep limit the use requests in an automated database, that requirement may necessitate a manual review of such requests received via multiple channels (e.g., offline, online) and multiple business personnel (e.g., data privacy officer, human resources, customer service, etc.). 	Not accounted for by BEAR / 0 hours and \$0 assigned
45.	§ 7102(a)(1)(F)	<u>Report elapsed time to respond to correction and limit the use requests.</u> The Proposed Regulation would require businesses that process personal information regarding more than 10 million Californians to compile and publish statistics regarding the median or mean number of days the business took to respond to correction requests and limit the use of sensitive personal information requests.	<p>The CPRA does <u>not</u> require businesses to publish metrics regarding correction requests.</p> <p>The current CCPA Regulations require that a business that collects personal information of more than 10 million Californians publish metrics regarding access, deletion, and opt-out requests; it does <u>not</u> require that such metrics be published regarding correction or limit the use requests.</p>	<ul style="list-style-type: none"> In addition to the compliance steps described above in relation to 7102(a)(1)(B) and 7102(a)(1)(E), a business would need to calculate the elapsed time between the date that each correction and limit the use request was received and the date that the business provided a substantive response to the request. For businesses that don't keep such requests in an automated database, this requirement may necessitate a manual review of the date that requests were received via multiple channels (e.g., offline, online) and multiple business personnel (e.g., data privacy officer, human resources, customer service, etc.), as well as the date the business substantively responded to the request. Note that businesses that have routinely handled correction-like requests prior to the CPRA (e.g., as a matter of course through customer service), the Proposed Regulation may require that such requests be centralized, managed, and tracked in a manner that facilitates reporting separate and apart from the manner in which they are currently handled. Businesses would be required to modify their privacy notices to include the new metric. 	Not accounted for by BEAR / 0 hours and \$0 assigned

Attn: Brian Soublet
 August 17, 2022
 Page 28

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CPPA / BEAR within the EIS
46.	§ 7304(c)	<p><u>Unannounced audits.</u> The Proposed Regulation would allow the CPPA to conduct "announced or unannounced" audits.</p>	<p>The CPPA and the Office of the California Attorney General do <u>not</u> currently conduct "unannounced" audits or investigations of companies. Currently inquiries from the Office of the California Attorney General take the form of notices of violation, requests for information, requests for documents, or requests for interviews; all such investigatory mechanisms have provided at least 30 days for the company to identify, collect, and transmit requested information or documents.</p> <p>The CPRA does <u>not</u> discuss "unannounced" or surprise audits.</p>	<ul style="list-style-type: none"> • Unannounced audits are – by their nature – disruptive to normal business operations as the company does not have time to efficiently review requests for materials in advance, prepare the requested materials, and identify relevant personnel with information requested. BEAR did not account for the business disruption inherent in responding to an unannounced audit by a government agency. • Businesses may need to develop a policy, procedure, and protocol for responding to unannounced audits. • Businesses may need to train their staff on the policy, procedure and protocol (see previous bullet) to ensure that staff notify correct personnel internally in the event of an unannounced audit, fully comply with legitimate requests of the auditor, and protect company and personal information from any request that may be overly broad, unduly burdensome, or injurious to the company or to the rights of other individuals. • Businesses that maintain government access policies (sometimes referred to as law enforcement policies) may need to revise those policies to account for unannounced audits. • The Proposed Regulation anticipates that the CPPA may request, as part of its audit, access to personal information. <i>See</i> Proposed Regulation § 7304(e). Business may need to determine whether granting access to personal information about Californians would also allow the CPPA to access personal information of non-Californians (i.e., residents of other jurisdictions). • To the extent that a business could not ensure during an "unannounced" audit that information about non-Californians could be screened from the CPPA, the business would need to determine whether the right of the CPPA to conduct unannounced audits would interfere with other non-California data privacy laws – such as the European GDPR – or contractual prohibitions that either prevent 	<p>Not accounted for by BEAR / 0 hours and \$0 assigned</p>

Attn: Brian Soublet
 August 17, 2022
 Page 29

	Proposed Regulation	New obligation that would be imposed on businesses	Comparison to existing law or regulation	Compliance burden that would be imposed by the Proposed Regulations (the "Delta")	Burden accounted for by the CPPA / BEAR within the EIS
				<p>the business from granting access to personal information or mandate that the business notify business partners and provide them with the opportunity to object and intervene prior to granting the auditor access to personal information.</p> <ul style="list-style-type: none"> • Among other things, businesses that have executed the European Commission approved Standard Contractual Clauses ("SCC") are required to conduct an analysis of the laws and practices of the jurisdiction in which data has been transmitted (in this case the United States/California) to determine whether any law would allow the "disclosure of data to public authorities or authori[ze] access by such authorities" and to document that analysis (often referred to as a "transfer impact assessment"). Businesses may need to revise and amend their transfer impact assessments to account for "unannounced" audits by the CPPA and present those impact assessments to contracting parties to determine whether the CPPA's powers prevent full compliance with the SCCs. 	

Attn: Brian Soublet
August 17, 2022
Page 30

As the above table reveals, BEAR did not account for the compliance burden of more than 45 new obligations in the Proposed Regulations.

As for the three compliance obligations that BEAR considered, BEAR's estimate of the compliance burden does not, on its face, account for the business processes needed to comply with the Proposed Regulations. The following details business processes that were not accounted for in the BEAR analysis with just one of those sections:

Attn: Brian Soublet
 August 17, 2022
 Page 31

	Proposed Regulation	Obligation that would be imposed upon businesses	Comparison to existing law or regulation	BEAR's analysis of the compliance burden	Deficiencies in BEAR's analysis	Actual Compliance Burden
47.	§ 7012(e)(6)	<u>Identify the name of third parties allowed to control collection of personal information.</u> The Proposed Regulation defines, for the first time, third parties that “control the collection” of a personal information. ⁷³ The Proposed Regulation would require that if Business A allows third parties to control the collection of personal information, Business A must include the “name of all third parties” within Business A’s notice at collection.	The BEAR Report correctly identifies that the CPRA and current CCPA Regulations do not include a similar requirement.	BEAR determined that an analogous requirement is imposed by the European GDPR, and that industry estimates indicate that 16.37% of CCPA-subjected firms are also subject to the GDPR. BEAR assumed that all GDPR-subject firms were already in compliance with this provision, and thus assigned \$0 in compliance burden to those firms. For those companies that are not subject to the GDPR, BEAR estimated that it would take “approximately 1 hour of work” to “add a drop-down menu disclosing their (pre-existing list of third parties).” Their estimate was based on a number of assumptions including the assumption that “any company affected by the CCPA will use an existing employee at the firm level who is familiar with the code base opposed to a consultant.” Bear Report at 12. They also assumed that there would only be a one-time cost because “[a]lthough the list of third parties might require updating from time-to-time, this will be a simple task and is unlikely to change significantly over the course of a 12-month period.”	BEAR’s assumption that organizations subject to the GDPR are already in compliance with this obligation is speculative. While the GDPR requires that companies disclose the names of third parties that collect personal information on websites, for US companies subject to the Art. 3(2) jurisdiction of the GDPR that requirement only applies to the company’s EEA-directed websites. As a result, companies that maintain EEA-directed website and separate US-directed websites would <u>not</u> be in compliance with this obligation in connection with their US-directed websites. BEAR did not make any effort to (a) determine the percentage of GDPR-governed companies that operate jurisdiction-specific websites, or (b) investigate whether jurisdiction-specific websites in the US and the EEA allow the same third parties to collect personal information. BEAR assumed that companies have already identified a list of third parties that control the collection of information. That assumption lacks foundation. Although the CPRA and the current CCPA Regulations require companies to identify whether they are sharing information with third parties, they do <u>not</u> require companies to identify which third parties fall under the new definition of third parties that control collections, nor do they require that companies identify which third parties control the collection of personal information for each website that the company operates. BEAR assumed the use of third parties is “unlikely to change significantly over time.” That assumption also lacks foundation; BEAR did not identify the rate at which businesses modify the third parties allowed to collect personal information on a website. BEAR assumed the list of third parties mandated by the Proposed Regulation would only need to be updated once every 12 months. The Proposed Regulations do not appear to contain any such limitation.	<ul style="list-style-type: none"> • Businesses would need to audit each website that they maintain to determine which third parties are allowed to collect personal information from those websites. • Businesses would need to modify their notice at collection to identify those third parties by name. • Businesses would need to design an internal process by which the addition, or subtraction, of third parties that are allowed to collect personal information from websites triggers a process by which the notice at collection is updated for accuracy.

⁷³ Proposed Regulation § 7012(g).

Attn: Brian Soublet
 August 17, 2022
 Page 32

* * * *

The CPPA has failed to comply with administrative processes and, as a result, has raised significant concerns about government transparency and the viability of the Proposed Regulations. Specifically:

- The CPPA’s economic consultant admitted that it identified more compliance burdens than the three that it analyzed, but that it was dissuaded by unidentified staff at the CPPA from including those compliance burdens in its Report.
- The CPPA has produced no notes or transcripts from the meeting held with its economic consultant and has asserted that, if any records exist, they are exempt from disclosure based upon the attorney-client privilege (without identifying the requisite foundation for such an assertion).
- As shown in this comment, the Proposed Regulations would impose on businesses more than 45 new obligations unaccounted for by the CPPA, and that would result in significant new compliance burdens. An analysis of these 45 requirements would undoubtedly cause the Proposed Regulations to be classified as a “major regulation” under California law.
- The CPPA has disregarded the procedural requirements for promulgating a major regulation, including creating a SRIA or consulting with the DOF.

To remedy the above deficiencies the CPPA should complete a SRIA, submit it to the DOF for analysis and publication, and consider alternatives and modifications to the Proposed Regulations that would decrease the significant compliance impact of the Proposed Regulations. Only once that process has been completed should a revised Proposed Regulation be resubmitted for 45-day notice and comment. Without adhering to the APA’s processes, which are designed to give consumers, stakeholders, and government agencies alike proper notice of the impact a proposed regulation might have, the Proposed Regulations (if adopted) will be susceptible to collateral attack as invalid and unenforceable.

The CPPA had to adopt final regulations implementing the CPPA by July 1, 2022.⁷⁴ The CPPA missed that timeline by a large mark. Indeed, it didn’t even publish its notice of proposed rulemaking until after the time that the regulations were supposed to be finalized. Lost time cannot be made up by short-circuiting the administrative process designed to protect the public from legislation by regulation. If the agency continues to deprive the public of the protections of the APA, the resulting regulations will not be in the best interest of the state of California, will lead to confusion and inefficiencies for businesses, and will be ripe for judicial challenge.

⁷⁴ CAL. CIV. CODE § 1798.185(d) (West 2022).

Attn: Brian Soublet

August 17, 2022

Page 33

Sincerely,



David A. Zetony, Shareholder & Co-Chair US Privacy and Security Practice

Andrea Maciejewski, Associate

Madison Etherington, Intern

EXHIBIT A:
Response to Public Records Act Request from Amos E. Hartston
Dated July 26, 2022

From: [Amos Hartston](#)
To: [Etherington, Madison \(LC-DEN-IP-Tech\)](#)
Subject: Your Public Records Act request (2022-01522)
Date: Tuesday, July 26, 2022 3:12:33 PM
Attachments: [Response to Etherington PRA Request \(2022-01522\).pdf](#)

EXTERNAL TO GT

Dear Ms. Etherington,

Please find the attached correspondence related to your Public Records Act request.

Amos E. Hartston
Deputy Attorney General
California Department of Justice
300 S. Spring Street, Suite 1702
Los Angeles, CA 90013


CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.

ROB BONTA
Attorney General

State of California
DEPARTMENT OF JUSTICE



300 SOUTH SPRING STREET, SUITE 1702
 LOS ANGELES, CA 90013

Public: (213) 269-6000

Facsimile: (213) 897-4951

E-Mail: [REDACTED]

July 26, 2022

Madison Etherington
 [REDACTED]

Re: Your Public Records Act Request (2022-01522)

Dear Ms. Etherington:

This letter responds to your July 18, 2022 request, in which you seek various records pursuant to the Public Records Act as set forth in Government Code section 6250 *et seq.* Specifically, you requested the following records:

Any notes and transcripts related to a discussion which occurred prior to June 27, 2022, between Berkeley Economic Advising and Research (BEAR) and the California Privacy Protection Agency (CPPA) and staff regarding the economic and regulatory impacts of the California Consumer Privacy Act Regulations proposed by CPPA.

The comments to your request further clarify the discussion for which you are seeking notes or transcripts as follows:

Berkeley Economic Advising and Research (“BEAR”) state on page 1-2 in their Report, available here: https://cppa.ca.gov/regulations/pdf/std_399_attachment.pdf, that during their initial review of the Proposed Regulations they “initially believed that there could be a regulatory impact.” The Report alludes to a “discussion” with the CPPA and unidentified “supporting staff” during which the supporting staff apparently argued that “most of the potential regulatory ‘deltas’” that BEAR had identified “were reiterated [in] the existing CPRA amendments or existing regulations from the CCPA.”

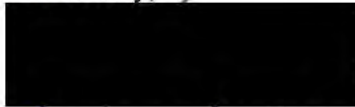
Our Office does not have the requested notes or transcripts. Further, the California Privacy Protection Agency (“CPPA”) has entered into a contract with BEAR, referenced as California Privacy Protection Agency Economic Analysis Consulting Services Contract, Agreement No. CPPA-21-96710, pursuant to which BEAR performs threshold economic analyses in support of the agency’s rulemaking efforts. Accordingly, the records you seek may be subject to exemptions from disclosure. In addition, our Office serves as legal counsel to the CPPA. To the extent our Office maintains records related to our representation of the agency, such records are exempt from disclosure. Confidentiality privileges set forth elsewhere in law, including the attorney-client privilege contained in Evidence Code section 954, are expressly

Madison Etherington
July 26, 2022
Page 2

incorporated into the Public Records Act and the public interest is served in supporting our Office's ability to provide confidential advice and counsel to the agency. (Gov. Code, §§ 6254, subd. (k), 6255.)

We hope the information we are able to provide is of assistance to you.

Sincerely,



AMOS E. HARTSTON
Deputy Attorney General

For ROB BONTA
Attorney General

EXHIBIT B:
Response to Public Records Request from CPPA
Dated August 10, 2022

From: Legal@CPPA
To: [Etherington, Madison \(LC-DEN-IP-Tech\)](#)
Subject: RE: ATTN: PRA Coordinator
Date: Wednesday, August 10, 2022 10:55:45 AM
Attachments: [image001.png](#)
[California Privacy Protection Agency DOF - 130, Major Regulations..pdf](#)
[DOF-130 2022 Major Reg \(002\).pdf](#)
[BEAR SRIA Contract.pdf](#)

EXTERNAL TO GT

The California Privacy Protection Agency (CPPA) acknowledges receipt of your August 4, 2022, request made pursuant to the California Public Records Act (Government Code Section 6250 et seq.) for copies of the following records:

1. Any notes and transcripts related to a discussion which occurred prior to June 27, 2022, between Berkeley Economic Advising and Research (BEAR) and the California Privacy Protection Agency (CPPA) and staff regarding the economic and regulatory impacts of the California Consumer Privacy Act Regulations proposed by CPPA.
2. Any documents notifying the Department of Finance of the California Privacy Protection Agency's intent to propose a major regulation and any Statement of Regulatory Impact Assessment provided by CPPA to the Department of Finance related to such major regulation.
3. A copy of the California Privacy Protection Agency Economic Analysis Consulting Services Contract, Agreement No. CPPA-21-96710.

In compliance with Government Code Section 6253, the CPPA hereby responds:

1. Any notes and transcripts related to discussions between Berkeley Economic Advising and Research and the CPPA are subject to exemptions from disclosure. The records maintained by the Agency are exempt from disclosure pursuant to the confidentiality privileges set forth in California law, including the attorney-client privilege contained in Evidence Code section 954, which are expressly incorporated into the Public Records Act and the public interest is served in supporting Agency counsel's ability to provide confidential advice and counsel to the Agency. (Government Code § 6254, subd. (k); see also Gov. Code § 6255.)
2. Attached please find:
 - A. Email dated January 28, 2022 to MajorRegulations@dof.ca.gov from Brian Soublet.
 - B. Form DF-130, 2022 California Major Regulations Calendar.
3. Attached please find a copy of Standard Agreement CPPA 21-96710.

From: [REDACTED]

Sent: Thursday, August 4, 2022 9:09 AM
To: Legal@CPPA <Legal@cpha.ca.gov>
Subject: ATTN: PRA Coordinator

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello,

Pursuant to the California Public Records Act (Government Code § 6250 et. seq.), I request that you make available for inspection and copying the following public records:

1. Any notes and transcripts related to a discussion which occurred prior to June 27, 2022, between Berkeley Economic Advising and Research (BEAR) and the California Privacy Protection Agency (CPPA) and staff regarding the economic and regulatory impacts of the California Consumer Privacy Act Regulations proposed by CPPA.
2. Any documents notifying the Department of Finance of the California Privacy Protection Agency's intent to propose a major regulation and any Statement of Regulatory Impact Assessment provided by CPPA to the Department of Finance related to such major regulation.
3. A copy of the California Privacy Protection Agency Economic Analysis Consulting Services Contract, Agreement No. CPPA-21-96710.

If you are not the custodian of records for this request, please forward this request to the appropriate person or let me know which person(s) has custody of these records. I ask that records available in electronic format be transmitted by email to [REDACTED]

Best,
Madison

Madison Etherington
Law Clerk

Greenberg Traurig, LLP
1144 15th Street, Suite 3300 | Denver, Colorado 80202

[REDACTED] | www.gtlaw.com

GT GreenbergTraurig

If you are not an intended recipient of confidential and privileged information in this email, please delete it, notify us immediately at postmaster@gtlaw.com, and do not use or disseminate the information.

From: [REDACTED]
To: MajorRegulations@dof.ca.gov
Subject: California Privacy Protection Agency DOF - 130, Major Regulations.
Date: Friday, January 28, 2022 2:48:00 PM
Attachments: [DOF-130 2022 Major Reg.pdf](#)

Attached please find the form DOF-130, identifying a potential 2022 major regulation for the California Privacy Protection Agency

Thanks,

Brian G. Soublet
Acting General Counsel
California Privacy Protection Agency.

2022 CALIFORNIA MAJOR REGULATIONS CALENDAR

DF-130 (REV12/21)

Agency Name and Responsible Agency Unit:	
Name of Proposed Regulation:	Projected Date of Notice of Proposed Action:
CCR Title and Sections Affected:	Statute(s), Propositions or Court Decision Being Implemented:
Brief summary of the proposed regulation (1 paragraph or less):	Contact Person:
	Email Address:
	Telephone Number:
	Mailing Address:

SCO ID: 1703-CPPA2196710

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT

STD 213 (Rev. 04/2020)

AGREEMENT NUMBER

CPPA 21-96710

PURCHASING AUTHORITY NUMBER (If Applicable)

1703

1. This Agreement is entered into between the Contracting Agency and the Contractor named below:

CONTRACTING AGENCY NAME

California Privacy Protection Agency

CONTRACTOR NAME

Berkeley Economic Advising and Research, LLC

2. The term of this Agreement is:

START DATE

March 21, 2022 or upon DGS/OLS approval, whichever is later

THROUGH END DATE

March 20, 2023

3. The maximum amount of this Agreement is:

\$220,720.00 - Two Hundred Twenty Thousand Seven Hundred Twenty Dollars and Zero Cents

4. The parties agree to comply with the terms and conditions of the following exhibits, which are by this reference made a part of the Agreement.

Exhibits	Title	Pages
Exhibit A	Scope of Work	4
Exhibit A, Attachment 1	Contractor Key Personnel Resumes	8
Exhibit B	Budget Detail and Payment Provisions	2
+ - Exhibit B, Attachment 1	Cost Sheet	3
+ - Exhibit C *	General Terms and Conditions	GTC 04/2017
+ - Exhibit D	Special Terms and Conditions	4

Items shown with an asterisk (*), are hereby incorporated by reference and made part of this agreement as if attached hereto.

These documents can be viewed at <https://www.dgs.ca.gov/OLS/Resources>

IN WITNESS WHEREOF, THIS AGREEMENT HAS BEEN EXECUTED BY THE PARTIES HERETO.

CONTRACTOR

CONTRACTOR NAME (if other than an individual, state whether a corporation, partnership, etc.)

Berkeley Economic Advising and Research, LLC

CONTRACTOR BUSINESS ADDRESS

1442A Walnut St., Suite 108

CITY

Berkeley

STATE

CA

ZIP

94709

PRINTED NAME OF PERSON SIGNING

David Wells Roland-Holst

TITLE

Executive Director

CONTRACTOR AUTHORIZED SIGNATURE

DATE SIGNED

03/15/2022

SCO ID: 1703-CPPA2196710

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT

STD 213 (Rev. 04/2020)

AGREEMENT NUMBER CPPA 21-96710	PURCHASING AUTHORITY NUMBER (If Applicable) 1703
--	--

STATE OF CALIFORNIA

CONTRACTING AGENCY NAME

California Privacy Protection Agency

CONTRACTING AGENCY ADDRESS

2101 Arena Blvd.

CITY

Sacramento

STATE

CA

ZIP

95834

PRINTED NAME OF PERSON SIGNING

Ashkan Soltani

TITLE

Executive Director

CONTRACTING AGENCY AUTHORIZED SIGNATURE



DATE SIGNED

03/15/2022

CALIFORNIA DEPARTMENT OF GENERAL SERVICES APPROVAL



EXEMPTION (If Applicable)

EXHIBIT A

SCOPE OF WORK

Government Code Sections 11346.3 requires state agencies proposing to adopt, amend, or repeal any administrative regulation to assess the potential for adverse economic impact on California business enterprises and individuals, avoiding the imposition of unnecessary or unreasonable regulations or reporting, recordkeeping, or compliance requirements. In November of 2020, voters approved Proposition 24, The California Privacy Rights Act of 2020 (CPRA). The CPRA cements California's place as the nation's leader in consumer privacy by amending and extending the California Consumer Privacy Act of 2018 (CCPA), the first comprehensive consumer privacy law in the United States. The new law is intended to "protect consumers' rights, including the constitutional right of privacy." The rulemaking obligation should be completed by July 1, 2022 as stipulated in statute. Before the regulations can be adopted, a series of threshold economic impact analyses must be performed, including determining whether one or more Standardized Regulatory Impact Analyses are needed to support the California Privacy Protection Agency's ("CPPA" or "the Agency" herein) rulemaking efforts. (Gov. Code Sections 11342.548, 11346.2 (b)(2)(B), and 11346.3 (c)).

1. AGREEMENT SUMMARY

- A. Based on regulatory assumptions provided by the Agency related to the provisions of the California Privacy Rights Act of 2020 ("CPRA" herein), Contractor shall conduct Economic Impact Analyses assessing the potential for adverse economic impact caused by implementing proposed regulations. If Contractor's initial analyses concludes that the regulatory assumption provided by the Agency will have an impact of more than \$50 million, contractor shall prepare the necessary Standardized Regulatory Impact Assessments (SRIA) required by Government Code Sections 11346.2 (b)(2)(B) and 11346.3 (c).
- B. Berkeley Economic Advising and Research (Contractor) shall utilize qualified and experienced economists/experts and support staff in the field of Economics, Economic policy, and the California Privacy Protection Act. A "qualified and experienced economist" is a person who has a minimum of three (3) years of experience conducting economic analysis in the state of California and is familiar with the Department of Finance and Legislative Analyst's Office Standardized Regulatory Impact Assessment (SRIA) review and approval process.
- C. The rate(s) specified in Exhibit B, Attachment 1, Cost Sheet, shall stay in effect for the entire Agreement term.

2. PROJECT REPRESENTATIVES

The project representatives during the term of this Agreement will be:

State: CPPA	Contractor: Berkely Economic Advising and Research
Name: Vongayi Chitambira	Name: David Wells Roland-Holst
Phone: [REDACTED]	Phone: [REDACTED]
Email: [REDACTED]	Email: [REDACTED]

Either party may make changes to the above contract information by giving written notice to the other. Said changes shall not require an amendment to this Agreement.

3. LOCATION

- A. The services shall be performed primarily at the Contractor's office and at the discretion and approval of the CPPA, occasional in-person meetings at CPPA's office located in Sacramento, California.
- B. Travel costs, if approved by the CPPA, will be reimbursed in accordance with the State's Department of Human Resources (CalHR).
 1. Contractor will submit a travel request prior to making travel arrangements. The request must identify the number and qualifications of people to support the travel, estimated transportation costs and number of days that will be charged. The number of support staff must be in mutual agreement and travel request preapproved by the Contract Administrator prior to finalizing travel arrangements.
 2. The Contractor will be compensated for actual incurred travel expenses based upon the per diem rates used for State employees, upon receipt and approval of an itemized invoice. Travel Reimbursement rates and applicable restrictions are identified on the Employee/Travel Reimbursement section of the California Department of Human Resources website- (<http://www.calhr.ca.gov/employees/Pages/travel-reimbursements.aspx>).
 3. Contractor must submit Contract Administrator's written approval along with itemized receipts when invoicing for reimbursement.

4. PERFORMANCE DETAILS

- A. Contractor shall conduct and submit an economic impact analysis of the California Privacy Rights Act of 2020 (CPRA) to CPPA.
- B. If the impact exceeds the \$50 million threshold, Contractor shall conduct and complete a SRIA upon completion of the economic impact analysis and submit the SRIA to CPPA.
- C. Contractor shall make available via encrypted email delivery, or secured website, computer readable copies of the Economic Assessment and SRIA.
- D. Contractor shall submit the economic analysis and SRIA to, CPPA, the Department of Finance, and the Legislative Analyst's Office.
- E. All of the Contractor's work product and information provided by and to CPPA under this contract is confidential and shall not be disclosed, except as provided in paragraph 3 D herein, without the express written permission of the CPPA.
- F. Tasks:
 1. Project Team Management – The project will begin with the establishment of the project team and development of a detailed project plan for implementation.
 - a. Contractor shall develop a process of how the Fiscal Impact

Analysis (STD 399) will be performed in consultation with the rulemaking team.

- b. Contractor shall develop a process of how the Standard Regulatory Impact Assessment (SRIA) will be performed in consultation with the rulemaking team.
- c. Contractor will identify resources required to complete the project.
- d. Deliverables from this task are:
 - i. Team member(s), key milestones and key dates identified.
 - ii. Project plan to be delivered no later than 2 weeks of project initiation and maintained for the project duration.

2. Execution of the Project Plan – The Contractor shall start on research and analysis.

- a. The Contractor shall adhere to the project plan developed under Task 1 above.
- b. Deliverables from this task are:
 - i. Progress reports detailing the status of the project to be delivered to the CPPA Contract Administrator every 2 weeks for the duration of the project.
 - ii. Fiscal Impact Analysis and, if necessary, SRIA(s) developed and submitted in relation to rulemaking proposals as developed in an iterative process by the CPPA. Each shall include Methodology, Analysis of Impacts, and Summary of Economic Results.
 - iii. Project close-out report to be delivered at project conclusion which details everything completed during the project.
 - iv. Submission of cumulative summary of economic impact analysis of the California Privacy Rights Act of 2020 (CPRA) and SRIA, if applicable, to CPPA

5. PERFORMANCE REVIEW AND ACCEPTANCE CRITERIA

- A. It shall be CPPA's sole determination as to whether the Contractor's performance has been successfully completed and is acceptable to the State.

6. LATE REPORT SUBMISSION

- A. If the Contractor exceeds the turnaround timeframe on the assessment and SRIA without CPPA approving an extension in advance, the assessment and SRIA is deemed "late." Late completion shall be assessed a penalty equal to ten percent (10%) of the assessment value per day for each day late, starting the first day after the original due date. The penalty shall be reflected on the invoice submitted to CPPA. In the event the Contractor does not include the penalty on the invoice, CPPA may dispute the invoice and subtract the penalty from the invoice.

7. LIQUIDATED DAMAGES

- A. In the event that Contractor fails to deliver in accordance with the contract requirements, the parties agree that the delay will interfere with the proper implementation of the State's programs, to the loss and damage of the State. From the nature of the case, it would be impracticable and extremely difficult to fix the


actual damages sustained in the event of any such delay. The State and Contractor, therefore, presume that in the event of any such delay the amount of damage which will be sustained from a delay will be the amounts set forth in above, and the State and the Contractor agree that in the event of any such delay, Contractor shall pay such amounts as liquidated damages and not as a penalty. Amounts due the State as liquidated damages may be deducted by the State from any money payable to the Contractor. The State shall notify Contractor in writing of any claim for liquidated damages pursuant to this paragraph on or before the date State deducts such sums from money payable to the Contractor.

EXHIBIT A, ATTACHMENT 1

CONTRACTOR KEY PERSONNEL RESUMES

Curriculum Vitae **David W. Roland-Holst**

Business Address:

207 Giannini Hall
University of California
Berkeley, CA 94720-3310


Home Address:



Fields of Specialization:

Energy Economics, Environmental Economics, Economic Forecasting, International Economics

Higher Education:

B.A.	Economics	Case Western Reserve University
B.S.	Mathematics	Case Western Reserve University
M.A.	Economics	University of California, Berkeley
Ph.D.	Economics	University of California, Berkeley

Professional Experience:

Adjunct Professor, Departments of Economics and Agricultural and Resource
Economics, UC Berkeley
June, 2003 – Present

Managing Director, Berkeley Economic Advising and Research
Berkeley, California www.bearecon.com
June, 2001 - Present

Senior Economist and Head of Program, OECD Development Centre, Paris
June 1993 – June 1995

Senior International Economist, United States International Trade Commission
August 1989 – July 1990

Occasional consultant to government agencies, World Bank, IMF,
OECD, ADB, and other public and private organizations.

Team Lead on Following Economic Analyses (Selected Projects)

1. Decommissioning of the Diablo Canyon Nuclear Power Plant California Public Utilities Commission, September 2019.
2. Standardized Regulatory Impact Assessment (SRIA): California Consumer Privacy Act, Department of Justice. 2019.
3. SRIA: Occupational Exposure to Lead Safety Standards, Department of Industrial Relations. 2019.
4. SRIA: Fall Protection Standards - Construction/Roofing, Department of Industrial Relations. 2019.
5. Economic Assessment of California's Long-term Energy Scenarios (LTES), California Energy Commission, March, 2018.
6. SRIA: Title 8, Group V Elevator Safety Orders, Department of Industrial Relations. 2017.
7. SRIA: Appliance Efficiency Standards, California Energy Commission. 2016.
8. Economic Impact Assessment for SB 350, " Report to the California ISO. December 2016.
9. Cap and Trade Structural Transition in the California Economy. Energy Foundation. 2007.

David Roland-Holst is a Professor in the Departments of Economics and Agricultural and Resource Economics and Managing Director of Berkeley Economic Advising and Research, LLC. Dr. Roland-Holst has extensive research experience in economics related to energy, environment, and international trade, authoring five books and over 100 articles and chapters in professional journals and books. Professor Roland-Holst has served in academic posts in the United States, Europe, and Asia. He has conducted research in over 40 countries, working with many public institutions in the United States and abroad. More recently, he has been a prolific contributor to policy research in California. Addressing Cap and Trade, energy efficiency, electric vehicles, low-carbon fuels, and an array of climate adaptation challenges facing the state, Roland-Holst's research has been central to the passage, design, and implementation of California's path breaking Global Warming Solutions Act. Managing Director, Berkeley Economic Advising and Research Professor Roland-Holst holds a Ph.D. in Economics from the University of California, Berkeley and is a US citizen.

Selected Research on Economic Policy

Books

10. California Climate Change: Risk and Response, with Fredrich Kahrl, University of California Press, Berkeley, 2012.
11. Health and Agriculture in Developing Countries. with David Zilberman, Joachim Otte, and Dirk Pfeiffer, Springer: New York, 2012.
12. Agriculture, Élevage et Pauvreté an Afrique de l'Ouest, (ed.) with A.A. Mbaye a and J. Otte, Editions CREA-Panafrika, Dakar, 2007.

Recent Published Articles and Chapters in Books

13. "Achieving 40 percent Greenhouse Gas Emissions Reduction by 2030 in California," S. Yeh, A. R. Eggert, C. Yang, J.B. Greenblatt, M. Wei, J.H. Williams, G. Brinkman, J. Cunningham, Energy Strategy Reviews, Forthcoming.
14. "Comparison of Low-Carbon Pathways for California," with Geoff M. Morrison, Sonia Yeh, Anthony R. Eggert, Christopher Yang, James H. Nelson, Jeffery B. Greenblatt, Raphael Isaac, Mark Z. Jacobson, Josiah Johnston, Daniel M. Kammen, Ana Mileva, Jack Moore, Max Wei, John P. Weyant, James H. Williams, Ray Williams, Christina B. Zapata, Climatic Change, 131.4 (2015): 545-557.
15. "Climate Risk and Response in the Pacific Rim," (2013), in Singh and Kohli, Oxford Economic Handbook of the Pacific Rim, Oxford Univeristy Press, New York.
16. "Past as Prologue? Understanding energy use in post-2002 China," with F. Kahrl and D. Zilberman, Energy Economics, 2013, 36:759-771.
17. "Challenge of Biofuel: Filling the Tank without Emptying the Stomach," with D. Rajagopal, S.E. Sexton, and D. Zilberman, Environmental Research Letters, 2(2007), 044004 (9pp).

SAM HEFT-NEAL

Berkeley Economic Advising & Research
 1442A Walnut Street, Suite 108
 Berkeley, California 94705

Web: bearecon.com

EMPLOYMENT

Key Expert, Berkeley Economic Advising & Research (2007 - present)
 Research Fellow, Stanford University (2015 - present)

EDUCATION

Ph.D. in Agricultural & Resource Economics, University of California, Berkeley, 2015
 B.A. in Statistics & Economics with Honors, University of California, Berkeley, 2007

ARTICLES & STUDY REPORTS

BEAR 2021. "Beyond Mitigation: Quantifying the Development Benefits of Carbon Pricing". Prepared under contract for the World Bank as part of the Partnership for Market Readiness Project.

Sam Heft-Neal, Anne Driscoll, Wei Yang, Gary Shaw, & Marshall Burke. 2021. "Associations between wildfire smoke exposure during pregnancy and risk of preterm birth in California". *Environmental Research*, 203. [paper link].

Jonas Miller, Emily Dennis, Sam Heft-Neal, Booil Jo, & Ian Gotlib. 2021. "Fine Particulate Air Pollution, Early Life Stress, and their Interactive Effects on Adolescent Structural Brain Development: A Longitudinal Tensor-Based Morphometry Study". *Cerebral Cortex*, 346. [paper link].

Marshall Burke, Anne Driscoll, Sam Heft-Neal, Jenny Xue, Jennifer Burney, & Michael Wara. 2021. "The changing risk and burden of wildfire in the US". *PNAS*, 118 (2). [paper link].

Eran Bendavid, Ties Boerma, Nadia Akseer, Ana Langer, Espoir Bwenge Malembaka, Emelda A. Okiro, Paul Wise, Sam Heft-Neal, Robert E. Black & Zulfiqar A. Bhutta. 2021. "The effects of armed conflict on the health of women and children". *The Lancet*, 397 (10273). [paper link].

Sam Heft-Neal, Jen Burney, Eran Bendavid, Kara Voss & Marshall Burke. 2020. "Dust pollution from the Sahara and African infant mortality". *Nature Sustainability*, 3 (10). [paper link].

Nathan Lo, Ribhav Gupta, David Addiss, Eran Bendavid, Sam Heft-Neal, Alexei Mikhailov, Antonio Montresor & Pamela Sabina Mbabazi. 2020. "Comparison of World Health Organization and Demographic and Health Survey data to estimate sub-national deworming coverage in pre-school children". *PLOS Neglected Tropical Diseases*, 14 (8). [paper link].

BEAR. 2020. "Clean Transportation: An Economic Assessment of More Inclusive Vehicle Electrification in California" with David Roland-Holst, Annie Yi Chen, and Liam Frolund. Prepared on behalf of Next10.

BEAR. 2019. "Oregon's Cap-and-Trade Program (HB2020): An Economic Assessment" with David Roland-Holst, Sam Evans, and Drew Behnke. Prepared under contract for the Oregon Carbon Policy Office.

Zachary Wagner, Sam Heft-Neal, Paul Wise, Robert Black, Marshall Burke, Ties Boerma, Zulfiqar Bhutta & Eran Bendavid. 2019. "Women and children living in areas of armed conflict in Africa: a geospatial analysis of mortality and orphanhood". *The Lancet Global Health*, 7(12).

Nathan Lo, Sam Heft-Neal, Jean Coulibaly, Leslie Leonard, Eran Bendavid, & David Addiss. 2019. "State of

deworming coverage and equity in low-income and middle-income countries using household health surveys: a spatiotemporal cross-sectional study". *The Lancet Global Health*, 7(11).

Corey Bradshaw, Sarah Otto, Alicia Annamalay, Sam Heft-Neal, Zach Wagner, & Peter Le Souef. 2019. "Socio-economic and environmental determinants of child health among African nations". *BMJ Open*, 9(9).

BEAR. 2018. "Exploring Economic Impacts in Long-Term California Energy Scenarios" with David Roland-Holst Sam Evans, Drew Behnke, and Lucy Shim. Prepared under contract for the California Energy Commission.

Zach Wagner, Sam Heft-Neal, Zulfiqar Bhutta, Robert Black, Marshall Burke, & Eran Bendavid. 2018. "Armed conflict and child mortality in Africa: a geospatial analysis". *The Lancet*, 392 (10150).

Sam Heft-Neal, Jennifer Burney, Eran Bendavid, & Marshall Burke. 2018. "Robust relationship between air quality and infant mortality in Africa". *Nature*, 559 (7713).

Marshall Burke, Felipe Gonzalez, Patrick Baylis, Sam Heft-Neal, Ceren Baysan, Sanjay Basu, & Solomon Hsiang. 2018. "Rising temperatures increase suicide rates in the United States and Mexico". *Nature Climate Change*, 8 (1).

Nathan Lo, Jedidiah Snyder, David Addiss, Sam Heft-Neal, Jason Andrews, & Eran Bendavid. 2018. "Deworming in pre-school age children: A global empirical analysis of health outcomes". *PLOS Neglected Tropical Diseases*, 12 (5).

Sam Heft-Neal, Marshall Burke, & David Lobell. 2017. "Using remotely sensed surface temperature to estimate climate response functions". *Environmental Research Letters*, 12 (1).

BEAR. 2016. "Senate Bill 350 Study - Volume VII: Economic Impact Analysis" with David Roland-Holst, Drew Behnke, Sam Evans, and C Springer. Prepared for California ISO in response to SB 350's legislative requirements. June, 2016.

Marshall Burke, Sam Heft-Neal, & Eran Bendavid. 2016. "Understanding variation in child mortality across Sub-Saharan Africa: A spatial analysis". *The Lancet Global Health*, 4 (12).

"Modeling Asian Regional Integration, Supply Chains, Productivity, and Income Distribution" (2014) with David Roland-Holst and Sam Evans. Working paper prepared for the Asian Development Bank.

BEAR. 2013. "Economic Assessment of Market Conditions for PHA/PHB Bioplastics Produced from Waste Methane". with David Roland-Holst, Ryan Triolo and Bijan Bayrami. Prepared under contract for the California Department of Resources Recycling and Recovery. September 30, 2013.

BOOK CHAPTERS

Early Warning Techniques for Local Climate Resilience - Smallholder Rice in Lao PDR (with David Roland-Holst and Drew Behnke) in *Climate Smart Agriculture, forthcoming*

"SMS marketing of native poultry in northern Thailand via eBird" (with David Roland-Holst, Drew Behnke, Zongyot Chaiwong, and Ryan Triolo) in *Decision Tools for Family Poultry Development*. FAO Animal Production and Health Guidelines No.16, 2014 Rome, Italy.

"Promoting Rural Livelihoods and Public Health through Poultry Contracting: Evidence from Thailand" (with D Roland-Holst and J Otte) in *Health and Animal Agriculture in Develop Countries*, edited by J. Otte, D. Roland-Holst, D. Pfeiffer, and D. Zilberman, Springer, 2011.

PAPERS AND PROJECTS IN PROGRESS

“Cost-Benefit analysis of proposed well-stimulation permit phase-out”
(with BEAR for the CA Department of Conservation).

“Exposures and behavioral responses to wildfire smoke” (with Marshall Burke, Jessica Li, Anne Driscoll, Patrick Baylis, Matthieu Stigler, Joakim Weill, Jen Burney, Jeff Wen, Marissa Childs, & Carlos Gould)

“Geographically-resolved social cost of anthropogenic emissions accounting for both direct and climate-mediated effects” (with Geeta Persad, Jen Burney, Eran Bendavid, Jon Proctor, & Marshall Burke)

“Global Biomass Fires and Infant Mortality” (with Hemant Pullabhotla, Mustafa Zahid, Vaibhav Rathi, & Marshall Burke)

“Global stunting impacts from prenatal pollution exposure: evidence from a million children” (with Martin Heger, Vaibhav Rathi, & Marshall Burke)

“Medium and long run impacts of wildfire smoke exposure on hospitalizations” (with Chris Oh, Eran Bendavid, & Marshall Burke)

FELLOWSHIPS AND AWARDS

Top 10 Clinical Research Achievement Award 2018 (*for Heft-Neal et al 2018*)

National Science Foundation Graduate Research Fellowship 2011-2014

Outstanding Teaching Award, UC Berkeley, Fall 2012

One Health Research Fellowship, University of California Global Health Institute, 2011

Drew Behnke

CONTACT INFORMATION

Web: www.bearecon.com

EDUCATION

University of California, Santa Barbara

Ph.D., Economics, 2017

M.A., Economics, 2012

University of California, Berkeley

B.A., Economics, 2008

FIELDS OF SPECIALIZATION

Applied Econometrics and Environmental Economics

EMPLOYMENT

Department of Agriculture and Resource Economics, University of California, Berkeley, *Postdoctoral Scholar*
 Berkeley, CA, 2018 - Present

Berkeley Economic Advising and Research (BEAR), *Principal*
 San Francisco, CA, 2014 - Present

- BEAR is a professional partnership dedicated to the highest quality economic analysis.

SELECTED CONSULTING EXPERIENCE

Name of Assignment or Project: Guide on the Co-Benefits of Carbon Pricing

Year: 2020 - Present

Location: California, United States

Clients: World Bank

Main Project Feature: Responsible for creating a guide to help policymakers understand and incorporate carbon pricing co-benefits into their quantitative assessments.

Position Held: Senior Economist

Activities Performed: Duties include identifying relevant co-benefits and creating a user-friendly model to be used in the guide. Responsible for producing written report and presenting findings to key stakeholders.

Name of Assignment or Project: Standardized Regulatory Impact Assessment for California Regulations

Year: 2019 - Present

Location: California, United States

Clients: California Department of Industrial Relations, California Department of Justice, California Highway Patrol

Main Project Feature: California law requires that economic impacts analysis be performed for major state regulations. BEAR works with various state agencies to conduct economic analysis of proposed regulations. Analysis includes both microeconomic impacts and impacts on the State economy.

Position Held: Senior Economist

Activities Performed: Duties include collecting and analyzing relevant data, coordinating with experts with State government, conducting economic impact analysis, and writing detailed reports of findings.

Name of Assignment or Project: Diablo Canyon Power Plant Economic Impact Assessment

Year: 2018 - 2019

Location: California, United States

Client: California Public Utilities Commission (CPUC) **Main Project Feature:** At the request of the CPUC, we undertook an economic impact study on San Luis Obispo and neighboring communities resulting from the closure in 2024 — 2025 of the Diablo Canyon Power Plant (DCPP). Economic impacts were evaluated for DCP closure, including shutdown of operations, the actions necessary to safely retire the plant and make the site eligible for alternative use, and the implementation of Senate Bill 1090, a special assistance measure to offset adjustment costs for the San Luis Obispo community.

Position Held: Senior Economist

Activities Performed: Developed Input-Output modeling strategies and scenario design. Estimated local economic and fiscal effects using input-output model. Performed econometric analysis on local housing and bond market. Attended stakeholder and client meetings. Reported and presented results.

Name of Assignment or Project: Economic Assessment of California's Long Term Energy Scenarios (LTES)

Year: 2017

Location: California, United States

Client: California Electricity Commission (CEC)

Main Project Feature: The California Energy Commission commissioned an economic analysis of California's Long-term Energy Strategy (LTES). This integrated policy framework is designed to accelerate Greenhouse Gas (GHG) emission reductions with a combination of more renewable electric power, electrification of transportation and heating, and a wide array of technology-driven energy efficiency improvements. Using a dynamic forecasting model of the California economy, BEAR conducted a detailed assessment of how these low carbon energy policies would affect incomes, employment, and health outcomes across the state. In addition, BEAR incorporate health co-benefits into our CGE model.

Position Held: Economist

Activities Performed: Prepared data inputs for model calibration. Assisted with spatial incidence analysis to identify effects on local demographic groups, with special reference to low income communities.

PUBLICATIONS

"Early Warning Techniques for Local Climate Resilience: Smallholder Rice in Lao PDR" with Sam Heft-Neal and David Roland-Holst (2017). In Leslie Lipper, Nancy McCarthy, David Zilberman, Solomon Asfaw, and Giacomo Branca (Eds.), *Climate Smart Agriculture: Building Resilience to Climate Change* (pp. 105 - 136). New York: Springer.

"Micro Contracting and the Smallholder Poultry Supply Chain in Lao PDR" with David Roland-Holst, and Joachim Otte (2012). In David Zilberman, Joachim Otte, David Roland-Holst, Dirk Pfeiffer (Eds.), *Health and Animal Agriculture in Developing Countries* (pp. 353-370). New York: Springer.

"Regional Trade Opportunities for Asian Agriculture" with Shikha Jha, David Roland-Holst, and Songsak Sriboonchitta (2010). In John Gilbert (Ed.), *New Developments in Computable General Equilibrium Analysis for Trade Policy* (pp. 272-302). London: Emerald.

Andrew Roger Lee

EDUCATION

University of California, Santa Barbara PhD Sociology	2020-present
University of California, Berkeley Master of Development Practice	2015
University of Michigan, Ann Arbor B.A. Economics and English	2011

PROFESSIONAL EXPERIENCE

- | | |
|--|---------------------|
| Berkeley Academic Advising & Research, Berkeley, CA
Project Manager | 2020-present |
| <ul style="list-style-type: none"> ❖ Provide proposal writing, editing, and organizational support in development efforts ❖ Synthesize information on complex technical topics (e.g. livestock tracing technology, phytosanitary standards, food production supply chains), translate into concise, accessible language | |
| Public Policy Institute of California, San Francisco, CA
Research Assistant II | 2017-2020 |
| <ul style="list-style-type: none"> ❖ Oversaw technical programming efforts on longitudinal study of English Learners in the California public school system ❖ Produced a variety of graphics on data procedures, research design, and outcomes for Institute projects; drafted technical appendices for external reports | |
| Acumen LLC, Burlingame, CA
and Policy Analyst II | 2015-17 |
| <ul style="list-style-type: none"> ❖ Led SAS programming and reporting efforts on a prostate cancer research project for FDA clients; managed several million observations of Medicare and National Cancer Institute data in SAS and R ❖ Served as key organizational representative on biweekly conference calls; provided technical updates on research efforts in concise, accessible language and graphics | |
| United Nations Food and Agriculture Organization, Rome, Italy
Consultant | 2015 |
| <ul style="list-style-type: none"> ❖ Established database of 'climate-smart agriculture' academic papers; extracted study design information and empirical findings for meta-analysis ❖ Wrote code in STATA summarizing longitudinal climate data affecting Vietnamese coffee industry; produced graphics for presentation to national policymakers | |

EXHIBIT B

BUDGET DETAIL AND PAYMENT PROVISIONS

1. INVOICING AND PAYMENT

- A. For services satisfactorily rendered, and upon receipt and approval of the invoices, the State agrees to compensate the Contractor in accordance with the rates specified in Exhibit B, Attachment 1, Cost Sheet.
- B. Invoices shall be submitted in arrears of the service performed. Invoices must be submitted with the Contractor's letterhead information exactly matching the Contractor name on the Standard Agreement 213 and be signed by an authorized representative.
- C. Invoices will include, as applicable:
 - 1) Contract Number
 - 2) Date of Invoice
 - 3) Date of Service
 - 4) Location of Service – Each Building to be billed separately
 - 5) Description of Service(s), applicable rate(s) and total dollar amount
 - 6) Contractor's California Certified Small Business Certification Reference Number
 - 7) Contact phone number for billing questions
- D. Contractor shall send invoices, billings and other correspondence related to Contractor's services to:

California Privacy Protection Agency
Attention: Vongayi Chitambira
2101 Arena Blvd.
Sacramento, CA 95834
Email: admin@coppa.ca.gov

Should an invoice be disputed, Contractor will correct any/all disputed items on the invoice and resubmit the invoice as indicated above. Failure to provide and resubmit corrected invoice will result in a delay of payment. Under no circumstances will a credit memo be accepted in lieu of a corrected invoice.

2. BUDGET CONTINGENCY CLAUSE

- A. It is mutually agreed that if the Budget Act of the current year and/or any subsequent years covered under this Agreement does not appropriate sufficient funds for the program, this Agreement shall be of no further force and effect. In this event, the State shall have no liability to pay any funds whatsoever to the Contractor or to furnish any other considerations under this Agreement and the Contractor shall not be obligated to perform any provisions of this Agreement.
- B. If funding for any fiscal year is reduced or deleted by the Budget Act for purposes of this program, the State shall have the option to either cancel this Agreement with no liability occurring to the State, or offer an Agreement Amendment to the Contractor to reflect the reduced amount.

- C. This contract is subject to any additional restrictions, limitations or conditions enacted by the Legislature that may affect the provisions, terms or funding of this contract in any manner.

3. PROMPT PAYMENT CLAUSE

- A. Payment will be made in accordance with, and within the time specified in, Government Code Chapter 4.5, commencing with section 927.

4. CONTRACTOR OVERPAYMENTS

- A. If the State determines that an overpayment has been made to the Contractor, the State will seek recovery immediately upon discovery of the overpayment by: (a) calling the Contractor's accounting office to request a refund of the overpayment amount, or (b) offsetting subsequent Contractor payments by the amount of the overpayment if Contractor repayment or credit is not received within thirty (30) days from the date of notice.
- B. If Contractor discovers it has received an overpayment, Contractor must notify the State and refund the overpayment immediately.

EXHIBIT B, ATTACHMENT 1

COST SHEET

1. Task 1

	(A) Name	(B) Company	(C) Classification	(D) Hourly Rate*	(E) Fringe Benefit Rate**	(F) Overhead Rate***	(G) Profit Rate****	(H) Loaded Rate (D+E+F+G)	(I) # of Hours for Task 1	(J) TOTAL COST (H x I)
1	David Roland- Holst	BEAR, LLC	Principal	\$268.80	\$76.80	\$96.00	\$38.40	\$480.00	30	\$ 14,400.00
2	Andrew Lee	BEAR, LLC	Program Manager	\$156.80	\$44.80	\$56.00	\$22.40	\$280.00	27	\$ 7,560.00
3	Samuel Heft- Neal	BEAR, LLC	Senior Economist	\$179.20	\$51.20	\$64.00	\$25.60	\$320.00	23	\$ 7,360.00
4	Drew Behnke	BEAR, LLC	Senior Economist	\$179.20	\$51.20	\$64.00	\$25.60	\$320.00	22	\$ 7,040.00
	TRAVEL COSTS*****									\$ 500.00
	MATERIALS COSTS*****									\$ No Charge
	TASK 1 COST SHEET - TOTAL									\$ 36,860.00

2. Task 2

	(A) Name	(B) Company	(C) Classification	(D) Hourly Rate*	(E) Fringe Benefit Rate**	(F) Overhead Rate***	(G) Profit Rate****	(H) Loaded Rate (D+E+F+G)	(I) # of Hours for Task 2	(J) TOTAL COST (H x I)
1	David Roland- Holst	BEAR, LLC	Principal	\$268.80	\$76.80	\$96.00	\$38.40	\$480.00	152	\$ 72,960.00
2	Andrew Lee	BEAR, LLC	Program Manager	\$156.80	\$44.80	\$56.00	\$22.40	\$280.00	136	\$ 38,080.00
3	Samuel Heft- Neal	BEAR, LLC	Senior Economist	\$179.20	\$51.20	\$64.00	\$25.60	\$320.00	116	\$ 37,120.00
4	Drew Behnke	BEAR, LLC	Senior Economist	\$179.20	\$51.20	\$64.00	\$25.60	\$320.00	110	\$ 35,200.00
TRAVEL COSTS*****										\$ 500.00
MATERIALS COSTS*****										\$ No Charge
TASK 2 COST SHEET - TOTAL										\$183,860.00

3. Total Cost

Task 1 Total	\$ 36,860.00
Task 2 Total	\$ 183,860.00
Task 1 and Task 2 Total	\$ 220,720.00

Definitions

***Direct Labor Rate:** Insert the maximum hourly or monthly labor rate (unloaded) by employee job classification/title to be billed during the approved term of the agreement. This is the highest salary or wage rate that is actually paid to the employee before the application of fringe benefits, indirect costs or profit.

****Fringe Benefit Rate:** Insert the maximum fringe benefit rate to be charged during the approved term of the agreement. Round percentages up to the nearest hundredth (two decimal places). For example, manually enter 20.26% instead of 20.2581%. Most companies will have a standard Fringe Benefit % rate, but for purposes of this contract, they should convert that to a dollar amount appropriate to this contract.

*****Overhead Rate:** The indirect cost rates on this form are caps, or the maximum amount allowed to be billed. The Contractor/Recipient/Subcontractor can only bill for actual indirect costs incurred, not to exceed the rates specified in these forms. All indirect costs charged must be reasonable, allocable to the project, and fully supported by backup documentation. DGS reserves the right to request supporting documentation of all indirect costs reimbursed or

charged as match share. Indirect costs must adhere to the Agreement Terms and Conditions, Generally Accepted Accounting Principles (GAAP) and the OMB Circular or Federal Acquisition Regulations applicable to your organization.

******Profit Rate:** Contractors and subcontractors can include up to a maximum total of 10% profit, fees or markups on their own actual allowable expenses less any expenses further subcontracted to other entities (i.e., profit, fees and markups are not allowed on subcontractor expenses). For example, if a contractor has \$100,000 in actual allowable costs but has further subcontracted \$20,000 to another entity, then the contractor can only include up to 10% profit on \$80,000 (\$100,000 minus \$20,000).

Other Direct Costs

******Travel:** Travel reimbursement will be in accordance with state reimbursement rates as approved by the California Department of Human Resources. More information about Travel Reimbursement can be located at: <http://www.calhr.ca.gov/employees/pages/travel-reimbursements.aspx>. All travel must be pre-approved in writing by the Contract Administrator prior to scheduled trip. Contractor will be compensated for actual incurred travel expenses upon receipt and approval of an itemized invoice.

*******Materials:** Appropriate materials costs will be reimbursed as pre-approved by the DGS Contract Administrator. Contractor will be compensated for actual incurred material expenses upon receipt and approval of an itemized invoice.

Cost Evaluation

Cost will be evaluated based on the cumulative total of all tasks, detailed on each of the individual task cost sheets and summarized on the Summary Cost Sheet.

The cost sheets and rates identified will be used for the resulting contract and shall be binding for the term of the agreement.

EXHIBIT D

SPECIAL TERMS AND CONDITIONS

1. STANDARD CONDITIONS OF SERVICE

- A. Contractor will abide by all State and Federal laws in performance of this contract.
- B. The Contractor shall maintain all license(s) required by law for accomplishing any work required with this agreement. In the event any license(s) expire at any time during the term of this agreement, Contractor agrees to provide to the State a copy of the renewed license(s) within thirty (30) days following the expiration date. In the event the Contractor fails to keep in effect at all times all required license(s), the State may, in addition to any other remedies it may have, terminate this agreement upon occurrence of such event.
- C. The Contractor certifies that it has appropriate systems and controls in place to ensure that State funds will not be used in the performance of this Contract for the acquisition, operation or maintenance of computer software in violation of copyright laws.
- D. If signing this contract as a sole proprietor, Contractor certifies that it is not an alien that is ineligible for state and local benefits, as defined in Subtitle B of the Personal Responsibility and Work Opportunity Act (8 U.S.C. § 1601 et seq.).
- E. Pursuant to Public Contract Code section 10295.4, persons or companies identified as the largest tax delinquents by the Franchise Tax Board (FTB) or the California Department of Tax and Fee Administration (CDTFA) are ineligible to enter into any contract with the state for non-IT goods or services. Any contract entered into in violation of section 10295.4 is void and unenforceable.
- F. If contract activities include collection of organic waste, the Contractor must be aware and adhere to Public Resources Code § 42649.1 et. seq. concerning organic waste recycling requirements. Organic waste includes; food waste, green waste, landscape and pruning waste, nonhazardous wood waste, and food-soiled paper waste that is mixed in with food waste.

2. **EXCISE TAX:** The State of California is exempt from Federal Excise Taxes, and no payment will be made for any taxes levied on employees' wages. The State will pay for any applicable State of California or local sales or use taxes on the services rendered or equipment or parts supplied pursuant to this agreement. California may pay any applicable sales or use tax imposed by another state.

3. RIGHT TO TERMINATE

- A. The State reserves the right to cancel all or a portion of the service for any reason, subject to thirty (30) days written notice to the Contractor.
- B. This agreement can be immediately terminated for cause. The term "for cause" means that the Contractor fails to meet the terms, conditions, and/or responsibilities of the contract. In this instance, the contract termination shall be effective as of the date indicated on the State's notification to the Contractor.

4. RESOLUTION OF CONTRACT DISPUTES

- A. In the event of a dispute, Contractor will attempt resolution with the CPPA Contract Administrator with a written explanation of the situation. If no resolution is found,

Contractor shall file a "Notice of Dispute" with the CPPA within ten (10) days of the failed resolution at the following address:

California Privacy Protection Agency
 Attn: CPPA Executive Director
 2101 Arena Boulevard
 Sacramento, CA 95834

- B. CPPA Executive Director or designee shall meet with the Contractor for purposes of resolving the dispute. The decision of the CPPA Executive Director or the designee shall be final. In the event of a dispute, the language contained within this agreement and its attendant Exhibits shall prevail over any other language.
- C. Neither the pendency of a dispute nor its consideration by the CPPA Executive Director will excuse the Contractor from full and timely performance in accordance with the terms of the Agreement.

5. HEALTH and SAFETY PROVISIONS

- A. Contractor and all subcontractors shall abide by all health and safety mandates issued by federal, state, and local governments and/or public health officers as well as those issued by DGS, and worksite specific mandates. If multiple mandates exist, the Contractor and subcontractors shall abide by the most restrictive mandate. The term "employee", "worker", "state worker" or "state employee" in health and safety mandates includes contractor and subcontractor personnel.
- B. Costs associated with adhering to health and safety mandates are the responsibility of the Contractor. Contractor is responsible for the tracking and compliance of health and safety mandates and may be audited upon request.

6. POTENTIAL SUBCONTRACTORS

- A. Nothing contained in this Agreement or otherwise, shall create any contractual relationship between FMD and any subcontractors, and no subcontract shall relieve the Contractor of its responsibilities and obligations hereunder. The Contractor agrees to be as fully responsible to FMD for the acts and omissions of its subcontractors and of persons either directly or indirectly employed by the Contractor. The Contractor's obligation to pay its subcontractors is an independent obligation from FMD's obligation to make payments to the Contractor. As a result, FMD shall have no obligation to pay or to enforce the payment of any monies to any subcontractor.

7. INSURANCE REQUIREMENT

- A. General Provisions Applying to All Policies
 - 1) Coverage Term – Coverage needs to be in force for the complete term of the contract. If insurance expires during the term of the contract, a new certificate must be received by the State at least thirty (30) days prior to the expiration of this insurance. Any new insurance must still comply to the original terms of the contract.
 - 2) Policy Cancellation or Termination & Notice of Non-Renewal – Contractor is responsible to notify the State within 5 business days of any cancellation, non-renewal or material change that affects required insurance coverage. In the event

- Contractor fails to keep in effect at all times the specified insurance coverage, the State may, in addition to any other remedies it may have, terminate this Contract upon the occurrence of such event, subject to the provisions of this Contract.
- 3) Deductible – Contractor is responsible for any deductible or self-insured retention contained within their insurance program.
 - 4) Primary Clause – Any required insurance contained in this contract shall be primary, and not excess or contributory, to any other insurance carried by the State.
 - 5) Insurance Carrier Required Rating – All insurance companies must carry a rating acceptable to the Office of Risk and Insurance Management. If the Contractor is self insured for a portion or all of its insurance, review of financial information including a letter of credit may be required.
 - 6) Endorsements – Any required endorsements requested by the State must be physically attached to all requested certificates of insurance and not substituted by referring to such coverage on the certificate of insurance.
 - 7) Inadequate Insurance – Inadequate or lack of insurance does not negate the contractor's obligations under the contract.
- B. Commercial General Liability – Contractor and any subcontractors shall maintain general liability on an occurrence form with limits not less than \$1,000,000 per occurrence for bodily injury and property damage liability combined. If Commercial General Liability insurance or other form with a general aggregate limit is used, either the general aggregate limits shall apply separately to this project/location or the general aggregate limit shall be twice the required occurrence limit. If the aggregate applies "per project/location" it shall so state on the certificate. The policy shall include coverage for liabilities arising out of premises, operations, independent contractors, products, completed operations, personal & advertising injury, and liability assumed under an insured contract. This insurance shall apply separately to each insured against whom claim is made or suit is brought subject to the Contractor's limit of liability. **The policy must be endorsed to include the State of California, its officers, agents and employees as additional insured, but only with respect to work performed under the contract. The additional insured endorsement shall be provided with the certificate of insurance.**
- C. Automobile Liability – Contractor shall maintain motor vehicle liability with limits not less than \$1,000,000 combined single limit per accident. Such insurance shall cover liability arising out of a motor vehicle including owned, hired and non-owned motor vehicles. **The policy must be endorsed to include the State of California, its officers, agents and employees as additional insured, but only with respect to work performed under the contract. The additional insured endorsement shall be provided with the certificate of insurance.**
- D. Workers Compensation and Employers Liability – Contractor shall maintain statutory worker's compensation and employer's liability coverage for all its employees who will be engaged in the performance of the Contract. Employer's liability limits of \$1,000,000 are required. **The Workers' Compensation policy shall be endorsed with a waiver of subrogation in favor of the State.**
- E. Errors and Omissions/Professional Liability – Contractor shall maintain Errors and Omissions/Profession liability with limits of not less than \$1,000,000 each incident and \$2,000,000 aggregate covering damages caused by negligent, acts or omissions. The

policy retro date must be shown on a certificate of insurance and must be before the date contract work begins.

- F. Certificate of Insurance - The Contractor shall furnish a Certificate of Insurance. The Certificate of Insurance will provide the above listed liability coverages and the Certificate Holder shall read:

Attn: CSS – 21-96710
Department of General Services
Office of Business and Acquisition Services
707 Third Street, MS 508
West Sacramento, CA 95605

8. **EVALUATION**: Contractor will be evaluated based on the Contractor's performance, which includes, but is not limited to, work product, adherence to timelines and deadlines, staffing, timely processing of contract task orders, accepting of work, and the level of success in meeting all other contractual agreements.
9. **NEWS RELEASES**: News releases pertaining to award of or work performed as a result of contract may not be made without prior written approval of:

The Public Information Officer
707 Third Street, MS 101
West Sacramento, CA 95605
Phone: (916) 376-5037
Email: DGSPublicAffairs@dgs.ca.gov

From: **Khara Boender** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CCIA - CPPA Public Comment
Date: 18.08.2022 13:45:31 (+02:00)
Attachments: 2022-8-18_CCIA Comments to Cal. Priv. Prot. Agency on Draft Regulations.pdf (19 pages), 2022-8-18_CCIA Comments to Cal. Priv. Prot. Agency on Draft Regulations.pdf (19 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good morning,

On behalf of the Computer & Communications Industry Association (CCIA), I am pleased to provide input on the California Privacy Protection Agency's (CPPA) proposed rulemaking under the California Consumer Privacy Act (CCPA). CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms. For 50 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.

CCIA has long supported the evolution of privacy policy to keep pace with evolving technologies. We appreciate that state lawmakers have a continued interest in adopting regulations that will guide businesses and protect consumers. The proposed regulations are an impressively comprehensive set of protections and are, by far, the most developed guidelines in the nation. In the attached document, CCIA provides comments regarding several provisions in the proposed regulations.

Thank you for the opportunity to comment on the CPPA's rulemaking activities. Please do not hesitate to contact me at [REDACTED] if you would like any further information regarding these comments and recommendations.

Sincerely,

Khara Boender

--

Khara Boender
State Policy Director
Computer & Communications Industry Association (CCIA)

[REDACTED]
[@CCIANet](https://twitter.com/CCIANet)

www.ccianet.org



Computer & Communications
Industry Association
Tech Advocacy Since 1972



August 18, 2022

Via Electronic Mail (regulations@cpha.ca.gov)

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

Re: CPPA Public Comment

The Computer & Communications Industry Association (“CCIA”)¹ is pleased to respond to the California Privacy Protection Agency (the “Agency” or “CPPA”) [Notice of Proposed Rulemaking](#) on the Proposed Regulations (the “Regulations”) that will implement the California Privacy Rights Act of 2020 (the “CPRA”).

INTRODUCTION

CCIA has long supported the evolution of privacy policy to keep pace with evolving technologies. We appreciate that state lawmakers have a continued interest in adopting regulations that will guide businesses and protect consumers. The Regulations are an impressively comprehensive set of protections and are, by far, the most developed guidelines in the nation.

These comments focus on a few provisions in the Regulations that warrant revision. The aim of these suggestions is manyfold. First, to ensure that the Regulations are reflective of the mandates stated in the CPRA. Secondly, that the Regulations are

¹ CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms. For 50 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. A list of CCIA members is available at <https://www.cciagnet.org/members>.

feasible to implement in a timely and clear manner. Third, that the Regulations allow flexibility in order not to not inhibit innovation. Finally, to prevent any unintended retroactive application of this new set of rules.

CCIA's suggested amendments to the Regulations are set forth in **Attachment**

A.

I. CONSENT AND OPT-OUT

A. Opt-Out Preference Signals – § 7025(b)

By requiring that businesses recognize global opt-out preference signals, the draft Regulations go beyond, and actually contradict, what is stated in the CPRA. Section 1798.135 of the statute makes clear that businesses may choose to either (i) provide links for consumers to opt-out of “selling,” “sharing,” or certain uses and disclosures of sensitive personal information; or (ii) recognize universal opt-out preference signals. The draft Regulations, by contrast, reject this approach and instead require businesses to honor global opt-out preference signals. Section 7025(b) of the draft rules should be revised to treat recognition of global opt-out preference signals as voluntary in line with the statute. See Attachment A.

In addition, CCIA suggests that the regulations should permit consumers to both turn on and turn off the opt-out mechanism discussed in § 7025(b). The opt-out mechanism should also harmonize treatment of that signal with the confirmatory display discussed in § 7026(f)(4).

These provisions would make the signal more user friendly, which is a stated goal of these Regulations as indicated in § 7025(a). They would also be consistent with treatment of cookie settings (which encompasses signals such as this) under the General Data Protection Regulation (GDPR) and Europe's ePrivacy Directive, which

provide clarity that: (1) a business's website should feature a consent banner that allows visitors to either give or refuse consent to the non-necessary cookies that process personal information;² and (2) methods for offering a right to refuse or requesting consent should be made as user-friendly as possible, and settings should remain available for users to revisit and adjust, as they prefer.³ Consistent treatment of signals and settings assists businesses with compliance by creating a unified, global approach.

B. Appropriate Notice to Obtain Opt-Out – § 7013(e)(3)

Section 7013(e)(3) requires a business to provide a notice to opt out of data sale and data sharing in the same manner in which the business collects the personal information. The Initial Statement of Reasons (ISOR) indicates that the Agency crafted this requirement to address new ways in which businesses are collecting personal information and to ensure that the notice is effective.⁴ CCIA is concerned, however, that § 7013(e)(3) exceeds the mandate of the CPRA. We suggest that this rule be more consistent with what is becoming the national approach.

The stated provisions go beyond the CPRA requirements and similar state omnibus laws. That is, Section 1798.130(a)(5) of the CPRA requires only that the business disclose the consumer's right in its online privacy policy or on the internet webpage. A business that collects personal information outside a website should be able to satisfy its obligation by directing the consumer to its website. For instance, §

² See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Council Directive 95/46/EC (General Data Protection Regulation), 26 O.J. (L 119), <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

³ See OFFICIAL JOURNAL OF THE EUROPEAN UNION, DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 25 NOVEMBER 2009, SECTION 20(a).

⁴ See Cal. Privacy Protection Agency, *Initial Statement of Reasons* (Jun. 6, 2022) [hereinafter *ISOR*], https://cppa.ca.gov/meetings/materials/20220608_item3_isr.pdf.

7013(e)(3)(A) explains that a brick-and-mortar store can post signage directing consumers to an online notice. This is less burdensome than the example in § 7013(e)(3)(B), which would require a business collecting personal information over the phone to “orally” walk through the notice. The same issue arises for connected devices in § 7013(e)(3)(C). In these settings, the business should have the option of “orally” directing the consumer to the website notice, as permitted for physical stores.

By way of comparison, the Virginia Consumer Data Protection Act (VCDPA) and Colorado Privacy Act (CPA) only require businesses to present opt-out methods clearly and conspicuously in privacy notices and in readily accessible locations outside of privacy notices.⁵ These opt-outs are not required to be presented in the same manner of data collection.⁶

If it expands notice obligations by requiring businesses to offer opt-out in the same manner as it discloses how data is collected, the Agency would impose significant burdens on businesses that maintain a website but collect personal information by other means. Adopting the approach taken in other state privacy laws, by contrast, will be beneficial to businesses and to consumers as there is a clearer path forward regarding how best to provide and act upon consumer rights. Moreover, this result would be more consistent with § 1798.130(a)(5) of the CPRA, which requires only that the business disclose the consumer’s rights via online privacy policy or internet webpage.

C. Opt-Out Consent for Pre-Data Collection – § 7013(h)

As written, the Regulations do not provide language specifying when the

⁵ See [VA. CONSUMER DATA PROT. ACT](#), H 2307, 2021 SPECIAL SESSION, § 59.1-574(c) (2022); see also [COL. PRIVACY ACT](#), SB 21-190, 2021 REG. SESS., § 6-1-1306 (1)(a)(III) (2022).

⁶ See *id.*

requirement to obtain opt-out consent for pre-data collection applies. CCIA suggests reworking § 7013(h) to ensure that businesses and consumers understand that the requirement will apply to data collected after the notice requirement goes into effect.

More specifically, CCIA suggests that the Agency clarify § 7013(h) to require affirmative consent to sell/share information collected *prior* to the opt-out notice, but limiting it to information collected *after* the notice requirement goes into effect. These temporal specifications will align the Regulations privacy laws in other states, which do not prevent businesses from engaging in targeted advertising based on information already collected.

D. Notifying Third Parties of a Consumer’s Opt-Out – §§ 7026(f)(2) and (3)

The requirement to notify third parties of a consumer’s opt-out status should apply on a going-forward basis only; it should not require a company to go back to previous transactions by passing the opt-out request to all downstream partners. In any case, the notification requirement should (1) be limited only to the third parties to whom the business has sold or shared the customer’s personal information, as opposed to § 7026(f)(3)’s requirement to notify all third parties with whom the business makes personal information available; and (2) include the disproportionate effort standard, to prevent a business from expending unnecessary time and resources with little benefit to consumers. Indeed, while the GDPR does require notice to third parties when a consumer exercises their rights, it does not require such notice if it would require the business to expend disproportionate effort.⁷

E. Confirmation of Consumer Opt-Outs – § 7026(f)(4)

⁷ See General Data Protection Regulation, *supra* note 2, art. 19, (“Notification Obligation Regarding Rectification or Erasure of Personal Data or Restriction of Processing”).

The Regulations would require a business that sells or shares personal information to provide a means by which a customer can confirm that the business has processed their opt-out request. This new requirement appears to extend beyond the statutory requirements in the CPRA. See Cal. Civ. Code § 1798.120(a) & (b). Although it discusses opt-out options and mentions forthcoming regulations that will “define the requirements and technical specifications for” opt-out options, the CPRA makes no mention of the requirement to confirm processing of opt-out requests. Further, this requirement does not appear in the CDPA, CPA, Connecticut Act Concerning Personal Data Privacy and Online Monitoring (CTDPA), the Utah Consumer Privacy Act (UCPA), or VCDPA. Such a regulation, namely, one that travels well beyond its statutory basis and other state privacy laws is a slippery slope CCIA strongly advises against.

In addition to being overly broad, the requirement to confirm the processing of opt-out requests is unnecessary. The CPRA already includes enforcement provisions that motivate businesses to honor and process consumer requests. Imposing a further obligation to confirm opt-outs seems like overkill. We note that the ISOR discloses that the Agency considered the alternative of requiring businesses to confirm receipt of opt-out requests, but determined that such a requirement was “too prescriptive.”⁸ Requiring opt-out confirmation would be equally prescriptive. CCIA respectfully suggests that the Agency eschew both forms of additive obligation.

The most important aspect of the Regulations is the goal of ensuring a supportive user experience. With regard to opt-out, if businesses are required to display preference, they should have the option of showing preference on their website or within

⁸ ISOR, *supra* note 4, at 42.

privacy settings so that the consumer’s experience is not cluttered. Enabling this type of choice furthers the Agency’s desire to use a “performance-based standard that gives flexibility to the business regarding how to display the status of the consumer’s request,” as stated in the ISOR.⁹

II. THIRD-PARTY SERVICE PROVIDERS AND CONTRACTORS

A. The Proposed Rules Improperly Default to Converting Third Parties Into Primary Actors – § 7051(c)

Section 7051, as written, improperly converts service provider/contractor relationships into third party relationships, which imposes a host of additional legal obligations set forth in § 7052 if the contract is deemed not fully compliant with the Regulations. This language creates a double penalty whereas failure to have an appropriate contract and comply with the law holds penalty enough. This layering of additional legal exposure seems both unnecessary — the business would already have violated the contract regulations — and punitive. In addition, the triggered third-party classification would not reflect the actual relationship between the business and the external party, which might be engaged in an otherwise permitted business purpose that is neither selling nor sharing.

No other U.S. State’s law creates this kind of regulatory layering. Under the GDPR, a processor is responsible for its own violation of the law. For these reasons, CCIA suggests that § 7051(c) be deleted.

B. The Rules Should Include Liability Exemptions for Violations Committed by Service Providers and Contractors – §§ 7051(e) and 7053(e)

Section 1798.145 of the CPRA includes an exemption that exculpates

⁹ ISOR, *supra* note 4, at 46.

businesses from service provider and contractor non-compliance where appropriate due diligence has been conducted. As the Agency works to promulgate regulations on when this section applies, CCIA encourages it to provide added clarity by listing factors that affirmatively indicate a violation, as opposed to leaving businesses to formulate a reasonable belief that the external party is in violation. We suggest updating §§ 7051(e) and 7053(e) in order to incorporate specific factors to be considered.

By listing affirmative factors, the Regulations will not place additional burdens on businesses to confirm the absence of violations. Rather, businesses will be equipped with guidance on how to best conduct due diligence, which is similar to the guidance provided to data exporters in the European Commission's Standard Contractual Clauses (SCCs). Just as the SCCs offer guidance to data exporters by instructing them that they may, "take into account relevant certifications held by the data importer" when deciding on a review or audit, the Regulations can and should also offer more clarity to businesses in this section.¹⁰

C. The Rules Should Not Contain Overly Prescriptive Requirements for Contracts with Third Parties

The Regulations as they pertain to contracts, and specifically the provisions related to use of consumer data, third party data collection, and deadlines for providing notice of inability to comply, warrant some revision in order not to create onerous or duplicative compliance burdens that will not substantially increase privacy protections.

1. Use of Consumer Data – § 7051(a)(3)

¹⁰ EUROPEAN COMMISSION, ANNEX TO THE COMMISSION IMPLEMENTING DECISION ON STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES PURSUANT TO REGULATION (EU) 2016/679, Module 2 (8.9)(c), Transfer Controller to Processor: Documentation and Compliance, <https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors>, .

Section 7051(a)(3)'s requirement that contract provisions include a prohibition against using information for other purposes *in addition to* the purposes of processing seems overly prescriptive. Neither the GDPR (through SCCs) nor other state laws require contracts to include such a prohibition. Instead, they primarily require contracts with third parties to include language regarding the nature of processing, parameters around purpose, and duration; clear instructions for processing data; and both parties' rights and obligations under the agreement.¹¹ These laws also place confidentiality, deletion, compliance, and assessment/audit requirements on the respective parties, although these are not required to be listed in the contracts. None of these laws require contracts to include a prohibition against using information for other purposes.

2. Third-Party Data Collection – § 7012(g)(3)

Similarly, the third-party data collection requirement in § 7012(g)(3) also seems too prescriptive. The Regulations should permit notice that is “reasonable” in the context of the method of data collection. For instance, if a store or restaurant employs a third-party voice assistant device that does not contain a physical display, then a notice directing the consumer to the third-party device's website should be sufficient.

The Federal Trade Commission (FTC) has already provided guidance for providing appropriate disclosures in various contexts through its *Dot Com Disclosures*, which make clear that ensuring clear disclosure of appropriate terms based on text and available means is the more important standard upon which to rely.¹² For instance, the

¹¹ See [VA. CONSUMER DATA PROT. ACT](#), *supra* note 5, § 59.1-575 (2022); see also [COL. PRIVACY ACT](#), *supra* note 5, § 6-1-1305 (2022); [UT. CONSUMER PRIVACY ACT](#), S.B. 227, 2022 Gen. Sess., § 13-61-301 (2022).

¹² See FTC, DOT COM DISCLOSURES: Information About Online Advertising (May 2000), <https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-issues-guidelines-internet-advertising/0005dotcomstaffreport.pdf>.

FTC makes clear that using email instead of direct mail may be appropriate as long as a website operator discloses the manner in which it will provide information and provides it in a form that consumers can retain.¹³ The FTC demonstrates an understanding of the need for flexibility and adaptability in creating a meaningful user experience. The Regulations should adopt the flexibility allowed by the FTC by permitting said third parties to provide notice in a reasonable manner. Updating § 7012(g)(3) accordingly will help to permit businesses to better engage with service providers and still allow meaningful disclosures to consumers.

D. The Deadline for Third Parties to Provide Notice of Inability Should Be Increased to Ten Business Days – § 7051(a)(8)

Section 7051(a)(8) imposes a very short period—five business days—for a service provider or contractor to notify a business it can no longer meet its obligations. According to the ISOR, the slim five-day window is “necessary so that the business can take prompt action” and will help businesses “protect consumer personal information from unauthorized use.”¹⁴ The ISOR also states that this is a reasonable and feasible maximum timeframe for service providers to provide notice.¹⁵

Though prompt action is important, the time period is overly burdensome. For this reason, a 10-business day window would be more appropriate and more like the Agency’s past rulemaking efforts. When enacting California Consumer Privacy Act regulations, the Agency implemented a 10-business day window for businesses to acknowledge receipt of data subject access requests (DSAR).¹⁶ Other entities provide

¹³ *See id.*

¹⁴ ISOR *supra* note 4, at 51.

¹⁵ *Id.*

¹⁶ [CAL. CONSUMER PRIVACY ACT REGULATIONS](#), § 11 CCR 7021(a) (2022).

even longer notice periods, as seen with the GDPR’s requirement that controllers handle DSAR requests without undue delay and “in any event within one month of receipt of the request.”¹⁷

III. CONSUMER RIGHTS

A. Collection and Use of Consumer Data – § 7002(a)

The CPRA restricts the collection and use of personal information to what is “reasonably necessary and proportionate.” Cal. Civ. Code § 1798.100(c). Section 7002(a) of the draft Regulations would implement that standard to mean “what an average consumer would expect when the personal information was collected.” This interpretation somewhat alters the CPRA standard in a manner that will make implementation quite difficult.

Inserting an “average consumer” gloss on the CPRA restriction for data usage creates a mutable and subjective standard. As the mind of the “average consumer” is difficult to accurately ascertain, and consumers, businesses, and regulators may differ on what an average consumer expects, a focus on the purpose provides more clarity for businesses seeking to comply with the Regulations.

CCIA notes that the GDPR contains the same restriction as the CPRA – data usage must be limited to what is necessary in relation to the purposes for which they are processed – without adoption of an additional “average consumer” standard.¹⁸

B. Data Minimization – § 7002(b)(1)

The illustrative examples of data minimization practices in § 7002(b) are quite

¹⁷ See General Data Protection Regulation, *supra* note 2, art. 12, (“Transparent Information, Communication, and Modalities for the Exercise of the Rights of the Data Subject”).

¹⁸ See *id.* art. 5(c), (“Principles Relating to Processing of Personal Data”).

narrow. CCIA is concerned that this list will restrict innovation. For instance, the Regulations assume that the primary function of a service should be the exclusive function, an assumption more narrow than the GDPR's data minimization provision, which allows businesses to process personal information in ways that are adequate and relevant to what is necessary in relation to the purposes for which it is processed.¹⁹ In illustrative example § 7002(b)(1), a mobile flashlight application should only provide flashlight services and not offer ancillary benefits that might rely on collected data such as identifying restaurants that are too dimly lit or public areas with insufficient street lighting. In fact, these additional features benefit the consumer. To that end, it would also be helpful for the Regulations to include an example where the use of data to improve and build net new features are not incompatible with the original purpose.

C. Correction Requests – § 7023(c)

With regard to consumer requests for correction, a “disproportionate effort” standard should apply. With the potential that tens of billions of requests will start coming in, the Agency should adopt some kind of material delimiter to this obligation.

Relieving businesses from exerting disproportionate effort in meeting correction requests would comport with other state privacy laws. The CDPA, CPA, and CTDPA allow businesses an exemption from fulfilling requests for correction where it would be unreasonably burdensome for the controller to associate the request with the personal information.²⁰

This same type of delimiter should apply to the obligation in § 7022(c)(4) to notify

¹⁹ See *id.*

²⁰ See [VA. CONSUMER DATA PROT. ACT](#), *supra* note 5, § 59.1-577 (2022); see also [COL. PRIVACY ACT](#), *supra* note 5, § 6-1-1307 (2022); [CT. ACT CONCERNING PERSONAL DATA PRIVACY AND ONLINE MONITORING](#), PA 22-15, 2022 Gen. Assemb., § 9(c) (2022).

third parties when a deletion is made. CCIA suggests that the rule be modified to require “reasonable efforts” to notify third parties.

IV. DARK PATTERNS

When designing consumer requests and obtaining consent, businesses should be required to ensure that the language is easy to understand, that there is no manipulative or confusing language, that there is symmetry in choice, and that the methods present “easy-to-execute” options. The Regulations appropriately state that non-compliant design methods may be considered dark patterns that do not result in valid consent. But the broad “symmetry in choice” standard in § 7004(a)(2) should be honed somewhat.

CCIA suggests that the Agency adopt the FTC’s approach to dark patterns, which focuses on eliminating practices that are harmful rather than prescribing specific design practices that will limit innovation and creativity in design. Specifically, the FTC’s enforcement policy statement forbids businesses from engaging in processes that fail “to provide clear, up-front information, obtain consumers’ informed consent, and make cancellation easy.”²¹ The FTC does not, however, impose a requirement akin to §7004(a)(2) (“The path for a consumer to exercise a more privacy-protective option shall not be longer more burdensome than the path to exercise a less privacy-protective option”). Rather than prohibiting longer privacy-protective options, § 7004(a)(2) should adjust the requirement that *more burdensome* privacy-protective options are prohibited, rather than simply prohibiting *longer* privacy-protective options.

²¹ Juliana Gruenwald Henderson, *FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions*, Federal Trade Commission (Oct. 28, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions>

CONCLUSION

CCIA and its members thank the Agency for this opportunity to provide suggestions on how to perfect the Regulations in ways that protect consumer data, are feasible to implement, and retain flexibility for customization and innovation. The suggested alternative language discussed herein, which is also provided in Attachment A in redline form for ease of review, is offered as a means for achieving the best result for consumers, regulators, and the online ecosystem.

Respectfully submitted,

Stephanie A. Joyce
Chief of Staff and Senior Vice President
Khara Boender
State Policy Director
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, DC 20001

[REDACTED]

August 18, 2022

ATTACHMENT A

Suggested Amendments to Proposed Rules

§ 7002(a): A business's collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purpose(s) for which the personal information was collected or processed. ~~To be reasonably necessary and proportionate, the business's collection, use, retention, and/or sharing must be consistent with what an average consumer would expect when the personal information was collected.~~ A business's collection, use, retention, and/or sharing of a consumer's personal information may also be for other disclosed purpose(s) if they are compatible with ~~what is reasonably expected by the average consumer~~ the context in which the personal information was collected. A business shall obtain the consumer's explicit consent in accordance with section 7004 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.

§ 7002(b)(1): Business A provides a mobile flashlight application. Depending on the circumstances, Business A should not collect, or allow another business to collect, consumer geolocation information through its mobile flashlight application without the consumer's explicit consent because the collection of geolocation information is incompatible with the context in which the personal information is collected, i.e., provision of flashlight services. The collection of geolocation data ~~may is not be within the reasonable expectations of an average consumer, nor is it~~ may is not be within the reasonable expectations of an average consumer, nor is it reasonably necessary and proportionate to achieve the purpose of providing, improving, or adding features to a flashlight function.

§ 7004(a)(2): Symmetry in choice. The path for a consumer to exercise a more privacy-protective option shall not be ~~longer~~ more burdensome than the path to exercise a less privacy-protective option. Illustrative examples follow.

§ 7004(a)(4): Avoid manipulative language or choice architecture. The methods should not use language or wording that ~~guilts or shames~~ threatens or misleads the consumer into making a particular choice ~~or bundles consent~~ so as to subvert the consumer's choice. Illustrative examples follow.

...

(B) Requiring the consumer to click through false or misleading reasons why submitting a request to opt-out of sale/sharing is ~~allegedly~~ a bad choice before being able to execute their choice to opt-out is manipulative ~~and shaming~~.

(C) It is manipulative to bundle choices so that the consumer is only offered the option to consent to using personal information for reasonably expected purposes

together with purposes that are incompatible to the context in which the personal information was collected. For example, a business that provides a location-based service, such as a mobile application that posts gas prices within the consumer's location, shall not require the consumer to consent to incompatible uses (e.g., sale of the consumer's geolocation to data brokers) together with the expected use of providing the location-based services, which does not require consent. This type of choice architecture is manipulative because the consumer is forced to consent to incompatible uses in order to obtain the expected service. The business should provide the consumer a separate option to consent to the business's use of personal information for unexpected or incompatible uses.

§ 7012(g)(3): A business that, acting as a third party, controls the collection of personal information on another business's premises, such as in a retail store or in a vehicle, shall also provide a notice at collection in a conspicuous manner, [which takes into account the method of the data collection](#), at the physical location(s) where it is collecting the personal information.

§ 7013(e)(3)(B): A business that sells or shares personal information that it collects over the phone ~~may~~ **shall** provide notice orally during the call when the information is collected.

§ 7013(e)(3)(C): A business that sells or shares personal information that it collects through a connected device (e.g., smart television or smart watch) shall provide notice in a manner that ensures that the consumer will encounter the notice [or direct the consumer to where the notice can be found online](#) while using the device.

§ 7013(h): A business shall not sell or share the personal information it collected [after the effective date and](#) during the time the business did not have a notice of right to opt-out of sale/sharing posted unless it obtains the consent of the consumer.

§ 7022(c)(4): Notifying any other service providers, contractors, or third parties that may have accessed personal information from or through the service provider or contractor, unless the information was accessed at the direction of the business, to delete the consumer's personal information unless this proves impossible or involves disproportionate effort. ~~If the service provider or contractor claims that such a notification is impossible or would involve disproportionate effort, the service provider or contractor shall provide the business a detailed explanation that shall be relayed to the consumer that includes enough facts to give a consumer a meaningful understanding as to why the notification was not possible or involved disproportionate effort. The service provider or contractor shall not simply state that notifying those service providers, contractors, and/or third parties is impossible or would require disproportionate effort.~~

§ 7023(c): A business that complies with a consumer's request to correct shall correct the personal information at issue on its existing systems and implement measures to ensure that the information remains corrected. The business shall also instruct all service providers and contractors that maintain the personal information at issue in the course of providing services to the business to make the necessary corrections in their respective systems unless such notification proves impossible or involves disproportionate effort. Service providers and contractors shall comply with the business's instructions to correct the personal information or enable the business to make the corrections and shall also ensure that the information remains corrected. Illustrative examples follow.

§ 7025 (b): A business that elects to provide an opt-out preference signal pursuant to subdivision (b) of Section 1798.135 shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing:

(1) The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field.

(2) The signal shall have the capability to indicate that the consumer has selected to turn off the opt-out preference signal.

~~(2)~~(3) The platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer, whether in its configuration or in disclosures to the public, that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information. The configuration or disclosure does not need to be tailored only to California or to refer to California.

(4) In no event should a business be expected to process a preference signal in a manner that exceeds the technical capability of the platform, technology, or mechanism that sends the opt-out preference signal. For instance, where a signal is in an HTTP header field format, the business shall process the signal only where it is received on a browser.

§ 7025(c): If the opt-out preference signal conflicts with a consumer's business-specific privacy setting that allows the business to sell or share their personal information, the business shall process the opt-out preference signal, but may notify the consumer of the conflict and provide the consumer with an opportunity to consent to the sale or sharing of their personal information. The business shall comply with section 7004 in obtaining the consumer's consent to the sale or sharing of their personal information. If the consumer consents to the sale or sharing of their personal information, the business may ignore the opt-out preference signal for as long as the consumer is known to the business, but the business must display ~~in a conspicuous manner~~ the status of the consumer's choice in accordance with section 7026, subsection (f)(4).

§ 7026(f)(2): ~~Notifying all third parties to whom the business has sold or shared the consumer's personal information, after the consumer submits the request to opt-out of sale/sharing and before the business complies with that request, that the consumer has~~

~~made a request to opt-out of sale/sharing and directing them to comply with the consumer's request and forward the request to any other person with whom the person has disclosed or shared the personal information during that time period.~~

§ 7026(f)(3): Notifying all third parties to whom the business has sold or shared the consumer's ~~makes~~ personal information ~~available, including businesses authorized to collect personal information or controlling the collection of personal information on the business's premises,~~ that the consumer has made a request to opt-out of sale/sharing and directing them ~~1) to comply with the consumer's request~~ unless such notification proves impossible or involves disproportionate effort ~~and 2) to forward the request to any other person with whom the third party has disclosed or shared the personal information during that time period.~~ In accordance with section 7052, subsection (a), those third parties ~~and other persons~~ shall no longer retain, use, or disclose the personal information unless they become a service provider or contractor that complies with the CCPA and these regulations.

§ 7026(f)(4): Providing a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business. For example, the business may display on its website or its consumer privacy controls "Consumer Opted Out of Sale/Sharing" or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.

§ 7051(a)(3): Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business for any purposes other than those specified in the contract or as otherwise permitted by the CCPA and these regulations. ~~This section shall list the specific business purpose(s) and service(s) identified in subsection (a)(2).~~

§ 7051(a)(8): Require the service provider or contractor to notify the business no later than five ten business days after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.

~~**§ 7051(a)(10):** Require the business to inform the service provider or contractor of any consumer request made pursuant to the CCPA that they must comply with, and provide the information necessary for the service provider or contractor to comply with the request.~~

~~**§ 7051(c):** A person who does not have a contract that complies with subsection (a) is not a "service provider" or a "contractor" under the CCPA. For example, a business's disclosure of personal information to a person who does not have a contract that complies with these requirements may be considered a sale for which the business must provide the consumer with the right to opt-out of sale/sharing.~~

§ 7051(e): Whether a business conducts due diligence of its service providers and

contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract [where the business knows or has reason to believe that a violation of the CCPA and these regulations occurred](#) nor exercises its rights to [assess](#), audit or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.

§ 7053(e): Whether a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract [where the business knows or has reason to believe that a violation of the CCPA and these regulations occurred](#) might not be able to rely on the defense that it did not have reason to believe that the third party intends to use the personal information in violation of the CCPA and these regulations at the time of the business disclosed the personal information to the third party.



Computer & Communications
Industry Association
Tech Advocacy Since 1972



August 18, 2022

Via Electronic Mail (regulations@coppa.ca.gov)

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

Re: CPPA Public Comment

The Computer & Communications Industry Association (“CCIA”)¹ is pleased to respond to the California Privacy Protection Agency (the “Agency” or “CPPA”) [Notice of Proposed Rulemaking](#) on the Proposed Regulations (the “Regulations”) that will implement the California Privacy Rights Act of 2020 (the “CPRA”).

INTRODUCTION

CCIA has long supported the evolution of privacy policy to keep pace with evolving technologies. We appreciate that state lawmakers have a continued interest in adopting regulations that will guide businesses and protect consumers. The Regulations are an impressively comprehensive set of protections and are, by far, the most developed guidelines in the nation.

These comments focus on a few provisions in the Regulations that warrant revision. The aim of these suggestions is manyfold. First, to ensure that the Regulations are reflective of the mandates stated in the CPRA. Secondly, that the Regulations are

¹ CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms. For 50 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. A list of CCIA members is available at <https://www.ccianet.org/members>.

feasible to implement in a timely and clear manner. Third, that the Regulations allow flexibility in order not to not inhibit innovation. Finally, to prevent any unintended retroactive application of this new set of rules.

CCIA's suggested amendments to the Regulations are set forth in **Attachment**

A.

I. CONSENT AND OPT-OUT

A. Opt-Out Preference Signals – § 7025(b)

By requiring that businesses recognize global opt-out preference signals, the draft Regulations go beyond, and actually contradict, what is stated in the CPRA. Section 1798.135 of the statute makes clear that businesses may choose to either (i) provide links for consumers to opt-out of “selling,” “sharing,” or certain uses and disclosures of sensitive personal information; or (ii) recognize universal opt-out preference signals. The draft Regulations, by contrast, reject this approach and instead require businesses to honor global opt-out preference signals. Section 7025(b) of the draft rules should be revised to treat recognition of global opt-out preference signals as voluntary in line with the statute. See Attachment A.

In addition, CCIA suggests that the regulations should permit consumers to both turn on and turn off the opt-out mechanism discussed in § 7025(b). The opt-out mechanism should also harmonize treatment of that signal with the confirmatory display discussed in § 7026(f)(4).

These provisions would make the signal more user friendly, which is a stated goal of these Regulations as indicated in § 7025(a). They would also be consistent with treatment of cookie settings (which encompasses signals such as this) under the General Data Protection Regulation (GDPR) and Europe's ePrivacy Directive, which

provide clarity that: (1) a business's website should feature a consent banner that allows visitors to either give or refuse consent to the non-necessary cookies that process personal information;² and (2) methods for offering a right to refuse or requesting consent should be made as user-friendly as possible, and settings should remain available for users to revisit and adjust, as they prefer.³ Consistent treatment of signals and settings assists businesses with compliance by creating a unified, global approach.

B. Appropriate Notice to Obtain Opt-Out – § 7013(e)(3)

Section 7013(e)(3) requires a business to provide a notice to opt out of data sale and data sharing in the same manner in which the business collects the personal information. The Initial Statement of Reasons (ISOR) indicates that the Agency crafted this requirement to address new ways in which businesses are collecting personal information and to ensure that the notice is effective.⁴ CCIA is concerned, however, that § 7013(e)(3) exceeds the mandate of the CPRA. We suggest that this rule be more consistent with what is becoming the national approach.

The stated provisions go beyond the CPRA requirements and similar state omnibus laws. That is, Section 1798.130(a)(5) of the CPRA requires only that the business disclose the consumer's right in its online privacy policy or on the internet webpage. A business that collects personal information outside a website should be able to satisfy its obligation by directing the consumer to its website. For instance, §

² See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Council Directive 95/46/EC (General Data Protection Regulation), 26 O.J. (L 119), <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

³ See OFFICIAL JOURNAL OF THE EUROPEAN UNION, DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 25 NOVEMBER 2009, SECTION 20(a).

⁴ See Cal. Privacy Protection Agency, *Initial Statement of Reasons* (Jun. 6, 2022) [hereinafter *ISOR*], https://cppa.ca.gov/meetings/materials/20220608_item3_isr.pdf.

7013(e)(3)(A) explains that a brick-and-mortar store can post signage directing consumers to an online notice. This is less burdensome than the example in § 7013(e)(3)(B), which would require a business collecting personal information over the phone to “orally” walk through the notice. The same issue arises for connected devices in § 7013(e)(3)(C). In these settings, the business should have the option of “orally” directing the consumer to the website notice, as permitted for physical stores.

By way of comparison, the Virginia Consumer Data Protection Act (VCDPA) and Colorado Privacy Act (CPA) only require businesses to present opt-out methods clearly and conspicuously in privacy notices and in readily accessible locations outside of privacy notices.⁵ These opt-outs are not required to be presented in the same manner of data collection.⁶

If it expands notice obligations by requiring businesses to offer opt-out in the same manner as it discloses how data is collected, the Agency would impose significant burdens on businesses that maintain a website but collect personal information by other means. Adopting the approach taken in other state privacy laws, by contrast, will be beneficial to businesses and to consumers as there is a clearer path forward regarding how best to provide and act upon consumer rights. Moreover, this result would be more consistent with § 1798.130(a)(5) of the CPRA, which requires only that the business disclose the consumer’s rights via online privacy policy or internet webpage.

C. Opt-Out Consent for Pre-Data Collection – § 7013(h)

As written, the Regulations do not provide language specifying when the

⁵ See [VA. CONSUMER DATA PROT. ACT](#), H 2307, 2021 SPECIAL SESSION, § 59.1-574(c) (2022); see also [COL. PRIVACY ACT](#), SB 21-190, 2021 REG. SESS., § 6-1-1306 (1)(a)(III) (2022).

⁶ See *id.*

requirement to obtain opt-out consent for pre-data collection applies. CCIA suggests reworking § 7013(h) to ensure that businesses and consumers understand that the requirement will apply to data collected after the notice requirement goes into effect.

More specifically, CCIA suggests that the Agency clarify § 7013(h) to require affirmative consent to sell/share information collected *prior* to the opt-out notice, but limiting it to information collected *after* the notice requirement goes into effect. These temporal specifications will align the Regulations privacy laws in other states, which do not prevent businesses from engaging in targeted advertising based on information already collected.

D. Notifying Third Parties of a Consumer’s Opt-Out – §§ 7026(f)(2) and (3)

The requirement to notify third parties of a consumer’s opt-out status should apply on a going-forward basis only; it should not require a company to go back to previous transactions by passing the opt-out request to all downstream partners. In any case, the notification requirement should (1) be limited only to the third parties to whom the business has sold or shared the customer’s personal information, as opposed to § 7026(f)(3)’s requirement to notify all third parties with whom the business makes personal information available; and (2) include the disproportionate effort standard, to prevent a business from expending unnecessary time and resources with little benefit to consumers. Indeed, while the GDPR does require notice to third parties when a consumer exercises their rights, it does not require such notice if it would require the business to expend disproportionate effort.⁷

E. Confirmation of Consumer Opt-Outs – § 7026(f)(4)

⁷ See General Data Protection Regulation, *supra* note 2, art. 19, (“Notification Obligation Regarding Rectification or Erasure of Personal Data or Restriction of Processing”).

The Regulations would require a business that sells or shares personal information to provide a means by which a customer can confirm that the business has processed their opt-out request. This new requirement appears to extend beyond the statutory requirements in the CPRA. See Cal. Civ. Code § 1798.120(a) & (b). Although it discusses opt-out options and mentions forthcoming regulations that will “define the requirements and technical specifications for” opt-out options, the CPRA makes no mention of the requirement to confirm processing of opt-out requests. Further, this requirement does not appear in the CDPA, CPA, Connecticut Act Concerning Personal Data Privacy and Online Monitoring (CTDPA), the Utah Consumer Privacy Act (UCPA), or VCDPA. Such a regulation, namely, one that travels well beyond its statutory basis and other state privacy laws is a slippery slope CCIA strongly advises against.

In addition to being overly broad, the requirement to confirm the processing of opt-out requests is unnecessary. The CPRA already includes enforcement provisions that motivate businesses to honor and process consumer requests. Imposing a further obligation to confirm opt-outs seems like overkill. We note that the ISOR discloses that the Agency considered the alternative of requiring businesses to confirm receipt of opt-out requests, but determined that such a requirement was “too prescriptive.”⁸ Requiring opt-out confirmation would be equally prescriptive. CCIA respectfully suggests that the Agency eschew both forms of additive obligation.

The most important aspect of the Regulations is the goal of ensuring a supportive user experience. With regard to opt-out, if businesses are required to display preference, they should have the option of showing preference on their website or within

⁸ ISOR, *supra* note 4, at 42.

privacy settings so that the consumer’s experience is not cluttered. Enabling this type of choice furthers the Agency’s desire to use a “performance-based standard that gives flexibility to the business regarding how to display the status of the consumer’s request,” as stated in the ISOR.⁹

II. THIRD-PARTY SERVICE PROVIDERS AND CONTRACTORS

A. The Proposed Rules Improperly Default to Converting Third Parties Into Primary Actors – § 7051(c)

Section 7051, as written, improperly converts service provider/contractor relationships into third party relationships, which imposes a host of additional legal obligations set forth in § 7052 if the contract is deemed not fully compliant with the Regulations. This language creates a double penalty whereas failure to have an appropriate contract and comply with the law holds penalty enough. This layering of additional legal exposure seems both unnecessary — the business would already have violated the contract regulations — and punitive. In addition, the triggered third-party classification would not reflect the actual relationship between the business and the external party, which might be engaged in an otherwise permitted business purpose that is neither selling nor sharing.

No other U.S. State’s law creates this kind of regulatory layering. Under the GDPR, a processor is responsible for its own violation of the law. For these reasons, CCIA suggests that § 7051(c) be deleted.

B. The Rules Should Include Liability Exemptions for Violations Committed by Service Providers and Contractors – §§ 7051(e) and 7053(e)

Section 1798.145 of the CPRA includes an exemption that exculpates

⁹ ISOR, *supra* note 4, at 46.

businesses from service provider and contractor non-compliance where appropriate due diligence has been conducted. As the Agency works to promulgate regulations on when this section applies, CCIA encourages it to provide added clarity by listing factors that affirmatively indicate a violation, as opposed to leaving businesses to formulate a reasonable belief that the external party is in violation. We suggest updating §§ 7051(e) and 7053(e) in order to incorporate specific factors to be considered.

By listing affirmative factors, the Regulations will not place additional burdens on businesses to confirm the absence of violations. Rather, businesses will be equipped with guidance on how to best conduct due diligence, which is similar to the guidance provided to data exporters in the European Commission's Standard Contractual Clauses (SCCs). Just as the SCCs offer guidance to data exporters by instructing them that they may, "take into account relevant certifications held by the data importer" when deciding on a review or audit, the Regulations can and should also offer more clarity to businesses in this section.¹⁰

C. The Rules Should Not Contain Overly Prescriptive Requirements for Contracts with Third Parties

The Regulations as they pertain to contracts, and specifically the provisions related to use of consumer data, third party data collection, and deadlines for providing notice of inability to comply, warrant some revision in order not to create onerous or duplicative compliance burdens that will not substantially increase privacy protections.

1. Use of Consumer Data – § 7051(a)(3)

¹⁰ EUROPEAN COMMISSION, ANNEX TO THE COMMISSION IMPLEMENTING DECISION ON STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES PURSUANT TO REGULATION (EU) 2016/679, Module 2 (8.9)(c), Transfer Controller to Processor: Documentation and Compliance, <https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors>, .

Section 7051(a)(3)'s requirement that contract provisions include a prohibition against using information for other purposes *in addition to* the purposes of processing seems overly prescriptive. Neither the GDPR (through SCCs) nor other state laws require contracts to include such a prohibition. Instead, they primarily require contracts with third parties to include language regarding the nature of processing, parameters around purpose, and duration; clear instructions for processing data; and both parties' rights and obligations under the agreement.¹¹ These laws also place confidentiality, deletion, compliance, and assessment/audit requirements on the respective parties, although these are not required to be listed in the contracts. None of these laws require contracts to include a prohibition against using information for other purposes.

2. Third-Party Data Collection – § 7012(g)(3)

Similarly, the third-party data collection requirement in § 7012(g)(3) also seems too prescriptive. The Regulations should permit notice that is “reasonable” in the context of the method of data collection. For instance, if a store or restaurant employs a third-party voice assistant device that does not contain a physical display, then a notice directing the consumer to the third-party device's website should be sufficient.

The Federal Trade Commission (FTC) has already provided guidance for providing appropriate disclosures in various contexts through its *Dot Com Disclosures*, which make clear that ensuring clear disclosure of appropriate terms based on text and available means is the more important standard upon which to rely.¹² For instance, the

¹¹ See [VA. CONSUMER DATA PROT. ACT](#), *supra* note 5, § 59.1-575 (2022); see also [COL. PRIVACY ACT](#), *supra* note 5, § 6-1-1305 (2022); [UT. CONSUMER PRIVACY ACT](#), S.B. 227, 2022 Gen. Sess., § 13-61-301 (2022).

¹² See FTC, DOT COM DISCLOSURES: Information About Online Advertising (May 2000), <https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-issues-guidelines-internet-advertising/0005dotcomstaffreport.pdf>.

FTC makes clear that using email instead of direct mail may be appropriate as long as a website operator discloses the manner in which it will provide information and provides it in a form that consumers can retain.¹³ The FTC demonstrates an understanding of the need for flexibility and adaptability in creating a meaningful user experience. The Regulations should adopt the flexibility allowed by the FTC by permitting said third parties to provide notice in a reasonable manner. Updating § 7012(g)(3) accordingly will help to permit businesses to better engage with service providers and still allow meaningful disclosures to consumers.

D. The Deadline for Third Parties to Provide Notice of Inability Should Be Increased to Ten Business Days – § 7051(a)(8)

Section 7051(a)(8) imposes a very short period—five business days—for a service provider or contractor to notify a business it can no longer meet its obligations. According to the ISOR, the slim five-day window is “necessary so that the business can take prompt action” and will help businesses “protect consumer personal information from unauthorized use.”¹⁴ The ISOR also states that this is a reasonable and feasible maximum timeframe for service providers to provide notice.¹⁵

Though prompt action is important, the time period is overly burdensome. For this reason, a 10-business day window would be more appropriate and more like the Agency’s past rulemaking efforts. When enacting California Consumer Privacy Act regulations, the Agency implemented a 10-business day window for businesses to acknowledge receipt of data subject access requests (DSAR).¹⁶ Other entities provide

¹³ *See id.*

¹⁴ ISOR *supra* note 4, at 51.

¹⁵ *Id.*

¹⁶ [CAL. CONSUMER PRIVACY ACT REGULATIONS](#), § 11 CCR 7021(a) (2022).

even longer notice periods, as seen with the GDPR’s requirement that controllers handle DSAR requests without undue delay and “in any event within one month of receipt of the request.”¹⁷

III. CONSUMER RIGHTS

A. Collection and Use of Consumer Data – § 7002(a)

The CPRA restricts the collection and use of personal information to what is “reasonably necessary and proportionate.” Cal. Civ. Code § 1798.100(c). Section 7002(a) of the draft Regulations would implement that standard to mean “what an average consumer would expect when the personal information was collected.” This interpretation somewhat alters the CPRA standard in a manner that will make implementation quite difficult.

Inserting an “average consumer” gloss on the CPRA restriction for data usage creates a mutable and subjective standard. As the mind of the “average consumer” is difficult to accurately ascertain, and consumers, businesses, and regulators may differ on what an average consumer expects, a focus on the purpose provides more clarity for businesses seeking to comply with the Regulations.

CCIA notes that the GDPR contains the same restriction as the CPRA – data usage must be limited to what is necessary in relation to the purposes for which they are processed – without adoption of an additional “average consumer” standard.¹⁸

B. Data Minimization – § 7002(b)(1)

The illustrative examples of data minimization practices in § 7002(b) are quite

¹⁷ See General Data Protection Regulation, *supra* note 2, art. 12, (“Transparent Information, Communication, and Modalities for the Exercise of the Rights of the Data Subject”).

¹⁸ See *id.* art. 5(c), (“Principles Relating to Processing of Personal Data”).

narrow. CCIA is concerned that this list will restrict innovation. For instance, the Regulations assume that the primary function of a service should be the exclusive function, an assumption more narrow than the GDPR's data minimization provision, which allows businesses to process personal information in ways that are adequate and relevant to what is necessary in relation to the purposes for which it is processed.¹⁹ In illustrative example § 7002(b)(1), a mobile flashlight application should only provide flashlight services and not offer ancillary benefits that might rely on collected data such as identifying restaurants that are too dimly lit or public areas with insufficient street lighting. In fact, these additional features benefit the consumer. To that end, it would also be helpful for the Regulations to include an example where the use of data to improve and build net new features are not incompatible with the original purpose.

C. Correction Requests – § 7023(c)

With regard to consumer requests for correction, a “disproportionate effort” standard should apply. With the potential that tens of billions of requests will start coming in, the Agency should adopt some kind of material delimiter to this obligation.

Relieving businesses from exerting disproportionate effort in meeting correction requests would comport with other state privacy laws. The CDPA, CPA, and CTDPA allow businesses an exemption from fulfilling requests for correction where it would be unreasonably burdensome for the controller to associate the request with the personal information.²⁰

This same type of delimiter should apply to the obligation in § 7022(c)(4) to notify

¹⁹ See *id.*

²⁰ See [VA. CONSUMER DATA PROT. ACT](#), *supra* note 5, § 59.1-577 (2022); see also [COL. PRIVACY ACT](#), *supra* note 5, § 6-1-1307 (2022); [CT. ACT CONCERNING PERSONAL DATA PRIVACY AND ONLINE MONITORING](#), PA 22-15, 2022 Gen. Assemb., § 9(c) (2022).

third parties when a deletion is made. CCIA suggests that the rule be modified to require “reasonable efforts” to notify third parties.

IV. DARK PATTERNS

When designing consumer requests and obtaining consent, businesses should be required to ensure that the language is easy to understand, that there is no manipulative or confusing language, that there is symmetry in choice, and that the methods present “easy-to-execute” options. The Regulations appropriately state that non-compliant design methods may be considered dark patterns that do not result in valid consent. But the broad “symmetry in choice” standard in § 7004(a)(2) should be honed somewhat.

CCIA suggests that the Agency adopt the FTC’s approach to dark patterns, which focuses on eliminating practices that are harmful rather than prescribing specific design practices that will limit innovation and creativity in design. Specifically, the FTC’s enforcement policy statement forbids businesses from engaging in processes that fail “to provide clear, up-front information, obtain consumers’ informed consent, and make cancellation easy.”²¹ The FTC does not, however, impose a requirement akin to §7004(a)(2) (“The path for a consumer to exercise a more privacy-protective option shall not be longer more burdensome than the path to exercise a less privacy-protective option”). Rather than prohibiting longer privacy-protective options, § 7004(a)(2) should adjust the requirement that *more burdensome* privacy-protective options are prohibited, rather than simply prohibiting *longer* privacy-protective options.

²¹ Juliana Gruenwald Henderson, *FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions*, Federal Trade Commission (Oct. 28, 2021), <https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions>

CONCLUSION

CCIA and its members thank the Agency for this opportunity to provide suggestions on how to perfect the Regulations in ways that protect consumer data, are feasible to implement, and retain flexibility for customization and innovation. The suggested alternative language discussed herein, which is also provided in Attachment A in redline form for ease of review, is offered as a means for achieving the best result for consumers, regulators, and the online ecosystem.

Respectfully submitted,

Stephanie A. Joyce
Chief of Staff and Senior Vice President
Khara Boender
State Policy Director
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, DC 20001



August 18, 2022

ATTACHMENT A

Suggested Amendments to Proposed Rules

§ 7002(a): A business's collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purpose(s) for which the personal information was collected or processed. ~~To be reasonably necessary and proportionate, the business's collection, use, retention, and/or sharing must be consistent with what an average consumer would expect when the personal information was collected.~~ A business's collection, use, retention, and/or sharing of a consumer's personal information may also be for other disclosed purpose(s) if they are compatible with ~~what is reasonably expected by the average consumer~~ the context in which the personal information was collected. A business shall obtain the consumer's explicit consent in accordance with section 7004 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.

§ 7002(b)(1): Business A provides a mobile flashlight application. Depending on the circumstances, Business A should not collect, or allow another business to collect, consumer geolocation information through its mobile flashlight application without the consumer's explicit consent because the collection of geolocation information is incompatible with the context in which the personal information is collected, i.e., provision of flashlight services. The collection of geolocation data ~~may is not be within the reasonable expectations of an average consumer, nor is it~~ may is not be within the reasonable expectations of an average consumer, nor is it reasonably necessary and proportionate to achieve the purpose of providing, improving, or adding features to a flashlight function.

§ 7004(a)(2): Symmetry in choice. The path for a consumer to exercise a more privacy-protective option shall not be ~~longer~~ more burdensome than the path to exercise a less privacy-protective option. Illustrative examples follow.

§ 7004(a)(4): Avoid manipulative language or choice architecture. The methods should not use language or wording that ~~guilts or shames~~ threatens or misleads the consumer into making a particular choice ~~or bundles consent~~ so as to subvert the consumer's choice. Illustrative examples follow.

...

(B) Requiring the consumer to click through false or misleading reasons why submitting a request to opt-out of sale/sharing is ~~allegedly~~ a bad choice before being able to execute their choice to opt-out is manipulative ~~and shaming~~.

(C) It is manipulative to bundle choices so that the consumer is only offered the option to consent to using personal information for reasonably expected purposes

together with purposes that are incompatible to the context in which the personal information was collected. For example, a business that provides a location-based service, such as a mobile application that posts gas prices within the consumer's location, shall not require the consumer to consent to incompatible uses (e.g., sale of the consumer's geolocation to data brokers) together with the expected use of providing the location-based services, which does not require consent. This type of choice architecture is manipulative because the consumer is forced to consent to incompatible uses in order to obtain the expected service. The business should provide the consumer a separate option to consent to the business's use of personal information for unexpected or incompatible uses.

§ 7012(g)(3): A business that, acting as a third party, controls the collection of personal information on another business's premises, such as in a retail store or in a vehicle, shall also provide a notice at collection in a conspicuous manner, [which takes into account the method of the data collection](#), at the physical location(s) where it is collecting the personal information.

§ 7013(e)(3)(B): A business that sells or shares personal information that it collects over the phone ~~may~~ **shall** provide notice orally during the call when the information is collected.

§ 7013(e)(3)(C): A business that sells or shares personal information that it collects through a connected device (e.g., smart television or smart watch) shall provide notice in a manner that ensures that the consumer will encounter the notice [or direct the consumer to where the notice can be found online](#) while using the device.

§ 7013(h): A business shall not sell or share the personal information it collected [after the effective date and](#) during the time the business did not have a notice of right to opt-out of sale/sharing posted unless it obtains the consent of the consumer.

§ 7022(c)(4): Notifying any other service providers, contractors, or third parties that may have accessed personal information from or through the service provider or contractor, unless the information was accessed at the direction of the business, to delete the consumer's personal information unless this proves impossible or involves disproportionate effort. ~~If the service provider or contractor claims that such a notification is impossible or would involve disproportionate effort, the service provider or contractor shall provide the business a detailed explanation that shall be relayed to the consumer that includes enough facts to give a consumer a meaningful understanding as to why the notification was not possible or involved disproportionate effort. The service provider or contractor shall not simply state that notifying those service providers, contractors, and/or third parties is impossible or would require disproportionate effort.~~

§ 7023(c): A business that complies with a consumer's request to correct shall correct the personal information at issue on its existing systems and implement measures to ensure that the information remains corrected. The business shall also instruct all service providers and contractors that maintain the personal information at issue in the course of providing services to the business to make the necessary corrections in their respective systems unless such notification proves impossible or involves disproportionate effort. Service providers and contractors shall comply with the business's instructions to correct the personal information or enable the business to make the corrections and shall also ensure that the information remains corrected. Illustrative examples follow.

§ 7025 (b): A business that elects to provide an opt-out preference signal pursuant to subdivision (b) of Section 1798.135 shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing:

(1) The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field.

(2) The signal shall have the capability to indicate that the consumer has selected to turn off the opt-out preference signal.

~~(2)~~(3) The platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer, whether in its configuration or in disclosures to the public, that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information. The configuration or disclosure does not need to be tailored only to California or to refer to California.

(4) In no event should a business be expected to process a preference signal in a manner that exceeds the technical capability of the platform, technology, or mechanism that sends the opt-out preference signal. For instance, where a signal is in an HTTP header field format, the business shall process the signal only where it is received on a browser.

§ 7025(c): If the opt-out preference signal conflicts with a consumer's business-specific privacy setting that allows the business to sell or share their personal information, the business shall process the opt-out preference signal, but may notify the consumer of the conflict and provide the consumer with an opportunity to consent to the sale or sharing of their personal information. The business shall comply with section 7004 in obtaining the consumer's consent to the sale or sharing of their personal information. If the consumer consents to the sale or sharing of their personal information, the business may ignore the opt-out preference signal for as long as the consumer is known to the business, but the business must display ~~in a conspicuous manner~~ the status of the consumer's choice in accordance with section 7026, subsection (f)(4).

§ 7026(f)(2): ~~Notifying all third parties to whom the business has sold or shared the consumer's personal information, after the consumer submits the request to opt-out of sale/sharing and before the business complies with that request, that the consumer has~~

~~made a request to opt-out of sale/sharing and directing them to comply with the consumer's request and forward the request to any other person with whom the person has disclosed or shared the personal information during that time period.~~

§ 7026(f)(3): Notifying all third parties to whom the business has sold or shared the consumer's ~~makes~~ personal information ~~available, including businesses authorized to collect personal information or controlling the collection of personal information on the business's premises,~~ that the consumer has made a request to opt-out of sale/sharing and directing them ~~1) to comply with the consumer's request~~ unless such notification proves impossible or involves disproportionate effort ~~and 2) to forward the request to any other person with whom the third party has disclosed or shared the personal information during that time period.~~ In accordance with section 7052, subsection (a), those third parties ~~and other persons~~ shall no longer retain, use, or disclose the personal information unless they become a service provider or contractor that complies with the CCPA and these regulations.

§ 7026(f)(4): Providing a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business. For example, the business may display on its website or its consumer privacy controls "Consumer Opted Out of Sale/Sharing" or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.

§ 7051(a)(3): Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business for any purposes other than those specified in the contract or as otherwise permitted by the CCPA and these regulations. ~~This section shall list the specific business purpose(s) and service(s) identified in subsection (a)(2).~~

§ 7051(a)(8): Require the service provider or contractor to notify the business no later than five ten business days after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.

~~**§ 7051(a)(10):** Require the business to inform the service provider or contractor of any consumer request made pursuant to the CCPA that they must comply with, and provide the information necessary for the service provider or contractor to comply with the request.~~

~~**§ 7051(c):** A person who does not have a contract that complies with subsection (a) is not a "service provider" or a "contractor" under the CCPA. For example, a business's disclosure of personal information to a person who does not have a contract that complies with these requirements may be considered a sale for which the business must provide the consumer with the right to opt-out of sale/sharing.~~

§ 7051(e): Whether a business conducts due diligence of its service providers and

contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract [where the business knows or has reason to believe that a violation of the CCPA and these regulations occurred](#) nor exercises its rights to [assess](#), audit or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.

§ 7053(e): Whether a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract [where the business knows or has reason to believe that a violation of the CCPA and these regulations occurred](#) might not be able to rely on the defense that it did not have reason to believe that the third party intends to use the personal information in violation of the CCPA and these regulations at the time of the business disclosed the personal information to the third party.

From: **MacGregor, Melissa** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
CC: **Chamberlain, Kim** [REDACTED]
Subject: CPPA Public Comment
Date: 18.08.2022 19:49:27 (+02:00)
Attachments: California Privacy Regulation Letter - Aug 18, 2022.pdf (14 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Please the attached comments on the CPRA proposed rulemaking. Please reach out to us if you have any questions or comments.

Thanks!

Melissa MacGregor
Managing Director & Associate General Counsel
SIFMA
1099 New York Ave., Suite 600
Washington, DC 20001
[REDACTED]



August 18, 2022

Submitted via email: regulations@cpha.ca.gov

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

Re: CPPA Public Comment for CPRA Regulations

Dear Mr. Soublet,

The Securities Industry and Financial Markets Association (“SIFMA”)¹ appreciates the opportunity to respond to the California Privacy Protection Agency (“CPPA”) Notice of Proposed Rulemaking dated July 8, 2022 (the “Proposed Regulations”) that will implement regulations required under the Consumer Privacy Rights Act of 2020 (“CPRA”).² SIFMA appreciates the work that the CPPA has done to bring public attention to consumer privacy issues and work with companies to achieve a higher level of consumer protection.

SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets, including a significant presence in California. SIFMA has 24 broker-dealer and asset manager members headquartered in California. Further, there are approximately 384 broker-dealer main offices, nearly 40,000 financial advisers, and 93,522 securities industry jobs in California.³

SIFMA urges the CPPA to carefully consider the costs associated with potentially overly prescriptive regulations both for businesses and ultimately for customers. We highlight below several proposed requirements which may do little to protect investors but would be costly to comply with. Companies that must comply with the CPRA are already engaged in updating their policies, processes, procedures, contracts, and websites to meet the by January 1, 2023 deadline. Any new obligations in the Proposed Regulations that markedly change or expand upon the

¹ The Securities Industry and Financial Markets Association (SIFMA) is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's one million employees, we advocate on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit <http://www.sifma.org>.

² https://cpha.ca.gov/regulations/pdf/20220708_npr.pdf

³ <https://states.sifma.org/#state/ca>

CPRA requirements will create significant unnecessary expenditures of resources for all such companies, while not necessarily aligning with the expectations of the California citizens who voted for the law. The CPPA should avoid creating regulatory mandates that far exceed the requirements of the CPRA, which is itself an expansion of the existing privacy law in California.

Also, SIFMA continues to remain concerned about the potential expiration of the employee and business-to-business (“B2B”) data exemptions in the CPRA. If, or when, the exemptions expire, the CPRA and its regulations will apply to employee personal information and personal information belonging to an employee or an individual associated with another legal entity involved in a commercial transaction with a business (e.g., B2B contact details). Applying the CPRA and its regulations to employee and B2B data will create unintended consequences and compliance problems which will be compounded by the new obligations that would be imposed by the Proposed Regulations.

1. Priority Issues

Although we provide detailed comments on a wide variety of issues below, we would like to highlight the following priority issues for your consideration:

- **Notice Regarding Third Party Data Collection** (*See #6 below*): The Proposed Regulations expand the notice at collection requirements to include, among other things, the names of all third parties that a business allows to control the collection of Personal Information (“PI”) from a consumer (e.g., through analytics cookies) or, as an alternative, provide the consumer with information about the third party’s information handling practices.
- **Restrictions on Additional Uses of PI** (*See #2 below*): The Proposed Regulations specify that a business’s collection, use, retention and sharing of PI must be “reasonably necessary and proportionate” to achieve the purpose for which the PI was collected or processed and define this standard in relation to what an “average consumer” would expect when the PI was collected. Any uses that are unrelated or incompatible with the original purpose requires prior explicit consent from the consumer.
- **Sensitive PI** (*See #8 and #15 below*): Although the Proposed Regulations list the permissible purposes for processing sensitive PI, unlike Section 1798.121(d) of the CPRA, the Proposed Regulations do not specify that a consumer’s right to limit use/disclosure of sensitive PI must be provided only when a business uses the sensitive PI to infer characteristics about the consumer.
- **Overly prescriptive contract requirements for third parties** (*See #16(b) below*): Failure to include all the newly required terms in a vendor contract means that under the CPRA, the vendor cannot be considered to be a service

provider, must be treated as a third party and any disclosure of PI to the vendor may be deemed to be a “sale” or “sharing” of personal information.

- **Business purpose disclosures in service provider/contractor/third party contracts** (*See #18(f) below*): New requirements to identify the specific business purposes and services for which PI will be processed on behalf of the business and specify that the business is disclosing the PI only for the limited and specified business purposes set forth in the contract between the parties - a generic description referencing the entire contract is not acceptable. Identifying these specific business purposes in a contract with a vendor is not a typical practice and complying with this obligation would require businesses to amend all contracts with service providers to include language that is specific and particular to the services that the service provider provides to the businesses. Adding such language in the contract does not serve any practical purpose, would impose significant burdens on businesses to include customized language in their contracts with service providers and ensure that the language in the contracts is kept current as the services provided expand and change over time.
- **Confusing treatment of providers of advertising services** (*See #16(a) below*): Any entity providing cross-context behavioral advertising to a business is considered to be a third party for CPRA purposes and cannot be a service provider or contractor even if the entity otherwise meets all of the CPRA requirements for a service provider or contractor.

2. Restrictions on Use of PI (Section 7002(a))

Section 1798.100(c) of the CPRA states that “[a] business’s collection, use, retention, and sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.” Section 1798.100(a)(1) of the statute permits the collection or use of PI for additional purposes that are incompatible with the disclosed purposes for which the PI was originally collected if the business notifies the consumer of the additional purposes.

Unlike Section 1798.100(a)(1) of the CPRA, Section 7002(a) of the Proposed Regulations requires the business to obtain “explicit consent” from consumers prior to collecting, using, retaining, or sharing PI for “any purpose that is unrelated or incompatible with the purpose(s) for which the personal information [was] collected or processed.” However, there is no basis in the CPRA for requiring a business to obtain a consumer’s explicit consent in these situations. This new requirement introduced by the Proposed Regulations will remove a business’s ability to rely on making updates to the disclosures in its privacy policy to address changes in its practices regarding the collection/use/retention and sharing of PI and the flexibility to respond to evolving business practices. Complying with this new requirement will also result

in material changes to data collection practices, add significant compliance costs, and adversely impact innovation while providing little additional benefit to consumers.

The CPPA should amend the Proposed Regulations to require that in situations in which the business collects, uses, retains or shares any PI for any purpose that is unrelated or incompatible with the purpose(s) for which the PI was originally collected or processed, the business would be required to provide to consumers notice of such new purposes, rather than obtaining the consumers' prior explicit consent.

3. Dark Patterns (Section 7004)

The Section 7004(c) of the Proposed Regulations significantly expands the current definition of "dark patterns" to include any user interface that "has the effect of substantially subverting or impairing user autonomy, decision making, or choice, *regardless of a business's intent*" (emphasis added). Section 7004(a) mandates that "a method that does not comply with subsection (a) may be considered a dark pattern." As a result, any method that does not comply with all of the concepts listed in 7004(a) may be considered to be a dark pattern.

This section potentially subjects businesses to strict liability regarding the development and implementation of their user interfaces, and the CPPA or Attorney General could initiate an enforcement action against a business that experienced technical, software, hardware, or other technology-related issues that accidentally or unintentionally caused a user interface to not meet all of the requirements set forth in subsection (a). It is common for businesses of all sizes to experience problems with their websites, online user interfaces, and mobile applications, particularly since there are an exponential number of combinations of hardware devices, browsers, applications and other hardware and software that users can use to access a business's websites and/or mobile applications, and most businesses at some point encounter situations in which the business's website or mobile application does not operate properly on a particular combination of hardware and software used by a user. Moreover, these problems in other scenarios can occur without the business's negligence, wrong-doing, or intent. Malicious actors, hackers, and other criminals can also alter or disrupt a business' online presence, despite the business' use of state-of-the-art security measures. A business should not be punished for something it did not intend or cause nor could have prevented.

The Proposed Regulations should be amended to align with the CPRA definition of "dark pattern" which does not include "regardless of a business's intent" with substantial subversion or impairment of choice concepts. Removing the phrase "regardless of a business's intent" would eliminate the strict liability consequences and take a more measured approach that considers the business's intent, knowledge, and other relevant factors such as information security practices. The Proposed Regulations should also eliminate the rigid mandate that any method that does not comply with all of the concepts listed in Section 7004(a) may be considered a dark pattern. There should be flexibility in assessing whether a particular practice is in fact a dark pattern and the items listed in 7004(a), as well as others, can be among the factors that are considered when determining whether a particular practice meets the definition of a dark pattern.

4. Additional Privacy Policy Requirements (Section 7011(e))

Proposed Section 7011(e) requires a business's privacy policy to include significantly more than what is required by the CPRA. For example, Section 7011(e)(1) requires "a comprehensive description of the business's online and offline practices regarding the collection, use, sale, sharing, and retention of personal information." The statute does not include any requirement that the privacy policy contain a "comprehensive description" of a business's "online and offline practices." The regulations should track with the statute and provide additional guidance or clarity, not create unanticipated requirements with undefined terms such as "comprehensive description."

The Proposed Regulations would also require businesses to provide details in the Privacy Policy and Notice at Collection on a category-by-category basis in a manner that goes well beyond what the CPRA would require, which is extremely difficult to maintain in an accurate fashion and will lead to long and wordy charts that evade the CPPA's stated goal of ensuring an easily digestible explanation of data processing practices to consumers.

This provision should be deleted because the current requirements under the CPRA are sufficient to protect consumers and should not be expanded.

5. Notice at Collection Online Requirement (Section 7012(f))

Section 7012(f) requires a business that collects PI online to provide the notice at collection by providing a "link that takes the consumer directly to the specific section of the business's privacy policy that contains the information required in subsection (e)(1) through (6)." The section continues by stating that directing the consumer to the beginning of the privacy policy or to any other section without the required information will not satisfy the notice at collection requirement. Not only is this requirement overly prescriptive and burdensome, but it is also impractical. Under the Proposed Regulations, the notice at collection would be required to be customized to the particular product or service requested by the consumer which seems to necessitate that every notice at collection would have different links to different sections of the business's privacy policy. Implementing such an arrangement will be extremely burdensome and may be difficult to implement or unnecessarily cumbersome from a technology perspective.

The Notice at Collection specifications also do not take into account the fact that some companies are global and may have different notice requirements for individuals located in different jurisdictions. Therefore, the Notice at Collection mandated in the Draft Regulations may take all website visitors to the section of a Privacy Policy that applies only to California consumers or perhaps US consumers, but that does not meet the specifications of GDPR (including by specifying the lawful bases for processing). This creates complexity and confusion for consumers, which the CPPA is clearly endeavoring to avoid.

The CPPA should delete this provision from the Proposed Regulations.

6. Notice Regarding Third Party Data Collection (Sections 7012(e) and (g))

Proposed Section 7012(e)(6) requires a business that allows third parties to control the collection of PI from a consumer to include in its notice at collection, “the names of all third parties; or, in the alternative, information about the third parties’ business practices.” The CPRA requires only disclosure of “categories” of third parties, never names or business practices, including in the privacy policy, other notices at collection, and in response to the right to know/access. This requirement will be burdensome while providing little benefit to the consumer when it is obvious to the consumer that their data is collected by a third party. The Proposed Regulations should track with the statute requiring disclosure of categories of third parties, not names or business practices. Proposed Section 7012(g)(1) further requires that both the business and the third parties provide a notice at collection, which the proposed regulations state can be provided with a link that carries the consumer to the specific section of the privacy policy that discusses such collection.

Section 7012(g)(1) also introduces a new concept also not in the CPRA regarding third parties who “control” the collection of PI, and the imposition of an obligation for such third parties to deliver their own privacy notice at collection. This section goes beyond the statute, creating new obligations not previously contemplated and should be addressed by the service provider, contractor, and third-party contractual requirements and related restrictions, and not by regulation.

The CPPA should clarify whether providing a list of third parties that control the collection of PI is required even when there may be confidentiality provisions governing disclosure of the existence of an agreement between businesses, or where it is obvious to the consumer that their data is collected by a third party; and where, for white labeled products where the identity of the third party is not disclosed, the first party’s information handling practices apply and will be presented to the consumer.

The CPPA should also clarify how multiple notices of collection are to be presented to consumers in cases where there are multiple third parties engaged in collection, particularly on websites. Finally, it may be operationally difficult for a business to collect sale/sharing opt-outs for itself and all third parties listed in its notice of collection.

7. Notice of Right to Opt-out of Sale/Sharing (Section 7013(e))

Proposed Section 7013(e) requires a business that “sells or shares” PI to provide a notice of right to opt-out of “sale/sharing.” Under the current CCPA statute and CCPA AG Regulations, a business that does not “sell” PI is not required to post a “Do Not Sell My Personal Information” link. Under the Proposed Regulations, if a business “shares” but does not “sell” PI, the regulations require a business to post a “Do Not Sell or Share My Personal Information” link or the alternative link. If a business “shares” but does not “sell,” data or vice versa, the business should be able to post the relevant link and not both links. For example, the business that does not “sell” but “shares” should be permitted to post a “Do Not Share My Personal Information” link without the inclusion of “sale.”

The CPPA should amend the Proposed Regulations to allow businesses more flexibility around how to tag the link. Labeling the link “Do Not Sell or Share My Personal Information” may be misleading to consumers in those cases where a business does one or the other, but not both. It also arguably contradicts a statement a business may make in its notice of collection that it does not sell information. Also, we note the term “share” as defined in the CPRA is arguably not what the average consumer understands sharing to mean and also conflicts with other “sharing” opt-outs that a business may offer (e.g., GLBA third-party sharing opt outs, FCRA affiliate sharing opt outs). Further, links with mandatory naming conventions are problematic for companies that have to comply with multiple different privacy laws across multiple jurisdictions.

8. Limitations on the Use of Sensitive PI (Section 7014)

Although the Proposed Regulations list the permissible purposes for processing sensitive PI, unlike Section 1798.121(d) of the CPRA, the Proposed Regulations do not specify that a consumer’s right to limit use/disclosure of sensitive PI must be provided only when a business uses the sensitive PI to infer characteristics about the consumer.

The Proposed Regulations should be amended to state that sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to the regulations’ requirements pertaining to sensitive personal information. This would align the Proposed Regulations with Section 1798.121(d) of the CPRA. Without the qualifier that is currently in the CPRA, the scope of what constitutes “sensitive information” is increased significantly beyond what is set forth in the CPRA, without any justification in the statute.

9. Permissible Deletion from Backup Systems (Sections 7022(b) and (d))

Section 7022(b)(1) requires businesses to delete a consumer’s PI from its existing systems except “archived or back-up systems,” seemingly indicating that requests to delete do not trigger a requirement to delete PI on archived or back-up systems. To the contrary, Section 7022(d) states that a business that stores any PI on archived or back-up systems “may delay compliance with the consumer’s request” until the archived or back-up system is “restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose.” These provisions open several interpretive questions such as when it may be permissible to delete PI from backup systems and what type of access may trigger the requirement to delete PI from a backup system. For example, “access” should clearly exclude de minimis, temporary, or transient access for maintenance, information security, fraud, system improvement, and other purposes that do not require length or permanent access nor use or disclosure of PI outside of the limited purposes mentioned.

The CPPA should clarify these distinctions and provide better examples of when PI does and does not need to be deleted from backup systems.

10. Documentation to Conduct Correction Assessments (Section 7023)

Proposed Section 7023 requires businesses to undergo an onerous process of looking at the “totality of the circumstances” in deciding to make a correction. This nebulous requirement

leaves firms without adequate guidance on how to perform such assessments and the examples provided are not helpful guides. Similarly, the documentation requirements are burdensome and inappropriate in some cases (e.g., requiring less documentation where there is a high impact to a consumer, such as challenging the appearance of a bankruptcy on their record). Also, the Proposed Regulations do not provide any guidance on how to determine if a request is fraudulent or abusive, leaving businesses that deny a request open to enforcement actions.

Additionally, the responsibility for correcting inaccurate PI should be reallocated, as it is currently overly burdensome for both the consumer and the business. Consumers should be directed to the source of inaccurate information to correct their PI – and that may not be the business in question. Specifically, Section 7023(i) of the Proposed Regulations provides that “[w]here the business is not the source of the information that the consumer contends is inaccurate, in addition to processing the consumer’s request, the business shall provide the consumer with the name of the source from which the business received the alleged inaccurate information.”

The proposed regulations should be revised to clarify that third-party sources of inaccurate information should be primarily responsible for ensuring that the incorrect PI is corrected in third-party systems. Businesses should only be required to inform the consumer of the name of the source from which the business received the allegedly inaccurate information.

11. Notification of External Parties of Denial of Correction Requests (Section 7023(f)(3))

Section 7023(f)(3) requires a business that has denied a consumer’s request either in whole or in part, to notify the consumer that, upon their request, the business will “note both internally and to any person with whom it discloses, shares, or sells the personal information” that the consumer has contested the accuracy of the PI, unless the request is fraudulent or abusive. This requirement goes beyond the statute by requiring a business to notify both internally and to any person with whom it discloses, shares, or sells the PI that the consumer has requested correction, despite the request having been denied. Assuming the denial is lawful, there is no reason a business should have to contact external parties to inform them of a denied request to correct. There is nothing for the external parties to do with this information.

12. The Right to Access Conflicts with the CPRA and Data Minimization Principles

Proposed Section 7024(h) appears to automatically require businesses to provide information they have about a consumer beyond the 12-month period required in the statute, and to provide a detailed explanation if this is not done. This provision conflicts with the CPRA and is unduly burdensome on businesses, as well as in some cases, likely to lead to a conflict with data minimization principles. Further, the requirement to provide information that has been collected by a third party or service provider on the business’s behalf requires clarification. For example, background check providers may collect certain information directly from individuals, but never share the details with the business. To require the business to now collect those details to share with a consumer in response to an access request increases breach exposure and constitutes a further violation of data minimization principles.

The CCPA should strike this requirement from the final rules.

13. Opt-out Preference Signals (Section 7025)

Section 1798.135(a) of the CPRA requires businesses to provide links on their websites that enable consumers to limit the sale and sharing of PI and the use and disclosure of sensitive PI. Section 1798.135(b) indicates that businesses are not required to comply with 1798.135(a) “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 sent with the consumer’s consent.” Section 1798.135(b)(3) further states that “[a] business that complies with subdivision (a) is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b).”

Proposed section 7025(e) states the exact opposite, stating that Section 1798.135 “does not give [a] business the choice between posting the above-referenced links or honoring opt-out preference signals. Even if the business posts the above-referenced links, the business must still process opt-out preference signal.” Section 7025(c)(6) adds additional confusion by saying a business “should display whether or not it has processed the consumer’s opt-out preference signal,” which suggests processing preference signals is optional.

The Proposed Regulations do not address what type of signal qualifies as “universal optout preference signal,” or the technical limitations in honoring universal opt-out preference signals. Currently, there is 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-out preference signals should be an optional method that businesses may use to opt-outs as outlined in the statute. Alternatively, the CPPA should clarify how a signal qualifies as one that businesses must recognize.

The Proposed Regulations directly conflict with the CPRA and should be amended to permit businesses the option to honor universal opt-outs. If businesses must recognize opt-out preference signals, there could be significant operational impacts on businesses, including, among other things, implementing technology to recognize and process such signals and applying them to individuals who may use a range of methods to access a business’s website.

14. Downstream notification of consumer opt-out requests to all third parties (Section 7026(f)(2))

Proposed Section 7026(f)(2) requires a business to notify all third parties to whom the business has sold or shared a consumer’s PI of their request to opt-out of sale/sharing and to forward the consumer’s opt-out request to “any other person with whom the person has disclosed or shared the personal information.” Both requirements go beyond the CPRA and would be technically challenging at the device level whether in connection with a one-off device interaction or in response to a global privacy control. Furthermore, the requirement to forward a consumer’s request to any person with whom the person has disclosed or shared the PI doesn’t take into consideration lawful disclosures to service providers, contractors, law enforcement,

government agencies, or disclosures to other businesses or individuals pursuant to an explicit request or direction from the consumers to make the disclosure.

The CPPA should amend these requirements because they go beyond the statute and are operationally difficult or impossible due to technological and practical limitations.

15. Sensitive PI (Section 7027)

Section 1798.121(d) of the CPRA states that “[s]ensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer, is not subject to this Section [Section 1798.121 on requests to limit use and disclosure of sensitive personal information], as further defined in regulations...and shall be treated as personal information for purposes of all other sections of this Act, including Section 1798.100.” Notably, the draft regulations do not clarify when sensitive PI is considered collected or processed for purposes other than inferring characteristics about a consumer. According to the statute, collecting or processing sensitive PI for purposes other than inferring characteristics about a consumer is exempt from the right to limit the use and disclosure of sensitive PI. However, the draft regulations read as if this exemption does not exist, and any collection or processing of sensitive PI is subject to the right to limit use and disclosure. The regulations should be amended to track the statute.

Also, in a number of sections, the Proposed Regulations contravene and narrow the scope of the statutory language, effectively disregarding Section 1798.121(a)-(b), which permit a business to use a consumer’s sensitive PI for uses that are “necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services,” even after receipt of a consumer’s request to limit. While the Regulations attempt to define permissible uses of sensitive PI in Section 7027(l), the seven use cases listed most certainly do not encompass all those uses of sensitive PI that may be “necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services.” The impact of this overreach by the Proposed Regulations will have significant adverse effects. As an example, in Section 7014(h), the Proposed Regulations purport to impose a springing consent requirement with respect to any use, outside the seven limited uses defined by Section 7027(l), of sensitive PI collected at a time when a business did not have a notice of right to limit posted. As a notice of right to limit is not required until January 1, 2023, any PI collected prior to January 1, 2023, absent consumer consent, may not be used for any purpose other than one of the seven purposes defined by Section 7027(l).

Similarly, in Section 7027(g)(1), the Proposed Regulations require that, upon receipt of a request to limit, a business must cease to use and disclose sensitive PI for any purpose other than the seven purposes listed in Section 7027(l); a restriction that conflicts with the language in 7027(a) and in 1798.121(a)-(b) that allows uses that are “necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services.” These inconsistencies are extremely problematic for constructing a compliance program. The above notwithstanding, the seven use cases identified in 7027(l) don’t even contemplate a use of sensitive PI to comply with a legal or regulatory obligation or otherwise address any use case that relates to uses of employee information.

The CPPA should revise the Proposed Regulations to limit overreach and resolve inconsistencies in the Proposed Regulations and with the CPRA.

16. Service Provider, Third-Party, and Contractor Relationships (Sections 7050, 7051 and 7053)

The combined effect of the service provider/third party/contractor provisions in the proposed regulations is confusing and could, in their present iteration, greatly impact any business that combines information from various sources. Section 1798.140(v) of the CPRA defines service providers as a person or entity, operating in a for-profit capacity, that processes PI on behalf of a business. Section 1798.140(w) defines third parties as people or organizations that is not: (1) a business that collects PI from consumers, nor (2) a person or entity to whom the business discloses a consumer's PI.

a. Confusing treatment of providers of advertising services

Proposed Sections 7050(a) and (c) expand the definition of “service provider” to include “contractors,” while treating vendors that provide cross-context behavioral advertising services (services for online advertising where a business provides information about its own customers to a vendor to perform advertising on behalf of the business) a list of its own customers' email addresses to a vendor as “third parties.” Specifically, under proposed Section 7050(c), any entity providing cross-context behavioral advertising to a business is a third party and cannot be a service provider or contractor. A business should have the right to contract with a vendor to provide cross-context behavioral advertising services to the business and if the vendor meets all the other requirements to qualify as a service provider, the arrangement should not result in the business being deemed to engage in selling and/or sharing PI and thus required to offer an opt-out to consumers.

The CCPA should delete the new restriction.

b. Overly prescriptive contract requirements for third parties

The Proposed Regulations also impose new contract terms a business must include in its agreements with service providers and contractors. Under proposed Section 7053, failure to include all the required terms in an agreement with a firm that is acting as a service provider/contractor means that under the CPRA, the firm must be treated as a third party to which the business may be deemed to “sell” or “share” PI. The Proposed Regulations do not conform to the requirements in Section 1798.100(d) of the CPRA and cover obligations already addressed in the CPRA with respect to both businesses and service providers. There is no value in requiring businesses and service providers to restate these obligations as contract terms. Furthermore, a business's failure to comply with the new requirement to include all the prescribed terms in agreements with service providers/contractors would result in a harsh consequence on the business and the service providers – the business would be required to treat those services providers as a third party and if the business provides PI to such parties, that sharing would need to be treated as a sale or sharing of PI. Both consequences would have a significant compliance impact for both businesses and service providers.

The Proposed Regulations should be amended to mirror the requirements in Section 1798.100(d) of the CPRA.

c. Notice and Consent

Proposed Section 7053(a) imposes new contract requirements for third parties including, among other things, that third parties, authorized to collect PI from consumers through a business’s website, check for and comply with a consumer’s opt out preference signal to not sell or share their PI. Any third-party involvement in the collection of PI must be communicated to consumers with notice, and a failure to have an agreement in place forbids a third party from processing PI received from the business. The Proposed Regulations would require an impractical amount of contract remediation to updated executed contracts with this information and goes far beyond what was contemplated by the CPRA.

The CPPA should clarify whether a person could be acting as both a business and a service provider with respect to the same personal data. Additionally, the CPPA should clarify whether explicit consent from a consumer could make restrictions on the use of PI originally obtained in the service provider context moot. The CPPA should also clarify the meaning of “third parties,” as it remains undefined compared to the term “service providers.”

d. Audit and Due Diligence

Proposed Section 7051(e) explains that “[f]or example, depending on the circumstances, a business that never enforces the terms of the contract nor exercises its rights to audit or test the service provider’s or contractor’s systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.” The CPPA should provide guidance regarding what “circumstances” would justify a business not exercising its right to audit. For example, would certification or representation that the service provider’s parent/affiliates are a GLBA-regulated entity be a sufficient circumstance?

Proposed Section 7051(e) and Section 7053(e) states that “[w]hether a business conducts due diligence of its” service providers, contractors, or third parties “factors into whether the business has reason to believe” the service provider, contractor, or third party is using PI in violation of the CCPA/CPRA. Furthermore, both provisions cite an example where a business that never enforces the terms of its contract nor exercises its rights to audit or test might not be able to rely on the defense that it did not have reason to believe that the service provider, contractor, or third party intended to use the PI in violation of the CCPA.

A business’s right to avail itself of the CPRA liability shield for violations committed by a service provider, contractor, or third party should not be conditioned on its due diligence of that service third party, but on whether the business had actual knowledge or reason to believe that the violation would be committed *consistent with the CPRA*. A business may not be able to secure the contractual right to periodically audit or test the systems of each service provider,

contractor, or third party to which it discloses PI and should instead be permitted to rely on independent assessments or audit reports prepared by a third parties (e.g., SOC 2).

e. Business purpose disclosures in service provider/contractor/third party contracts (Section 7051(a)(2) and Section 7053)

Proposed Section 7051(a)(2) requires businesses to identify, in each service provider or contractor agreement, the specific business purpose for which PI will be processed on behalf of the business and specify that the business is disclosing the PI only for the limited and specified business purposes set forth in the contract between the parties. The Proposed Regulations note that a generic description referencing the entire contract is not acceptable, which goes beyond the CPRA's obligations.

The CCPA should remove this requirement because specifying the business purpose for each PI processing activity is impractical. Large companies with thousands of vendors would have to spend significant time and resources to identify and list in its contracts with every service provider each specific business purpose for which the business discloses PI to the service provider. Furthermore, many businesses enter into master agreements with vendors and service providers and the details of the specific products or services that are provided under the agreement are specified in other documents (such as purchase orders or statements of work) or other communications between the companies (such as emails). Failure to specify the specific business purposes and services in an agreement with a vendor should not disqualify the vendor from being a service provider/contractor under the CPRA

17. Authorized Agents (Sections 7001 and 7063)

The Proposed Regulations would also loosen safeguards for requests from authorized agents which would allow requests from those who are not acting as a power of attorney for the customer. SIFMA believes that eliminating these safeguards will encourage fraudulent activity.

The CCPA should reinstate these safeguards and the requirement that authorized agents be registered California business entities.

18. CPPA Audit (Section 7304)

Section 7304 of the Proposed Regulations states that the CPPA “can conduct an audit if the collection or processing of PI presents a significant risk to consumer privacy or security, or if the subject has a history of noncompliance with CCPA or any other privacy protection law.”

This provision is extremely broad and potentially outside of the scope of the CPPA's authority under the CPRA and therefore should be struck from the Proposed Regulations.

19. The Effective Date for the Rule Should be No Earlier Than January 2024

SIFMA encourages the CPPA to delay the effective date and enforcement of any final CPRA rules until January 2024. To date, only a portion of the CPRA regulations have been proposed and some critical and potentially complex regulations including automated

decisionmaking are still forthcoming. The operational challenges highlighted in this letter clearly indicate that additional time will be needed for companies to fully and responsibly implement new requirements given the complexity of the Proposed Regulations. Requiring businesses to attempt to comply prior to that time will lead to confusion and sloppy execution that will only harm businesses and consumers alike.

* * * * *

SIFMA and its members appreciate the opportunity to provide these comments and welcome further discussion. Please reach out to Melissa MacGregor at [REDACTED] with any questions or to schedule a meeting.

Sincerely,

[REDACTED]

Melissa MacGregor
Managing Director & Associate General Counsel

cc: Kim Chamberlain, Managing Director, State Government Affairs, SIFMA

From: **Gmail - Personal** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment.
Date: 19.08.2022 08:30:38 (+02:00)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

As a marketing and data privacy professional with over 30 years of experience I have witnessed both sides of the equation when it comes to the issue of regulating information and data privacy. On one side of the equation is the fundamental right of citizens to access and own their personally identifiable data. On the other side of the equation is the need for businesses to understand the need to adapt and follow Fair Information Practices. When the right balance is struck I believe that consumers get more relevant products and services and businesses become more efficient at using information and consumer data and eventually become more profitable.

I feel that certain CA businesses and those companies wishing to do business with CA residents should be held to a different standard when it comes data protection and usage. A clear example of where regulation is lacking and needs to be addressed is in the use of biometric and ethnic data, which are specially protected fields of data. I have worked in a field and with specific clients that have used this data in the past to create programs and strategies, that while on the surface appear innocuous, are in reality a potential opportunity for serious abuse and liability. CA has one of the most diverse ethnic populations in the world. We have an obligation to protect the right of all the CA citizens....especially those that are linguistically and culturally isolated within our own communities. The CCPA and the CPRA must address the data privacy regulation as it relates to the many ethnic populations throughout our State that need it most. Exploitation, lack of inclusion and discrimination have been part of the multicultural narrative for far too long and my only wish is that the CCPA and CPRA acknowledge that these communities exist in CA and deserve a voice that needs to be included in this crucial portion of the process. CA is the only state that has privacy as a fundamental right. I want to make sure that this applies to all of our CA residents equally.

Elcid Choi

Certified Privacy Professional: CIPP/US

From: **Kirk Arner** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 19.08.2022 19:02:16 (+02:00)
Attachments: CPPA Comment Furchtgott-Roth Arner FINAL 8-19.pdf (4 pages)
WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

To whom it may concern,

Please find attached for submission to the public record a comment written by Harold Furchtgott-Roth and Kirk R. Arner, in our individual capacities, regarding the rulemaking implementing the CPRA.

Respectfully submitted,

Kirk R. Arner

Legal Fellow
Center for the Economics of the Internet
Hudson Institute
[REDACTED]



August 19, 2022

VIA EMAIL (REGULATIONS@CPPA.CA.GOV)

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

Re: CPPA Rulemaking Implementing CPRA

Harold Furchtgott-Roth is a senior fellow at the Hudson Institute and director of the Center for the Economics of the Internet at the Hudson Institute. Kirk R. Arner is a legal fellow at the Center for the Economics of the Internet. In our individual capacities, we respectfully submit these comments on the above-captioned matter. The views reflected herein are our own and do not necessarily represent those of any other individual or institution.

We have reviewed the proposals for regulations (the “Proposed Regulations”) implementing the California Privacy Rights Act (“CPRA”), as well as the economic impact assessment (“EIA”) provided by the California Privacy Protection Agency (“CPPA”) and the supporting materials provided by Berkeley Economic Advising and Research (“BEAR”). In our opinion, the EIS and BEAR Report routinely underestimate costs that would be incurred by firms and consumers as a result of the Proposed Regulations. Its conclusion that the Proposed Regulations would result in compliance costs of \$127.60 per company are indefensible from an economic perspective.

Among other things, the BEAR Report does not analyze informed measures of costs and benefits for each proposed regulation. While each of the many proposed regulations is likely a “major regulation,” there is no detailed or formal cost-benefit analysis conducted for any of them. As discussed in greater detail below, frequently in its place is a simple assertion that affected entities will incur \$0 of costs or 0 hours of labor to comply with many of the proposed regulations.¹

II.

The necessary elements for cost-benefit analyses are missing in the BEAR Report, and thus it does not constitute a proper cost-benefit analysis. Although it is entitled “Notes on

¹ California Consumer Privacy Agency Notes on Economic Impact Estimates for Form 399 at 20-21 (“BEAR Report”). *See also id.* at 1-2 (“[W]e determined that most of the potential regulatory ‘deltas’ we had identified were reiterat[ing] the existing CPRA amendments or existing regulations from the CCPA.”).

Economic Impact Estimates for Form 399,” the BEAR Report addresses only a few of the costs associated with the Proposed Regulations and virtually none of their possible benefits.²

Thus, even if the cost analysis of the report was complete—and we explain below why it is not—the report provides no basis to assess whether the costs of the proposed regulations are greater or lesser than the associated benefits. This makes the exercise of cost-benefit analysis impossible: that is, comparing the costs and benefits of a given item to determine whether the costs of that item outweigh the benefits.³

There is an additional, more specific flaw in the BEAR Report’s cost-benefit analysis. The BEAR Report specifically identifies existing CCPA regulations, as well as Europe’s GDPR, in determining the relevant baseline for cost-benefit analysis.⁴ But the proposed new CCPA regulations are not identical to existing CCPA rules or GDPR rules, and consequently, even firms that are currently GDPR-compliant and CCPA-compliant would have additional regulatory costs.⁵ Moreover, California’s Proposed Regulations create new enforcement mechanisms, even for existing rules. Thus, even firms that were already GDPR and CCPA-compliant would face new types of enforcement with which they would need to comply. Additionally, regarding the GDPR comparison, because of litigation risk, compliance costs in the U.S. are typically much higher than in Europe; thus, the comparison is flawed.

III.

Out of dozens of regulation changes, the BEAR Report reviewed only three specific changes when considering potential costs.⁶ Out of these three, the Report concluded that only two caused firms to incur costs.⁷

In contrast, Washington Legal Foundation (“WLF”) found over 40 instances where firms would incur costs.⁸ We largely agree with WLF’s analysis in this regard. We also share WLF’s concern regarding potential agency influence over the BEAR Report’s conclusions.⁹

² Section B of the Report, entitled “Estimated Costs,” does very briefly touch on potential benefits. *Id.* at 12-16. However, the only benefits considered are benefits to consumers, and only those connected to proposed §7012(e)(6) and §7026(g). Regardless, the overall conclusion of the report is that there will be zero benefit to consumers if the proposed rules are enacted. *Id.* at 16.

³ Tim Stobierski, *How to Do a Cost-Benefit Analysis & Why It’s Important*, Harvard Business School Online (Sept. 5, 2019), <https://online.hbs.edu/blog/post/cost-benefit-analysis> (“If the projected benefits outweigh the costs, you could argue that the decision is a good one to make. If, on the other hand, the costs outweigh the benefits, then a company may want to rethink the decision or project.”).

⁴ BEAR Report at 1.

⁵ See Comments of Washington Legal Foundation at 8-29, available at <https://www.wlf.org/2022/08/19/publishing/counsels-advisories/california-proposed-privacy-regulations-would-impose-significant-compliance-costs-on-business/>. See also section V, *infra*.

⁶ BEAR Report at 12-16.

⁷ *Id.* at 16.

⁸ Comments of Washington Legal Foundation at 8-29.

⁹ *Id.* at 6; BEAR Report at 1-2 (“In many sections [of the proposed rules], we initially believed there could be a regulatory impact. However, upon further discussion with the California Privacy Protection Agency (Agency) and supporting staff, we determined that most of the potential regulator “deltas” we had identified were reiterat[ing] the existing regulations from the CCPA.”).

IV.

The BEAR Report estimates that 79,010 firms will be impacted by the proposed regulation changes.¹⁰ It estimates 26,102 of these firms will be impacted because they meet a revenue threshold of \$25 million as established by the rules.¹¹ However, this analysis fails to consider those firms that do not currently have revenues of \$25 million+, but nevertheless plan to grow. In anticipation of one day meeting that threshold, firms that today have revenues under that threshold will nevertheless begin to comply with the rule changes. Consequently, the BEAR Report's estimate of firms incurring costs, as measured by revenue, is underinclusive.

In contrast to firms, the BEAR Report does not even attempt to estimate the number of consumers affected by the Proposed Regulations. Additionally, the Report, when concluding that the regulations will not cause any costs to consumers, does not consider the likelihood that California firms would pass along to consumers the regulatory costs of the new regulations, as a cost of doing business, in the form of higher prices or lower quality of service. Thus, there *would* be costs to consumers as a result of the proposed changes, despite the BEAR Report's assertion to contrary.¹²

V.

The BEAR Report should have considered the effect of the Proposed Regulations on firms and consumers outside of California. Many firms not subject to California enforcement would seek to comply with the rules, either as a consequence of doing business in California, or in anticipation of doing future business in California. Just as some California firms have incurred costs to become GDPR compliant, so too some firms outside of California would incur costs to become compliant with the proposed new CCPA regulations. As explained above, the costs faced by these firms would likely be passed along to consumers as a cost of doing business. The BEAR Report fails to capture any of these costs—either for firms or for consumers.

VI.

As discussed above, the BEAR Report routinely underestimates costs that would be incurred by firms and consumers as a result of the Proposed Regulations. The BEAR Report does not measure identifiable costs associated with the Proposed Regulations—including at least the following: (1) costs associated with changing business practices such as monitoring and recording inaccurate information; (2) administrative costs of complying with new regulations such as audit and reporting requirements; (3) insurance costs to insure against the risk of unknown compliance costs; and (4) litigation costs from disputes both with state government agencies as well as consumers. Instead, the BEAR Report routinely asserts that firms will incur \$0 of cost or 0 hours of labor for so-called “regulatory deltas.”¹³ In total, the Report estimates

¹⁰ BEAR Report at 8.

¹¹ *Id.* at 5-6, 8.

¹² *Id.*

¹³ *Id.* at 20-21.

that compliance with the Proposed Regulations will only take 1.5 hours of labor and cost affected entities a mere \$127.60.¹⁴

These estimates are indefensible. WLF's comments identify over 40 sections of the Proposed Regulations where this occurs, and we generally agree with them.¹⁵ WLF's comments include two particularly stand-out examples. The first, proposed regulation § 7004(a)(4)(A), would require firms to review the terminology used in consent mechanisms to avoid supposedly "shaming" statements such as "No, I don't want to save money."¹⁶ In another, proposed regulation § 7023(i), firms would be required to provide consumers with the name of a source of inaccurate information about the consumer, in response to a written petition from the consumer alleging an inaccuracy.¹⁷ In neither of these instances does the BEAR Report find that there would be any amount of work or cost incurred whatsoever by the firm to come into compliance. This analysis is clearly wrong.

Sincerely,

/s/ Harold Furchtgott-Roth
 Harold Furchtgott-Roth
Senior Fellow
Center for the Economics of the Internet
Hudson Institute

/s/ Kirk R. Arner
 Kirk R. Arner
Legal Fellow
Center for the Economics of the Internet
Hudson Institute

¹⁴ *Id.* at 12, 15.

¹⁵ Comments of Washington Legal Foundation at 8-29.

¹⁶ *Id.* at 10.

¹⁷ *Id.* at 16.

From: **Crenshaw, Jordan** [REDACTED]
To: **Regulations** <Regulations@cpga.ca.gov>
Subject: CPPA Public Comment
Date: 19.08.2022 21:10:28 (+02:00)
Attachments: 220819_Comments_CPRARegulationsNOPR_CPRA.pdf (7 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

To Whom It May Concern:

Please find attached comments from the U.S. Chamber of Commerce regarding the CPPA's request for public comments on its rules implementing the CPRA.

Thank you.

Best,

Jordan Crenshaw

Vice President

Chamber Technology Engagement Center

U.S. Chamber of Commerce
[REDACTED]



U.S. Chamber of Commerce

www.americaninnovators.com

@uschambertech



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://cpa.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 CPRPA which only requires notice if personal information and sensitive personal information are used for additional purposes “that are incompatible with the disclosed purpose for which the personal information was collected.”⁴ In addition, the proposed regulation ignores the secondary use standard in the CPRPA, 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 CPRPA 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 CPRPA, 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 CPRPA does not authorize the CPPA to legislate this new mandate.

The CPRPA 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 CPRPA 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 spirit 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 opposed¹⁰ 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 begin 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 [REDACTED] or [REDACTED].

Sincerely,

[REDACTED]

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

From: **Craig Erickson** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
Subject: CPPA Public Comment
Date: 20.08.2022 13:32:13 (+02:00)
Attachments: CPPA Public Comment.txt (1 page)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

I am a California Consumer who RSVP'd to attend and speak at the Public Hearing held in Oakland.

Attached is my written comment in plain text format. I was unable to find in the proposed regulations any mention of penalties for intentionally misleading consumers about whether a business does comply with the CCPA/CPRA or if it is exempt. If I could find out in advance if my comment is not in scope for the meeting, I will decline commenting in person.

Craig Erickson
Data Protection Officer
PrivacyPortfolio
[REDACTED]

My name is Craig Erickson, and I live in [REDACTED], California.

As a California Consumer who has exercised my CCPA rights with hundred of businesses,

I sometimes encounter businesses who publically state or imply that they are CCPA-compliant or will honor CCPA requests, but then also claim they are exempt when I submit a verifiable consumer request to them or file a consumer complaint with the Attorney General.

My question is:

If I want to file a complaint against an entity that abuses the CCPA's exemptions, does it fall under the CPPA's purview, or would my grievance be better handled through the FTC?

Craig Erickson,
a California Consumer

From: **Sebastian Zimmeck** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 21.08.2022 23:33:22 (+02:00)
Attachments: California_CCPA_Comments.pdf (2 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Good evening,

Please find attached my comment. Thank you for your consideration!

Best regards,

Sebastian

We launched [Global Privacy Control](#)
[privacy-tech-lab](#), Wesleyan University

**Mathematics and Computer Science Department**

265 Church Street
Middletown Connecticut 06459
860 685 2620 Fax: 860 685 2571
<https://www.wesleyan.edu/mathcs/>

Sebastian Zimmeck
Assistant Professor of Computer Science

August 21, 2022

**Via Email**

California Privacy Protection Agency

Attn: Mr. Brian Soublet

2101 Arena Blvd.

Sacramento, CA 95834

Dear Mr. Soublet,

I would like to comment on the regulations to implement the Consumer Privacy Rights Act of 2020. I am an assistant professor of computer science at Wesleyan University, where I direct the privacy-tech-lab [1]. Together with my students and collaborators I am working on privacy-enhancing technologies to enable people on the Internet to exercise their privacy rights effectively and efficiently. I am a co-creator of Global Privacy Control (GPC) [2], by which people can send requests to websites, apps, and other services to not sell or share their personal information with third parties. I would like to comment on §7025 Opt-Out Preference Signals.

1. Clarify in the regulations that selecting privacy-preserving products or product versions demonstrates sufficient intent to opt out.

If people select privacy-preserving products, e.g., install Brave, Firefox, or DuckDuckGo Privacy Essentials, it can be unambiguously inferred that they want to opt out from the sharing and sale of personal information, cross-contextual advertising, behavioral profiling, and similar data monetization practices. The same is true for privacy-focused versions of a general product. Requiring the consumer in these instances to re-confirm their intent would be detrimental to the usability of opt-out preference signals and not serve any additional purpose. Thus, it would be preferable to clarify this point in the regulations as well.

2. Further clarify in the regulations that the validity of a request to opt out of the sale or sharing of personal information does not require authentication or submission of additional information.

Whatever information a website, app, ad network, etc. uses to authenticate a user for purposes of data collection should also suffice for the authentication when exercising an opt out right. For example, if a website starts targeting a user simply upon visiting the site, all it should take for the user to opt out is to continue visiting the site with the opt-out preference signal enabled. The current practice of some sites to require additional information, e.g., name and email address, does not



facilitate the opt out if this information was not known by the site in the first place. Thus, for example, if a cookie ID is used to identify a particular user, all it should take for the site to facilitate the opt out is to associate that cookie ID with an opt out flag. It is not necessary to require authentication or additional information for that purpose. Any usability obstacles risk that the opt out right will not be effective. Thus, there is a risk that sections such as §7025(c)(2) (“However, a business may provide the consumer with an option to provide additional information”) can be misused to degrade the usability of opt-out preference signals if sites misuse that option, for example, by extensively displaying opt out banners. It would be worthwhile to clarify that additional information can only be asked for for purposes of extending the opt out, for example, from one browser to all browsers a consumer is using.

3. Respecting opt-out preference signals must remain mandatory.

The single most important factor for broadly enabling people to exercise their opt out rights is to require recipients of opt-out preference signals to follow those. The experiences with the Do Not Track signal, for which the California Online Privacy Protection Act only requires disclosure of whether or not it will be followed, demonstrate how crucial the mandatory nature of privacy preference signals is. Thus, it is critical that the regulations remain clear on this point.

4. Implementing GPC is technically easy and various tools are available for website operators to enable people to opt out.

Some site operators express concern that GPC is challenging to implement. However, that is not the case. GPC is based on basic web technologies that are easy to implement. Various implementation guidelines are available online and many consent management platforms offer support for GPC. I worked with various site operators of sites big and small and helped them implement GPC. If there is a challenge, it is one of switching to a privacy-preserving business model.

5. Consider pointing to opt-out preference signal specifications that satisfy the requirements of the regulations.

It would be valuable for website operators to know which opt-out preference signals satisfy the requirements of the law. To that end, you could provide a website resource or otherwise provide such clarification.

Thank you for your efforts in moving privacy forward and the opportunity to comment. I am available for further questions and clarifications.

Sincerely,



Sebastian Zimmeck

[1] privacy-tech-lab, <https://www.privacytechlab.org/>

[3] Global Privacy Control, <https://globalprivacycontrol.org/>

From: **Abigail Wilson** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
CC: **Kate Goodloe** [REDACTED]
Subject: CPPA Public Comment BSA | the Software Alliance
Date: 22.08.2022 15:09:41 (+02:00)
Attachments: 2022.8.22 - BSA Comments on Draft CCPA Regulations - Final.pdf (13 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Hello,

Please find BSA | the Software Alliance's comments on the draft CCPA Regulations attached.

Thank you,





BSA | The Software Alliance

Submission to the California Privacy Protection Agency on Proposed Regulations Implementing the Consumer Privacy Rights Act of 2020

BSA | The Software Alliance appreciates the opportunity to submit comments regarding the proposed regulations (“Proposed Regulations”) implementing the California Privacy Rights Act of 2020 (“CPRA”), which amended the California Consumer Privacy Act (“CCPA”). We appreciate the California Privacy Protection Agency’s (“CPPA’s”) work to address consumer privacy and to develop regulations that protect the privacy of Californians’ personal information.

BSA is the leading advocate for the global software industry before governments and in the international marketplace.¹ Our members are enterprise software companies that create the technology products and services that power other businesses. They offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, and collaboration software.

Businesses entrust some of their most sensitive data – including personal information – with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members’ operations. Indeed, many businesses depend on BSA members to help them better protect privacy and our companies compete to provide privacy-protective products and services. BSA members recognize that companies must earn consumers’ trust and act responsibly with their data, and their business models do not depend on monetizing users’ personal information.

Our comments focus on three aspects of the Proposed Regulations:

1. **Role of Service Providers.** The CCPA recognizes that businesses and service providers play different roles in protecting consumer privacy – and are therefore assigned different obligations under the statute based on their different relationships with consumers. Although many aspects of the Proposed Regulations reflect these unique roles, we strongly suggest revising two areas that risk upsetting the careful statutory assignment of responsibilities between businesses and service providers. First, the Proposed Regulations should be revised to clarify a service provider’s role in responding to consumer rights requests – including recognizing that service providers may fulfill their role of assisting a business by creating a tool that enables the business to respond to consumer rights requests for data held by the service provider. Second, the Proposed Regulations’ contractual requirements for service

¹ BSA’s members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, Prokon, PTC, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

providers should be limited to the requirements set forth in the statute, which ensures businesses and service providers can tailor agreements to the context of their relationship. In addition, we recommend the Proposed Regulations retain helpful examples that make clear that service providers can combine personal information to improve services offered at scale.

2. **Global Opt-Out Mechanism.** The CPPA is tasked with issuing regulations to implement a global opt-out mechanism. Although we believe the CCPA is best read to permit (but not require) companies to honor requests submitted through global opt-out mechanisms, it is critical that any opt-out mechanism recognized by the Proposed Regulations (whether mandatory or voluntary) be interoperable with mechanisms recognized by other states and function in practice. Accordingly, the Proposed Regulations should account for potentially conflicting opt-out requirements and the CPPA should work with other state regulators to ensure that opt-out requirements are consistent across state lines. We also strongly recommend the CPPA prioritize addressing practical issues around how any opt-out mechanism will be implemented, revise the Proposed Regulations to address specific topics set out in the statute, and promote consumer education about the role of opt-out mechanisms and their limits.
3. **Agency Audits.** The Proposed Regulations provide few details on the agency's audit authority – and create few guardrails to ensure the agency exercises its audit authority in a manner that does not inadvertently create privacy and security risks. We recommend revising the Proposed Regulations to create such guardrails, including limiting the use of on-site audits, which can present significant privacy and security risks not accounted for in the Proposed Regulations. Accordingly, the Proposed Regulations should explicitly state that audits will be conducted when there is a “significant risk” of violation of the CPPA and that such audits will be conducted remotely (absent specific circumstances warranting an on-site audit).

I. Role of Service Providers

Although the CCPA primarily focuses on businesses, which “determine[] the purposes and means of the processing of consumers’ personal information,”² the statute also recognizes that businesses may engage service providers to “process[] personal information on behalf of a business.”³ Service providers must enter into written contracts with businesses they serve, limiting how the service provider can retain, use, and disclose personal information provided to them by a business. In this way, the CCPA ensures that personal information is subject to statutory protections both when a business collects and processes a consumer’s personal information itself, and when that business hires service providers to process a consumer’s personal information on its behalf. The statute also recognizes the distinct roles of businesses and service providers by assigning them different obligations based on their different roles in handling consumers’ personal information.

A. The Proposed Regulations Should Be Revised to Reflect the Role of Service Providers in Responding to Consumer Rights Requests under the CCPA.

Under the CCPA, businesses are assigned the responsibility of responding to consumers’ requests to access, correct, and delete their personal information. This is consistent with all other state consumer privacy laws and leading data protection laws worldwide, which place

² Cal. Civ. Code § 1798.140(d)(1).

³ Cal. Civ. Code § 1798.140(ag)(1).

this obligation on companies that decide how and why to collect consumers' data – rather than the service providers acting on behalf of such companies. For example, under the CCPA consumers may:

- Access personal information, by “request[ing] that a business that collects personal information about the consumer disclose” certain information to the consumer, including the “specific pieces of personal information it has collected about that consumer.”⁴
- Correct personal information, by “request[ing] that a business that maintains inaccurate personal information about the consumer [] correct that inaccurate personal information.”⁵
- Delete personal information, by “request[ing] that a business delete any personal information about the consumer which the business has collected from the consumer.”⁶

The CCPA recognizes that service providers are not required to respond to consumer rights requests submitted to them by individuals – and for good reason. Under the statute, consumers are to exercise their rights by going to the consumer-facing company they interact with – the business – instead of forcing consumers to identify the dozens or more service providers that each consumer-facing business may utilize. This is both efficient for consumers and an important reflection of the role of service providers, which process data on behalf of other businesses and generally do not interact with individual consumers. Indeed, a service provider often lacks the information needed to identify an individual who submits a rights request – and does not make the types of decisions required to fulfill a request, which require determining the data sets to be provided to a consumer in response to a request to access personal information, assessing whether information a consumer seeks to correct is inaccurate, and analyzing whether information a consumer seeks to delete is subject to a statutory exception, such as when data is subject to a legal hold. Under the statute:

- For deletion requests, a service provider is “not [] required to comply with a deletion request submitted by the consumer directly to the service provider . . . to the extent the service provider . . . has collected, used, processed, or retained the consumer’s personal information in its role as a service provider or contractor to the business.”⁷
- For access requests, a service provider “shall not be required to comply with a verifiable consumer request [for access] received directly from a consumer or a consumer’s authorized agent” but instead shall “provide assistance to [the] business” in responding to that request.⁸
- For requests to limit the use of sensitive personal information, a service provider is “only required to limit its use of sensitive personal information received pursuant to a written contract with the business in response to instructions from the business and only with respect to its relationship with that business.”⁹

Of course, consumer rights created by the CCPA must be meaningful in practice – including when a business engages service providers to process personal information on its behalf. That is why the CCPA creates a clear set of obligations for service providers when consumer rights requests involve data held by a service provider. Under the statute, service providers are to either: (1) respond to consumer rights requests sent to the service provider by a

⁴ Cal. Civ. Code § 1798.110(a) (emphasis added).

⁵ Cal. Civ. Code § 1798.106(a) (emphasis added).

⁶ Cal. Civ. Code § 1798.105(a) (emphasis added).

⁷ Cal. Civ. Code § 1798.105(c)(3).

⁸ Cal. Civ. Code § 1798.130(a)(3)(A).

⁹ Cal. Civ. Code § 1798.121(c).

business, or (2) enable the business to respond to those requests. The statute's clear approach – and its recognition of two ways that service providers may assist businesses in responding to requests – is critical to ensuring that companies can fully and efficiently respond to consumer rights requests. Under the CCPA:

- For a deletion request, the role of a service provider is to “cooperate with the business in responding to a verifiable consumer request, and at the direction of the business, [to] delete, or enable the business to delete” information.¹⁰
- For access and correction requests, the role of a service provider is to “provide assistance to a business,” including “providing to the business the consumer’s personal information in the service provider[s] . . . possession,” “correcting inaccurate information,” or “enabling the business to do the same.”¹¹

The CCPA therefore recognizes that service providers may either execute consumer rights requests directly or enable a business to do so. This second option – enabling the business to respond to requests – is critical to ensuring that companies can respond to large volumes of consumer rights requests efficiently and effectively. For example, many service providers offer services at scale that are used by hundreds of business customers, each of which may receive thousands of consumer rights requests. Service providers can help their business customers efficiently respond to those requests by creating scalable tools that the business can use to access, correct, and delete information held by the service provider – and thereby establish processes for assessing and responding to a large volume of requests. Without such scalable tools, businesses would be forced to forward large volumes of consumer rights requests to service providers one-by-one. That can create a long backlog of requests, slowing down response times and creating the potential for long back-and-forth communications between the two companies about whether each request should be executed.

The Proposed Regulations do not fully account for – and at times contradict – the statute’s clear recognition that service providers can fulfill their obligation to assist businesses in responding to consumer rights request by enabling the business to respond to those requests. For example, for correction requests Section 7023 of the Proposed Regulations appropriately recognizes that the role of a service provider is to either “comply with the business’s instructions to correct the personal information or enable the business to make the corrections.”¹² However, at least three provisions in the Proposed Regulations do not acknowledge the statute’s recognition that service providers can “enable” a business to respond to requests and instead could be read to presume that the only role for a service provider is to respond to each individual consumer rights request forwarded to it by a business. Those provisions are:

- Section 7022(c), which sets out obligations for service providers after being notified of a consumer’s deletion request.¹³ This provision disregards the clear statutory language stating a service provider may fulfill its obligation to assist the business either by deleting the relevant personal information “or [by] enabl[ing] the business to delete” that information.¹⁴
- Section 7024(i), which sets out obligations for service providers for requests to access information. Although this provision recognizes the role of a service provider is to “provide assistance to the business” in responding to requests, it goes on to

¹⁰ Cal. Civ. Code § 1798.105(c)(3) (emphasis added).

¹¹ Cal. Civ. Code § 1798.130(a)(3)(A) (emphasis added).

¹² Proposed Regulations § 7023(c) [hereinafter Prop. Reg.] (emphasis added).

¹³ Prop. Reg. § 7022(c).

¹⁴ Cal. Civ. Code § 1798.105(c)(3).

state that a service provider is to assist a business “including by providing the business the consumer’s personal information it has in its possession that it obtained as a result of providing services to the business,” without clearly stating the service provider may fulfill its obligation by enabling the business to access the information.¹⁵

- Section 7051(a)(10), which sets out new requirements for contracts between businesses and service providers, including requiring a business to inform a service provider of “any consumer request made pursuant to the CCPA that they must comply with, and provide the information necessary for the service provider . . . to comply with the request.”¹⁶ This provision appears to start from the assumption that service providers will directly respond to consumer rights requests – disregarding the clear statutory language that service providers may fulfill their obligations by enabling a business to respond to such requests.

Recommendation: The Proposed Regulations should be revised to align with the CCPA’s clear recognition that service providers may fulfil their role in handling consumer rights requests by either executing those requests or by *enabling the business* to do so. We strongly recommend three revisions:

1. For deletion requests, Section 7022 should be revised in two ways:
 - First, 7022(c) should be revised to state: “A service provider or contractor shall [either enable the business to comply with the consumer’s request to delete their personal information or, upon notification by the business](#) comply with the consumer’s request to delete their personal information by”
 - Second, 7022(b)(2) should be revised to state that a business is to comply with a consumer’s request to delete personal information by: “[Either deleting personal information processed on behalf of the business by its service providers or contractors if enabled to so do in accordance with 7022\(c\), or notifying the business’s service providers or contractors to delete from their records the consumer’s personal information obtained in the course of providing services; and](#)”
2. For requests to access, Section 7024(i) should be revised to state: “A service provider or contractor shall provide assistance to the business in responding to a verifiable consumer request to know, including by providing the business the consumer’s personal information it has in its possession that it obtained as a result of providing services to the business, [or by enabling the business to access that personal information.](#)”
3. Finally, Section 7051(a)(10) should be eliminated, because it presumes that service providers will respond to requests one-by-one rather than enabling businesses to comply directly. If the provision is retained, however, it should be revised to reflect that a service provider may either enable a business to respond to requests or may respond to individual requests upon notice by the business. For example, it could be revised to state: “Require the [service provider or contractor to either enable the business to comply with consumer requests made pursuant to the CCPA or require the](#) business to inform the service provider or contractor of any consumer request made pursuant to the CCPA that they must

¹⁵ Prop. Reg. § 7024(i).

¹⁶ Prop. Reg. § 7051(a)(10).

comply with, and provide the information necessary for the service provider or contractor to comply with the request.”

B. The Proposed Regulations Should Not Create Contractual Obligations Beyond Those Set out in the CCPA’s Text.

Two provisions of the CCPA create statutory requirements for contracts between businesses and service providers. First, Section 1798.100(d) requires businesses that engage service providers to enter into agreements with such providers. Second, in the CCPA’s definition of the term “service provider” in Section 1798.140(ag), the statute requires that service providers be subject to contractual limitations in handling data on behalf of businesses.¹⁷ Beyond these requirements, the CCPA allows businesses and service providers to craft their own contracts. This is important, because it allows the parties to evaluate the nature of their relationship, the information to be processed, and the role of the service provider, and tailor the agreement accordingly.

However, the Proposed Regulations create contractual requirements that go beyond those in the statute, in at least three ways.

1. Section 7051(a)(7) of the Proposed Regulations appears to conflate two separate provisions of the CCPA.

First, Section 7051 of the Proposed Regulations states that contracts between a business and a service provider must:

Grant the business the right to take reasonable and appropriate steps to ensure that service provider . . . uses the personal information that it received from, or on behalf of, the business in a manner consistent with the business’s obligations under the CCPA and these regulations. Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider’s system and regular assessments, audits, or other technical and operational testing at least once every 12 months.¹⁸

This provision combines two separate statutory requirements, in a manner that can be read to impose additional contractual obligations beyond those in the statute. The first part of this provision is based on CCPA Section 1798.100(d)(3), which states that a contract

¹⁷ Under Section 1798.140(ag), a service provider must process data pursuant to a contract that prohibits it from:

- “[S]elling or sharing the personal information[.]”
- “Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract for the business, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract with the business, or as otherwise permitted by [the CCPA].”
- “Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business.”
- “Combining the personal information that the service provider receives from, or on behalf of, the business with [other] personal information . . . provided that the service provider may combine personal information to perform any business purpose as defined in regulations [to the CCPA]” other than in connection with cross-context behavioral advertising, or marking and advertising for consumers who exercised their opt-out rights.

This provision goes on to note that “the contract may, subject to agreement with the service provider, permit the business to monitor the service provider’s compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.”

¹⁸ Prop. Reg. § 7051(a)(7).

between a service provider and a business must “[g]rant[] the business rights to take reasonable and appropriate steps to help ensure that the . . . service provider . . . uses the personal information transferred in a manner consistent with the business’ obligations under this title.”¹⁹ The second part is based on the CCPA’s definition of service provider in 1798.140(ag)(1)(D), which states that the contract “may, subject to agreement with the service provider, permit the business to monitor the service provider’s compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.”²⁰

Section 7051 of the Proposed Regulations combines these two statutory provisions, in a manner that suggests several contractual commitments may be mandatory – even though the CCPA clearly makes those commitments permissive rather than required. Specifically, Section 7051 could be read to suggest that the compliance monitoring steps set out in the CCPA’s definition of a service provider (as actions that may be taken “subject to agreement with the service provider”) could be viewed as required provisions of a service provider contract. This is not consistent with the text of the statute, which allows parties to reach agreements that determine which “reasonable and appropriate steps” are suitable in the context of a given service. The Proposed Regulations should be revised to avoid suggesting otherwise.

Recommendation: Section 7051(a)(7) of the Proposed Regulations should be revised to delete this ambiguous language, so that the provision states that contracts between businesses and service providers shall: “(7) Grant the business the right to take reasonable and appropriate steps to ensure that service provider or contractor uses the personal information that it received from, or on behalf of, the business in a manner consistent with the business’s obligations under the CCPA and these regulations. ~~Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider’s system and regular assessments, audits, or other technical and operational testing at least once every 12 months.~~”

2. Section 7051(a)(2) of the Proposed Regulations appears to require specificity in contracts that goes beyond the CCPA’s requirements.

Second, Section 7051(a)(2) of the Proposed Regulations requires service provider contracts to “[i]dentify the specific business purpose(s) and service(s) for which the service provider . . . is processing personal information . . .”²¹ It goes on to state that “[t]he business purpose or service shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.”²²

This requirement to provide “specific” business purposes goes beyond the requirements of the CCPA. The statute affords service providers and businesses greater flexibility to identify the business purposes for which a service provider may process personal information – including by referring to their contract as appropriate. This flexibility is important because it helps to avoid the need for businesses and service providers to continually amend and re-negotiate data processing terms as new services are added to a contract. The requirement to provide each “specific” business purpose is not necessary to ensure that data remains protected when processed by a service provider, because the service provider is already required to handle data in line with the contract with the business and subject to safeguards

¹⁹ Cal. Civ. Code § 1798.100(d)(3).

²⁰ Cal. Civ. Code § 1798.140(ag)(1)(D) (emphasis added).

²¹ Prop. Reg. § 7051(a)(2).

²² *Id.*

set out in the statute. Requiring greater specificity about the “specific” purposes for processing covered by a contract is also unlikely to create a substantial benefit to consumers, given the statutory limits already imposed on service providers.

Recommendation: Section 7051(a)(2) of the Proposed Regulations should be revised to be consistent with the CCPA, as follows: “Identify the specific business purpose(s) ~~and service(s)~~ for which the service provider or contractor is processing personal information on behalf of the business and specify that the business is disclosing the personal information to the service provider or contractor only for the limited and specified business purpose(s) set forth within the contract. ~~The business purpose or service shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.~~”

3. Section 7051(a)(8) of the Proposed Regulations goes beyond the statute in creating a specific time period for notifying businesses about compliance.

Under the CCPA, service provider contracts must include a requirement for the service provider to inform the business if it can no longer comply with its obligations under the CCPA.²³ The statute is silent on the time period for the service provider to issue such notice. By not prescribing a specific time for notification, businesses and service providers are permitted to contractually determine the appropriate approach to notice, taking into account the specific context of each business-service provider relationship. However, the Proposed Regulations would eliminate this flexibility and instead require notice “no later than five business days after [the service provider] makes a determination that it can no longer meet its obligations under the CCPA and these regulations.”²⁴

To ensure that service providers have adequate time to correct temporary issues and gather the information necessary for notice, Section 7051(a)(8) should be revised to eliminate a specific time period for notice – as consistent with the CCPA.

Recommendation: Section 7051(a)(8) should be revised to eliminate a specific time period for notice, as follows: “Require the service provider or contractor to notify the business ~~if no later than five business days after~~ it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.”

C. The Proposed Regulations Should Continue to Clearly Recognize the Ability of Service Providers to Combine Personal Information.

Under the CCPA, a service provider is to be subject to a contract with certain limitations. These include prohibiting the service provider from combining certain types of personal information – but the statute expressly recognizes that service providers may combine personal information to perform business purposes under the statute, other than cross context behavioral advertising. Under the statute, the CPPA is required to issue regulations “further defining the business purposes for which service providers . . . may combine consumers’ personal information obtained from different sources.”²⁵ Section 7050 of the Proposed Regulations does so, including through Section 7050(b)(4), which recognizes that a service provider can use personal information to build or improve the quality of its services as long as it does not use the personal information to perform services on behalf of another person.

²³ Cal. Civ. Code § 1798.100(d)(4).

²⁴ Prop. Reg. § 7051(a)(8).

²⁵ Cal. Civ. Code § 1798.185(a)(10).

This issue is critical to service providers that offer services to business customers at scale, which rely on data collected across those business customers to protect and secure those services, facilitate research, develop artificial intelligence systems, improve their services, and serve multiple businesses working together. For example, an email service provider may be able to proactively identify accounts at risk of being hacked by analyzing and combining personal information associated with those accounts in the context of a particular threat actor. As another example, multiple academic institutions might ask a cloud storage provider to store research data from each of them – including personal information – in one joint repository. Indeed, there are many purposes for which service providers may combine personal information in a manner that benefits consumers, and are entirely unrelated to monetization.

Section 7050(b)(4) recognizes that service providers can retain, use, or disclose personal information to improve services offered at scale – and includes two illustrative examples that clarify how the Proposed Regulations are intended to work in practice. We strongly recommend the Proposed Regulations retain these examples, which clearly recognize that a service provider that offers services to multiple business customers can analyze data from each of those customers to “improve its services and offer those improved services to everyone.”

Recommendation: We strongly recommend the Proposed Regulations retain the illustrative examples in Section 7050(b)(4).

II. Global Opt-Out Mechanism

A. Any Global Opt-Out Mechanism Should be Consistent and Interoperable with Mechanisms Recognized by Other State Privacy Laws.

BSA believes that consumers should have clear and easy-to-use methods for exercising new rights given to them by any privacy law.

Under the CCPA, the CPPA is tasked with issuing regulations that define the requirements and technical specifications for an opt-out preference signal that indicates a consumer’s intent to opt out of the sale or sharing of that consumer’s personal information, and to limit the use or disclosure of the consumer’s sensitive personal information. These regulations are to be “updated from time to time” and, among other requirements, are not to conflict with “other commonly used privacy settings or tolls that consumers may employ.”²⁶ In our view, the best reading of the CCPA, as amended by CPRA, is that any such opt-out mechanism is permitted, but not required, by the statute.²⁷ The Proposed Regulations, however, contemplate a mandatory opt-out preference mechanism and require businesses to process opt-out preference signals meeting the requirements in Section 7025 of the Proposed Regulations.

Regardless of whether a global opt out mechanism is permissive or required, it is critically important that the mechanism be interoperable with other states’ privacy laws and any similar mechanisms recognized by other states. In particular, the new consumer privacy laws in Colorado and Connecticut create clear statutory requirements for companies to

²⁶ Cal. Civ. Code § 1798.185(a)(19)(A)(iv).

²⁷ See Cal. Civ. Code 1798.135(b)(3) (stating that a business that complies with provisions for providing consumers certain opt-out links “is not required to comply with subdivision (b) [governing opt-out preference signals]. For the purpose of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b)”).

honor global opt-out mechanisms starting July 1, 2024 (for Colorado) and January 1, 2025 (for Connecticut). We strongly recommend the CPPA engage with regulators in those states to ensure that any global opt-out mechanism recognized in California is consistent and interoperable with opt-outs under these other state laws. Creating an interoperable approach to global opt-out mechanisms will benefit both consumers, by creating a more user-friendly system that works across state lines, and companies, by driving investment in compliance processes that satisfy laws in multiple states and that accurately effectuate consumers' choices with respect to their data. If, however, one state develops requirements for a global opt-out mechanism that conflict with requirements in other states, consumers may be presented with multiple "global" opt-out links, which can create significant confusion.

Recommendation: The CPPA should work with regulators in other states to ensure any opt-out mechanism recognized in California is interoperable with mechanisms recognized in other states.

B. Any Global Opt-Out Mechanism Must Function in Practice.

It is also critical that both businesses and consumers be able to use global opt out mechanisms in practice. However, the Proposed Regulations do not address a range of practical issues that will confront businesses and consumers as these mechanisms are implemented.

For example, it is not clear from the Proposed Regulations how a business will be able to determine that a particular signal meets the regulations' requirements, or if that determination will be left to each business. Likewise, consumers will not know which mechanisms will be honored or to what extent a mechanism will be honored across state lines. One way to address such concerns is for the CPPA to publish a list of the signals that meet CCPA requirements and thus identify the mechanisms that companies should honor, but it is not clear from the Proposed Regulations that such a process is contemplated.

This rulemaking process should address these types of practical issues, with an eye toward ensuring that businesses have fair notice of the mechanisms they may use to comply with obligations under the CCPA. Companies will require time to build tools to respond to global opt-out mechanisms — and focusing on practical issues early on will help to foster the development of tools that work in practice.

Recommendation: The CPPA should address practical considerations including how a business will recognize if a particular signal meets the regulations' requirements. For example, the CPPA could develop a process for approving an opt-out signal and then publish a list of compliant signals; it could also work with stakeholders to create a process for nominating additional signals for the agency's approval, to help companies and consumers implement opt-out mechanisms in practice.

C. Any Global Opt-Out Mechanism Should Comply with the Requirements Enumerated in Section 1798.185(a)(19)(A) of the CCPA.

The CCPA also identifies six topics to be addressed by the CPPA's regulations on global opt-out mechanisms — many of which are not addressed in the Proposed Regulations.

For example, under the statute the regulations are to "define the requirements and technical specifications for an opt-out preference signal" and should, among other things, "[e]nsure that the opt-out preference signal is consumer-friendly, clearly described, and easy to use by an average consumer," "[c]learly represent a consumer's intent and be free

of defaults constraining or presupposing that intent,” “[e]nsure that the opt-out preference signal does not conflict with other commonly used privacy settings or tools that consumers may employ,” and “[p]rovide a mechanism for the consumer to selectively consent to a business’ sale of the consumer’s personal information, or the use or disclosure of the consumer’s sensitive personal information.”²⁸

Many of these topics relate to how an opt-out mechanism will interact with mechanisms recognized by other states, which will soon be “commonly used privacy settings or tools” once Colorado and Connecticut’s global opt-out mechanism requirements go into effect. The Proposed Regulations should be revised to address these issues, which will create greater clarity about how a global opt-out mechanism is to function.

Recommendation: Section 7025(b) should be revised to address the six categories of requirements set forth in Section 1798.185(a)(19)(A) of the CCPA. This section should also reflect an intent to re-evaluate the requirements and technical specifications after one year, to ensure the agency may timely review any updates that could further promote interoperability with opt-out mechanisms in other states or could further address practical issues that may arise as the global opt-out mechanism is implemented.

D. Consumer Education Around Global Opt Outs and Their Potential Limitations Will be Critical.

The CPPA should also prioritize educating consumers about global opt-out mechanisms and specifically the scope of what such mechanisms do, as well as their limitations. For example, if a consumer uses a browser-based mechanism to opt out of the sale or sharing of the consumer’s personal information, the browser may be able to effectuate that request for activity that occurs within the browser, but not activity outside of the browser (unless the consumer provides additional information to the company receiving the signal, such as by logging into an account for the company’s website). Consumers should be aware of this and other limitations. The CPPA, and developers of compliant opt-out signals, are well-positioned to provide that education.

Recommendation: The CPPA should prioritize educating consumers about global opt-out mechanisms, including their scope and their limitations.

III. Agency Audits

A. The CPPA Should Exercise its Audit Authority in a Manner that Minimizes Privacy and Security Risks to Consumers, Including by Limiting On-Site Audits.

Under the CCPA, the CPPA is granted authority to audit compliance with the law and is tasked with issuing regulations to define the scope of the agency’s authority and the process for exercising that authority. In particular, the statute requires that these regulations include establishing criteria for both selecting persons to audit and for “protect[ing] consumers’ personal information from disclosure to an auditor in the absence of a court order, warrant, or subpoena.”²⁹

The Proposed Regulations provide few details about – or guardrails for – this authority. Section 7304 of the Proposed Regulations states that the CPPA “may audit a business, service provider, contractor, or person to ensure compliance with any provision of the

²⁸ Cal. Civ. Code § 1798.185(a)(19)(A).

²⁹ Cal. Civ. Code § 1798.185(a)(18).

CCPA.”³⁰ But the regulations do not address how personal information will be protected from disclosure in the absence of a court order, warrant, or subpoena, as required by the statute. Nor do the Proposed Regulations clearly state how privileged information will be handled, which should be addressed. Rather, the Proposed Regulations state only that consumer personal information disclosed to the agency during an audit will be maintained in compliance with the state’s Information Practices Act of 1977.

We strongly recommend that the Proposed Regulations create additional safeguards to ensure that audits further the CCPA’s goal of protecting consumer privacy – and also that ensure the audit authority is not exercised in a manner that could inadvertently undermine consumer privacy or cybersecurity.

In particular, the Proposed Regulations should be revised to address how audits will be conducted – including whether they will occur on-site or off site – and to specifically limit the use of on-site audits absent specific circumstances warranting an on-site audit. Any audit should be required to have sufficient guardrails in place to mitigate the potentially significant privacy and security concerns. For example, an audit of a service provider that serves hundreds of business customers can create a range of privacy and security risks. This is particularly true when the audit is on-site, as opposed to remote. An on-site audit may inadvertently expose to auditors information relating to a range of businesses and consumers whose activities are not the intended focus of the audit, creating significant privacy risks. Moreover, in this context on-site audits would typically not provide information beyond that available through a remote audit, because the relevant information is accessible in either case. Indeed, remote audits can be more efficient in identifying relevant information without the attendant privacy and security risks of an on-site audit. For these reasons, the Proposed Regulations should be revised to limit the use of on-site audits and specifically endorse the use of remote audits, particularly when there are no special circumstances that merit the audit being conducted on-site and when an on-site audit may create privacy and security concerns.

Given the privacy and security risks that arise from exercising the agency’s audit authority, we recommend the CPPA limit the use of its audit authority to circumstances in which there is a “significant” concern that the statute has been violated. The agency may define such circumstances by example, consistent with other aspects of the Proposed Regulations.

Recommendation: We make two recommendations to focus the Agency’s audit authority:

1. Section 7304(a) should be revised to state: “(a) Scope. The Agency may audit a business, service provider, contractor, or person to ensure compliance with any provision of the CCPA. Audits will be conducted remotely, absent specific circumstances warranting an on-site audit. Where specific circumstances warrant more immediate intervention, the Agency shall require in writing the preservation of documents and information.”
2. Section 7304(b) should be revised to state “(b) Criteria for Selection. The Agency may conduct an audit in circumstances that create a significant risk of to investigate possible violations of the CCPA. Alternatively, the Agency may conduct an audit if the subject’s collection or processing of personal information presents significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA ~~or any other privacy protection law.~~”

³⁰ Prop. Reg. § 7304(a).

* * *

BSA supports strong privacy protections for consumers, and we appreciate the opportunity to provide these comments. We welcome an opportunity to further engage with the CPPA on these important issues.

—

For further information, please contact:
Kate Goodloe, Senior Director, Policy
[REDACTED]

From: **Annalee Akin** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
CC: **Mike Belote** [REDACTED]
Subject: CPPA Public Comment - Mike Belote
Date: 22.08.2022 17:34:23 (+02:00)
Attachments: CPPA Public Comment. 8.22.22.pdf (8 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Dear California Privacy Protection Agency:

On behalf of Mike Belote of California Advocates, please find comments in connection with the California Privacy Protection Agency Rulemaking attached here.

Thank you,
Annalee

Annalee Akin
Legislative Assistant
[California Advocates, Inc.](#)
1112 11th Street
Sacramento, CA 95814
[REDACTED]



August 22, 2022

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

RE: Comments in connection with the California Privacy Protection Agency Rulemaking regarding the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act

Dear California Privacy Protection Agency:

We have discussed the forthcoming California Privacy Protection Agency (CPPA) Rulemaking regarding the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act (CPRA), with various clients represented by our firm and appreciate the opportunity to provide input. We appreciate the CPPA's proactive efforts to shape positive regulation and respectfully offer the following comments on certain key issues.

1. The CPPA Should Provide Additional Clarity Regarding Unstructured Data to Ensure that California Consumers Receive Consistent Protections.

We agree that whether data is unstructured should be considered when assessing data subject rights requests, and we appreciate the CPPA's efforts to define the term "unstructured" and provide relevant examples. As currently drafted, however, the working definition of "unstructured" in the Proposed Regulations is vague and does not reflect modern technological capabilities.

§ 7001(hh)

"Unstructured" as it relates to personal information means personal information that is not organized in a pre-defined manner, such as text, video files, and audio files.

As an initial matter, some data should appropriately be considered unstructured, even when information could, as a strictly technical matter, be extracted from that data given significant effort. In other words, just because a tool is conceptually available to search data, this does not strip that data of its unstructured characteristics. For example, a series of handwritten letters could be scanned and analyzed by software to determine the contents of those letters, and a series of printed photos could be scanned into a database and run through facial recognition software. However, these efforts may require resources that are beyond the reasonable reach of a small business, and such information may not reasonably be expected by consumers as part of a rights request.

Dennis K. Albiani ~ Cliff Costa ~ Michael D. Belote ~ Faith L. Borges ~ Anthony Molina

1112 11th Street Sacramento, CA 95814 phone: (916) 441-5050 email: calad@californiaadvocates.com

CPPA_RM1_45DAY_0189

Additionally, the examples of unstructured data provided in the definition may not be accurate in all instances. For example, Microsoft Word and Adobe Acrobat both offer end-users the ability to search and organize text, even if it is not initially searchable. Similar functionality is built into systems that are used by businesses in their day-to-day operations. While not all text may be searchable without reorganization or technological intervention (e.g., depending on the language it is in, whether it is hand-written, and what system it is stored in), data may still be extracted from the text. Additionally, photo and video library programs increasingly allow for organization and search based on a variety of metadata, such as by person, date, or location, but it would be unreasonable to argue that this means the images or videos, themselves, are structured data.

As such, we encourage the CPPA to **revise the definition of “unstructured” to remove the examples**, as they do not appear to be accurate in every case.

§ 7001(hh)

“Unstructured” as it relates to personal information means personal information that is not organized in a pre-defined manner and would not reasonably be organized in such a manner without disproportionate effort on behalf of the business. ~~-, such as text, video files, and audio files.~~

2. **For AR/VR environments, businesses should be able to provide notices of the right to opt-out of sales/sharing and the right to limit at or before the point of collection of the relevant information.**

We support the CPPA’s efforts to ensure transparency with respect to businesses’ sales and sharing practices and their use and disclosure of consumers’ sensitive personal information. However, we are concerned that the Proposed Regulations do not afford sufficient flexibility to provide notices in a manner that avoids disrupting consumers’ experiences in augmented reality or virtual reality (“AR/VR”) environments.

Proposed section 7013 would require that any business that sells or shares personal information that it collects in augmented or virtual reality provide notice of the right to opt out of sales or sharing “in a manner that ensures that the consumer will encounter the notice *while in* the augmented or virtual reality environment.” (§ 7013(e)(3)(D) (emphasis added)).

Requiring businesses to provide these notices *while consumers are in* the AR/VR environment could be disruptive to consumers’ use and enjoyment of the AR/VR device by distracting from the augmented or virtual reality experience that the consumer is trying to achieve. Moreover, given the growing array of applications for AR/VR technologies—ranging from education, to manufacturing, to healthcare, and beyond—presenting consumers with notices “while in” the AR/VR environment could be especially disruptive to important tasks that consumers carry out through AR/VR environments. For example, forcing a sales/sharing opt-out notice to appear on an AR/VR headset that a doctor is using to practice a complicated medical procedure could be highly disruptive to that practice.

We encourage the CPPA to allow flexibility for businesses to provide notices of the sales/sharing opt-out rights, and the right to limit, at or before the point of collection of the relevant personal

information in the AR/VR environment. To that end, we recommend revising the Proposed Regulations as follows:

§ 7013(e)(3)(D)

A business that sells or shares personal information that it collects in augmented or virtual reality, such as through gaming devices or mobile applications, shall provide notice in a manner that ensures that the consumer will encounter the notice ~~while in the augmented or virtual reality environment~~ at or before the point of such collection.

3. For Sensitive Personal Information That was Collected Prior to the CPRA Taking Effect, Businesses Should be Permitted to Continue Using Such Information for the Same Purposes Without Obtaining Additional Consent.

We applaud the CPPA’s efforts to provide consumers with greater control over their sensitive personal information, and we generally support the requirements of proposed section 7014 aimed at ensuring that consumers receive adequate notice of their right to limit the use and disclosure of their sensitive personal information. However, we are concerned about the specific requirement in proposed subsection 7014(h), which could substantially disrupt business operations and long-term projects.

As currently drafted, subsection 7014(h) could be interpreted to have a retroactive effect. It would require a business to obtain a consumer’s consent to use and disclose (except for certain purposes specified in section 7027) any sensitive personal information collected “during the time the business did not have a notice of right to limit posted.” This language could be interpreted to apply to any sensitive personal information collected pre-CPRA. However, businesses likely would not have posted such a notice prior to the enactment of the CPRA, as it was not required under either the statute or the Regulations. Thus, subsection 7014(h) could be read to impose a retroactive restriction on businesses. This would create regulatory confusion and undermine confidence that the data that businesses collected in compliance with pre-CPRA law can continue to be used for the same purposes for which it originally was collected, including for long-term projects that span many years.

Rendering such data unusable for its pre-CPRA purposes could also substantially disrupt businesses’ operations and services to California residents. For example, a business might have lawfully collected certain consumer health information for purposes of a long-term research study that falls outside of relevant exceptions in section 1798.145(c). Prohibiting the business from continuing to use such data for the same purposes for which the business lawfully used the data prior to the CPRA unless a new consent was signed could seriously undermine the study, resulting in harm to consumers and the public by depriving them of the health benefits that the study otherwise would have provided.

To prevent these kinds of harms to both businesses and consumers, businesses should be permitted to continue using sensitive personal information lawfully collected prior to the CPRA taking effect, without obtaining additional consent, for the same purposes for which they were lawfully permitted to use it pre-CPRA. To ensure businesses’ ability to do so, **the CPPA should confirm expressly that subsection 7014(h) applies only to data collected on or after January 1, 2023.** This would prevent the aforementioned disruptions to businesses’ operations and long-term projects while still providing ample

protection for consumers' sensitive personal information moving forward. For this reason, we suggest revising subsection 7014(h) as follows:

*A business shall not use or disclose sensitive personal information it collected during the time the business did not have a notice of right to limit posted for purposes other than those specified in section 7027, subsection (l), unless it obtains the consent of the consumer. **This subsection shall apply only to sensitive personal information collected on or after January 1, 2023.***

4. To Ensure Accountability, Authorized Agents Should Continue to be Registered with the Secretary of State.

The Proposed Regulations have revised the definition of “authorized agent” in subsection 7001(c) to remove the language requiring business-entity authorized agents to be “registered with the Secretary of State to conduct business in California.” This change ultimately will harm consumers by removing an important requirement that helps to hold authorized agents accountable and protects consumers from fraud. We therefore encourage the CPPA to **add back the registration requirement.**

The requirement that business-entity authorized agents be registered to do business in California protects consumers by ensuring that such agents—who have broad access to consumer data—can be held accountable. The act of registering with the Secretary of State is a straightforward process that imposes a minimal burden on agents but helps to ensure that the Secretary has information about the business that is needed for proper oversight. For example, businesses that register with the Secretary must file an annual Statement of Registration to provide the Secretary with updated information about the business's management and its agent for service of process.¹ This helps to ensure that the state of California has information about the person(s) responsible for the business, thereby facilitating the state's appropriate oversight of the business.

Without any oversight from the state, it may be easier for entities acting as authorized agents to submit fraudulent requests related to consumer data. Our clients are companies that strive to provide the highest protections for consumers' information, and they see the continually evolving strategies that bad actors use in an attempt to gain unauthorized access to personal information. Removing the registration requirement would increase the likelihood that such bad actors could submit fraudulent requests and improperly access, correct, or delete consumers' personal information. For this reason, we strongly encourage the CPPA to restore the registration requirement for business-entity authorized agents.

The Initial Statement of Reasons indicates that the CPPA removed the relevant language (regarding registration with the Secretary of State) in subsection 7001(c) of the Proposed Regulations in response to confusion from businesses as to whether a separate registration process is required.² Specifically, the Initial Statement of Reasons states that businesses have “misinterpreted this language to mean that there is

¹ See, e.g., “Annual and biennial requirements for a business entity” in the California Secretary of State's Business Entities Frequently Asked Questions page, available at: <https://www.sos.ca.gov/business-programs/business-entities/faqs#annual>.

² See Initial Statement of Reasons, “Specific Purposes and Necessity of Each Section,” at 4.

a special registry with the Attorney General’s Office for authorized agents,” and that deleting the language is necessary to clear up the confusion.³

However, to the extent that this issue has arisen, it can be remedied better by clarifying that there is no separate or special registration process for business entities to act as authorized agents, rather than by removing one of the few existing qualifications for a business to act as an authorized agent. For example, the CPPA could revise the definition of “authorized agent” to make clear that the “registered with the Secretary of State to conduct business in California” language refers only to business entities and not natural persons, which would help to clarify that the language refers only to the process of registering to conduct business in California and not a special registration process for authorized agents. Below, we suggest a potential revision to this effect:

§ 7001(c)

“Authorized agent” means a natural person or a business entity ~~registered with the Secretary of State to conduct business in California~~ that a consumer has authorized to act on their behalf subject to the requirements set forth in section 7063. ~~Where a consumer has authorized a business entity to act on their behalf, such business entity must be registered with the Secretary of State to conduct business in California.~~

5. The CPPA Should Revise the Proposed Correction Request Requirements to Avoid Subjecting Businesses to Potentially Endless Requests and to Provide a Safe Harbor for Good-Faith Determinations.

The right to correct is an important consumer right. However, the Proposed Regulations would effectively place businesses in an impossible position: either honor every correction request, or just as problematic, face never-ending resubmitted requests.

The issue arises from the combined effect of proposed subsections 7023(d) and (g). First, subsection 7023(g) requires that businesses treat a correction request as a “new” request—even where the consumer has previously submitted a request to correct the same alleged inaccuracy within the past six months—so long as a consumer submits additional documentation. Second, subsection 7023(d) requires that businesses consider “any documentation that the consumer provides” in connection with a correction request. Coupled together, these two requirements mean that, so long as consumers include some additional piece of information, they can resubmit requests indefinitely, and businesses will be required to consider them.

To make matters worse, the Proposed Regulations do not require that this new quantum of information be germane, or even that it was discovered or created after the date of the initial request. As a result, a renewed request for the same alleged inaccuracy would seem to require a *de novo* review of the entire corpus of evidence in order to make a reasoned determination every single time the consumer files the request.

³ *Id.*

To avoid such a scenario while preserving the rights of consumers who submit legitimate requests to correct, the CPRA should: (a) require that consumers make a good-faith effort to include with the initial request all relevant documentation available at the time of such initial request; (b) require that any subsequent request to correct include new documentation that (i) is relevant to the request and (ii) was not available to the consumer at the time of the initial request; **and (c)** provide a safe harbor for good-faith determinations made by businesses in accordance with the Proposed Regulations (as amended pursuant to the preceding suggestions).

First, requiring that consumers make a good-faith effort to provide businesses with all relevant information available at the time of any initial request will benefit consumers by promoting efficiency and timeliness in the correction request process. Having consumers assume responsibility for submitting all relevant materials at the time of their initial request will also reduce the number of legitimate requests that are initially denied, shorten the overall process for consumers, and free up resources for businesses to focus on reviewing materials and fulfilling requests rather than requesting additional information. Furthermore, limiting fact-based appeals to those with newly discovered evidence would benefit consumers by providing an easy-to-understand and straightforward, bright-line approach for requests to correct.

Finally, a safe harbor would provide businesses with certainty that reasonably denying requests in accordance with the criteria of subsections 7023(b), (g), or (h) (as revised to reflect the suggestions above) would not subject them to undue liability, especially when faced with requests from bad actors. Also, by facilitating a greater sense of continuity and uniformity in businesses' decisions, a safe harbor would improve consistency and predictability for the consumers for whom the right is intended. It may also help spur faster responses to rights requests.

6. The “Reasonable Expectations” Standard and Corresponding Consent Requirement Exceed the Scope of the CPRA and Would Upend the Transparency-Based Privacy Model That California Voters Endorsed.

California voters—through their elected representatives in 2018 and directly on the ballot in 2020—have twice endorsed privacy frameworks that rely on transparency as a fundamental means to preserving consumer privacy. The CCPA and the CPRA forgo requirements that businesses obtain opt-in consent or rely on other legal bases to process personal information and instead impose unparalleled transparency requirements and provide consumers with new rights.

Yet the Proposed Regulations seem to disregard transparency as a guiding principle in California privacy law and instead would impose stringent limitations on the purposes for which businesses can process personal information based on the expectations of the “average” consumer, an interpretation that is both unworkable and that exceeds the scope of the CCPA’s statutory authority. **Indeed, the proposed obligation that businesses obtain separate consent for notified uses—including to develop new innovations—goes far beyond the voter-approved CPRA framework and fundamentally transforms the CPRA’s impact and scope.**

The Proposed Regulations have revised the statutory construction of a reasonable purpose limitation requirement with permissions to use data for compatible processes into an impracticable obligation that exceeds the requirements of even the EU GDPR. In particular, subsection 7002(a) of the Proposed

Regulations would create a novel standard that requires processing to be “consistent with what an average consumer would expect” and that permits other notified purposes only if they are “compatible with what is reasonably expected by the average consumer.” Any purportedly incompatible purposes would require express, opt-in consent.

As a threshold issue, the Proposed Regulations are entirely silent as to what constitutes the “average consumer,” an issue that poses compliance challenges for businesses and that can ultimately confuse consumers as to whether consent is required for certain processing. The requirement that businesses consider the expectations of the “average consumer” creates an implicit obligation for businesses either to speculate as to what the “average consumer” would expect—exposing the business to liability if they make even a good-faith miscalculation—or to track detailed information about the expectations of California residents, whether through observations or market research, and to tailor their processing activities to those individuals. This requirement provides little certainty as to whether consent is required for certain types of processing, for both businesses whose customer base may change over time, and for consumers who might patronize companies whose average customers may have different expectations. Contrary to the goal of reducing the need to read detailed privacy notices, this standard would make it even more important for consumers to scour privacy notices in detail. The California Attorney General had similarly introduced the concept of an “average consumer” during its rulemaking process but ultimately eliminated the process in response to confusion regarding the concept.⁴ We suggest the CPPA do the same.

Furthermore, the prohibition on a business’s use of personal information except for purposes that are aligned only with the reasonable expectations of the “average consumer,” even if there are additional disclosures, strays far afield from the CPRA’s statutory text and the CPPA’s authority.

The Proposed Regulations would greatly restrict a business from engaging in certain processing activities that the business has clearly disclosed in their privacy policies or other just-in-time notices and that engage in other privacy-protective efforts to help consumers understand the processing at hand and the consumer’s choices. This would be true even though the activity has been disclosed and even if consumers genuinely comprehend the processing is occurring.

The requirements of 7002(a) become extraordinarily problematic under the Proposed Regulations’ examples, which seem to require businesses to obtain opt-in consent for common practices that reasonable consumers would expect. Consider Example B, which suggests that new product development is an unexpected use of personal information, even when this use of data is explicitly disclosed in the company’s privacy policy or in product-specific privacy notices. This would make it immensely difficult for companies to develop innovative products for California consumers, especially because the line between a new product and a new feature of an existing product is not always clear or set in advance.

Simply put, the provisions in the Proposed Regulations regarding the expectations of the average consumer go beyond the scope of the statute and the CPPA’s authority. We therefore recommend that subsection 7002(a) be revised as follows:


⁴ Final Statement of Reasons, California Attorney General (June 1, 2020), <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor.pdf> (“Second, the phrase “understandable to an average consumer” was changed to “understandable to consumers.” This change was made because several public comments expressed confusion about the meaning of the term “average consumer.””).

§ 7002(a)

A business's collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purpose(s) for which the personal information was collected or processed. ~~To be reasonably necessary and proportionate, the business's collection, use, retention, and/or sharing must be consistent with what an average consumer would expect when the personal information was collected. A business's collection, use, retention, and/or sharing of a consumer's personal information may also be for other disclosed purpose(s) if they are compatible with what is reasonably expected by the average consumer. A business shall obtain the consumer's explicit consent in accordance with section 7004 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.~~

We thank the CPPA for considering these comments in its rulemaking process.

Sincerely,


Michael D. Belote
California Advocates, Inc.

From: **Don Marti** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 22.08.2022 12:46:08 (+02:00)
Attachments: CafeMedia-CPRA-comments-22-Aug-2022.pdf (3 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

CafeMedia
1411 Broadway, 27th Floor
New York, NY 10018 USA

22 August 2022

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

Dear Mr. Soublet:

This is a comment in response to the Notice of Proposed Rulemaking published on July 8, 2022.

CafeMedia, also operating as AdThrive, exclusively represents the advertising businesses of more than 3,600 web publishers, including 346 small and mid-sized web sites published in California. In aggregate, those thousands of publishers represent the 7th largest property on the internet, according to Comscore. They range in size between 100,000 to more than 50 million monthly pageviews. These independent publishers fill an important role on the internet by providing many kinds of free content to more than 183 million web users who visit at least once a month. As the largest ad representative of this type, we believe we have a unique position to speak for an under-represented constituency whose perspective is an important component of how to create a more fair and more private advertising ecosystem.

In the two and a half years since the California Consumer Privacy Act (CCPA) came into effect, the people of California have gained experience with the process of exercising basic privacy rights under the law. Unfortunately, several gaps in the existing CCPA regulations have made many of these rights impractical or impossible to exercise for many people. In the 2020 election, Proposition 24 was supported by an overwhelming majority of California voters. Today, the CPPA has an opportunity to implement the intent of California voters by clarifying and reforming California's privacy regulations that make it practical for everyone to exercise their basic privacy rights.

Some practical problems with the existing regulations include:

Regulations encourage arbitrarily complex verification processes. The regulations allow for a bewildering variety of approaches to verifying identity for the purpose of Right to Know and Right to Delete. California residents must take selfies, upload photos to poorly-tested web sites with limited device support, pass quizzes, pass quizzes that only work if you put in wrong answers, print documents, scan documents, and even have documents notarized.

Regulations must limit the verification pathways allowed, or mandate a baseline, repeatable process that businesses must offer as one option, in order to make it practical for anyone in California to exercise their Right to Know and Right to Delete under the law.

Categories of information, not values, must be disclosed. The proposed regulations state (§7024(k), page 35), "A business shall identify the categories of personal information, categories of sources of personal information, and categories of third parties to whom a business sold or disclosed personal information, in a manner that provides consumers a meaningful understanding

of the categories listed.” But there is nothing in the regulations requiring the actual personal data values to be in a comprehensible format. Since 2020, many Right to Know documents returned under the CCPA include incomprehensible alphanumeric codes with no explanation or decoding key. The regulations need to be extended to include “values for personal data points” in the list of information that must be disclosed in a manner that provides the consumer with a meaningful understanding.

A hash of personal information should be treated as personal information. Some businesses maintain personal information in the form of a hash value, calculated from the original using an algorithm. (For example, the hash value of the email address [REDACTED] calculated with the algorithm SHA-256 is [REDACTED]). Any party with knowledge of both the algorithm and the original value can obtain the same hash value.

A business or service provider that stores hash values of personal information and receives a Right to Know, Right to Correct, or Right to Delete containing the original values should be not be allowed to deny a request simply because they hold only the hash value; they should be required to run any hash algorithms they use on the original values from the request, and apply the request to any hash values found.

Unfortunately, some businesses that intend to evade their responsibilities under the law will continue to seek and exploit gaps in the regulations. It would be helpful for the CPPA to survey consumers who actively exercise their Right to Know in order to learn about new exploits and refine future regulations and guidance. We appreciate the opportunity to reply to this inquiry. CafeMedia, as an advertising service firm acting on behalf of independent publishers, believes that future privacy-preserving regulations and technologies can be designed to apply fairly and effectively to all businesses, and all uses of personal information. We would welcome any feedback on this letter and are available to answer any questions. Thank you.

Sincerely,

Paul Bannister
Chief Strategy Officer
[REDACTED]

Don Marti
VP, Ecosystem Innovation
[REDACTED]

CafeMedia
1411 Broadway, 27th Floor
New York, NY 10018 USA

22 August 2022

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

Dear Mr. Soublet:

This is a comment in response to the Notice of Proposed Rulemaking published on July 8, 2022.

CafeMedia, also operating as AdThrive, exclusively represents the advertising businesses of more than 3,600 web publishers, including 346 small and mid-sized web sites published in California. In aggregate, those thousands of publishers represent the 7th largest property on the internet, according to Comscore. They range in size between 100,000 to more than 50 million monthly pageviews. These independent publishers fill an important role on the internet by providing many kinds of free content to more than 183 million web users who visit at least once a month. As the largest ad representative of this type, we believe we have a unique position to speak for an under-represented constituency whose perspective is an important component of how to create a more fair and more private advertising ecosystem.

In the two and a half years since the California Consumer Privacy Act (CCPA) came into effect, the people of California have gained experience with the process of exercising basic privacy rights under the law. Unfortunately, several gaps in the existing CCPA regulations have made many of these rights impractical or impossible to exercise for many people. In the 2020 election, Proposition 24 was supported by an overwhelming majority of California voters. Today, the CPPA has an opportunity to implement the intent of California voters by clarifying and reforming

California's privacy regulations that make it practical for everyone to exercise their basic privacy rights.

Some practical problems with the existing regulations include:

Regulations encourage arbitrarily complex verification processes. The regulations allow for a bewildering variety of approaches to verifying identity for the purpose of Right to Know and Right to Delete. California residents must take selfies, upload photos to poorly-tested web sites with limited device support, pass quizzes, pass quizzes that only work if you put in wrong answers, print documents, scan documents, and even have documents notarized.

Regulations must limit the verification pathways allowed, or mandate a baseline, repeatable process that businesses must offer as one option, in order to make it practical for anyone in California to exercise their Right to Know and Right to Delete under the law.

Categories of information, not values, must be disclosed. The proposed regulations state (§7024(k), page 35), "A business shall identify the categories of personal information, categories of sources of personal information, and categories of third parties to whom a business sold or disclosed personal information, in a manner that provides consumers a meaningful understanding of the categories listed." But there is nothing in the regulations requiring the actual personal data values to be in a comprehensible format. Since 2020, many Right to Know documents returned under the CCPA include incomprehensible alphanumeric codes with no explanation or decoding key. The regulations need to be extended to include "values for personal data points" in the list of information that must be disclosed in a manner that provides the consumer with a meaningful understanding.

A hash of personal information should be treated as personal information. Some businesses maintain personal information in the form of a hash value, calculated from the original using an algorithm. (For example, the hash value of the email address [REDACTED] calculated with the algorithm SHA-256 is [REDACTED]). Any party with knowledge of both the algorithm and the original value can obtain the same hash value.

A business or service provider that stores hash values of personal information and receives a Right to Know, Right to Correct, or Right to Delete containing the original values should be not be allowed to deny a request simply because they hold only the hash value; they should be

required to run any hash algorithms they use on the original values from the request, and apply the request to any hash values found.

Unfortunately, some businesses that intend to evade their responsibilities under the law will continue to seek and exploit gaps in the regulations. It would be helpful for the CPPA to survey consumers who actively exercise their Right to Know in order to learn about new exploits and refine future regulations and guidance. We appreciate the opportunity to reply to this inquiry. CafeMedia, as an advertising service firm acting on behalf of independent publishers, believes that future privacy-preserving regulations and technologies can be designed to apply fairly and effectively to all businesses, and all uses of personal information. We would welcome any feedback on this letter and are available to answer any questions. Thank you.

Sincerely,

Paul Bannister
Chief Strategy Officer

[REDACTED]

Don Marti
VP, Ecosystem Innovation

[REDACTED]

From: **Lauren Scheib** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
CC: [REDACTED] [REDACTED]
Subject: CPPA Public Comment
Date: 22.08.2022 16:01:12 (+02:00)
Attachments: ATP Comments to CA Privacy Pro 8_22_22.pdf (13 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

BEFORE THE CALIFORNIA PRIVACY PROTECTION AGENCY

California Code of Regulations, Chapter 1 California Consumer Privacy Act Regulation Title 11, Div. 6 (§§7000-7304)

Comments on Proposed California Consumer Privacy Act Regulations

-
The Association of Test Publishers (“ATP”) submits these comments to address the concerns of the testing industry related to the California Consumer Privacy Act Proposed Regulations (“Proposed Regulations”), as published on July 8, 2022. **This submission is being made by the required date of August 23, 2022. [COMMENTS ATTACHED]**

Lauren Scheib
Chief Operating Officer
[Association of Test Publishers](#)
601 Pennsylvania Ave., NW
South Bldg., Suite 900
Washington D.C. 20004 USA
+1.717.755.9747
Fax: +1.717.755.8962
Email: [REDACTED]
www.testpublishers.org



Advancing equity, integrity, and learning

601 Pennsylvania Ave., N.W. Suite 900
 Washington D.C. 20004
 +1.717.755.9747
 www.testpublishers.org

Susan Davis-Becker, Ph.D., ACS Ventures, LLC
Jim Holm, Examity
John Kleeman, Questionmark
Andy McAnulla, BTL/Surpass
Rory McCorkle, Ph.D., PSIONline
Liberty Munson, Ph.D. Microsoft
Amy Riker, Curriculum Associates
Ashok Sarathy, GMAC
Divyalok Sharma, Pearson VUE
Kimberly Swygert, Ph.D., NBME
Alex Tong, ATA
**Alina von Davier, Ph.D., Duolingo*
Hazel Wheldon, MHS
**Chair*

Chief Executive Officer: *William G. Harris, Ph.D.*
Chief Operating Officer: *Lauren B. Scheib*
General Counsel: *Alan J. Thiemann, Esq.*
Secretary: *Andre Allen, FifthTheory LLC*
Treasurer: *Amy E. Schmidt, Ph.D, Pearson VUE*

BEFORE THE CALIFORNIA PRIVACY PROTECTION AGENCY

California Code of Regulations, Chapter 1 California Consumer Privacy Act Regulation Title 11, Div. 6 (§§7000-7304)

Comments on Proposed California Consumer Privacy Act Regulations

The Association of Test Publishers (“ATP”) submits these comments to address the concerns of the testing industry related to the California Consumer Privacy Act Proposed Regulations (“Proposed Regulations”), as published on July 8, 2022. This submission is being made by the required date of August 23, 2022.

The ATP is the global trade association for the assessment and learning industry. The ATP is comprised of hundreds of publishers, test sponsors (i.e., developers/owners of test content, such as certification bodies), and vendors that deliver tests used in various settings, including employment (e.g., employee selection and other HR functions), education (e.g., academic admissions), clinical diagnostic and other healthcare assessments, certification/ licensure (e.g., licensure/recertification of various professionals), and workforce credentialing, as well as businesses that provide testing services (e.g., test security, scoring) or administer test programs (collectively referred to herein as “Members”). Since its inception in 1987, the Association has advocated for the use of fair, reliable, and valid assessments, including ensuring the security of test content and test results. Our activities have included providing expertise to and lobbying the US Congress and state legislatures on proposals affecting the use of testing in employment and education, as well as representing the industry on regulatory matters and litigation surrounding the use of testing. The ATP developed and currently publishes compliance guidelines on the EU General Data Protection Regulation (“GDPR”) and are currently publishing a series of educational bulletins entitled “Privacy in Practice” that focus on compliance with both U.S. and international privacy laws and regulations, including the California Consumer Privacy Act (“CCPA”). The ATP also plans to publish a bulletin on these Proposed Regulations when final.

The ATP respects the goals the California Consumer Privacy Agency (the “Agency”) is expressing in the Proposed Regulations to provide for comprehensive implementation of the California Privacy Rights Act (“CPRA”), amendments to the California Consumer Privacy Act (“CCPA”), and to provide guidance to covered businesses that must comply. However, we strongly believe that specific circumstances common in the testing industry, which are shared by many smaller/medium-sized businesses in other industries, justify modification of the Proposed Regulations when balanced against the rights of individual test takers as consumers. Accordingly, the ATP urges the Agency to take these specific comments into account in adopting final regulations.

GENERAL BACKGROUND: ATP Members and the Assessment Industry

Many testing events occur that greatly benefit and protect the public, along with those who rely on test results, especially individual test takers. California consumers are no exception to the vast – and growing – population of users of assessments whose purpose is to advance themselves personally and/or professionally.¹

Individuals voluntarily participate in testing for many reasons. Among them is to obtain a driver’s license, to identify ways to improve their lives, to understand their academic strengths and weaknesses, to gain admittance to an institution of higher learning or other academic/adult educational program, to seek employment or to gain a promotion once employed, to become licensed/certified in a profession, to become certified in sport/recreation (e.g., flying, scuba) or professionally (e.g., IT certifications in literally thousands of technical skills), and even to understand their own health (e.g., diagnostic tests) or how to provide lifesaving procedures on others (e.g., CPR). In a majority of these instances, assessments are pivotal to a public interest and/or consumer protection motive (e.g., medical, legal, accounting, airline pilot, police, EMT).

Many of these situations involve the use of “high stakes” secure testing, i.e., where the outcome of a test carries a significant consequence for the test taker (such as a securing a job, getting admitted to a school, or being issued a license or certificate). In these cases, the test items are kept secure (even by the U.S. Copyright Office, which has separate copyright registration procedures for secure tests)² to ensure that future test takers cannot obtain advance knowledge of them – which would have the effect of invalidating the test results. In fact, if some test takers are able to obtain favorable results on a test by cheating, then the value of the testing program is completely undermined for everyone. Testing has become part of our daily lives; individuals generally well understand that testing provides them with benefits, directly or indirectly, by assisting to serve the public health, safety, and welfare of the community or society as a whole.

Thus, it is vitally important for every testing organization, particularly those using high-stakes tests, to ensure that its online registration process can be conducted in accordance with the CCPA, the CPRA Amendments and these Proposed Regulations, so that all test administrations, whether conducted in person or online, are fair to all test takers. In so doing, a testing organization must be able to ensure that an individual who takes a test is in fact the same individual who is registered to take the test (with or without establishing that s/he is eligible to take the test). Furthermore, testing organizations must monitor testing events to ensure that administration irregularities which may have an adverse impact on every test taker are detected and handled in an appropriate manner.³ Equally important, testing organizations seek to ensure that all personal information collected from test takers (i.e., “consumers”) is protected from unauthorized access and/or acquisition, and that all privacy-related requests from consumers are handled appropriately under the terms of the relevant laws. For all of these reasons, the ATP submits that every high-stakes testing organization shares the following legitimate purposes associated with the need for collecting and using the personal information of test takers: (1) to ensure fairness in testing;

¹ The ATP’s comments are not intended to apply to educational testing in K-12 classrooms. However, the ATP is aware that some school admissions testing of children is done by computer, as well as career-oriented K-12 educational and vocational education programs for children. In any situation involving the testing of minors, including for medical/diagnostic purposes, the ATP expects that the controlling business would require a test taker agreement to be signed by the child’s parent/guardian, because minors do not have legal status to enter into such an agreement. The ATP urges the Agency to exempt PII already subject to the Family Educational Rights and Privacy Act (“FERPA”) (20 U.S.C. § 1232g; 34 CFR Part 99) from these Proposed Regulations.

² See fn 5, *infra*

³ It is important to recognize that in most high-stakes tests, the test taker is expected to answer questions on his/her own, without having advance access to test questions, receiving any assistance from another person, using reference materials or notes, or having unauthorized access to the Internet. Obviously, these high-stakes tests are unique to the specific individual taking the test – the results/scores are only intended for and relevant to the specific individual who has registered for the test and then verified to take the test. Consequently, every testing organization pays significant attention to the security of test content and test taker information, to ensure that cheating on tests is prevented so that every test taker has an equally fair opportunity to succeed.

(2) to prevent fraud (i.e., cheating) by individuals taking a secure test; and (3) to protect proprietary (and often copyrighted) secure “high stakes” test items from being stolen by test takers and illegally distributed to future test takers.

Consistent with the above objectives, the ATP notes that many high-stakes testing programs are national in scope, drawing test takers from every state.⁴ For ease of business operations, ATP Members often adopt a uniform Privacy Policy to meet the needs of all test takers across the United States. Given that the CCPA has been in effect, we understand that many testing organizations have already modified their privacy policies to meet the CCPA requirements. Thus, it is very important for ATP Members to continue to be able to manage their operations to address all aspects of the CCPA and CPRA, while complying with other applicable state privacy laws. Through these comments, the ATP has addressed testing-specific issues to highlight interpretations and recommended ways to modify the Proposed Regulations.

General Background – Roles and Responsibilities in Testing

At the outset, the ATP needs to point out that a majority of the high stakes testing programs (e.g., in employment, education, certification/licensure) do NOT rely on a traditional two-party business relationship, where a consumer has a direct relationship to the business that is selling goods or services (e.g., going into a store or online to make a purchase directly from a seller). To accomplish smoothly functioning and efficient operations to serve their customers, many testing organizations have segmented their operations into two or more diverse roles in the provision of testing services: one entity that owns the test (that may have developed the test or contracted for its development) and makes all of the decisions about how to use any personal information obtained from an individual test taker; and one or more secondary entities that actually handle the delivery, administration and scoring of the testing services. It is such a secondary entity that in many instances is the one that actually has the direct contact with the test taker/consumer. Furthermore, there often are other parties who provide supporting services to either or both of the two principal businesses (i.e., function as a “service provider” under the CCPA). The ATP applauds the current CCPA regulations, which strongly support the role of service providers in dealing efficiently with privacy concerns on behalf of the controlling business. The final CPRA regulations must equally recognize that any business that functions as a “service provider” does not control the collection and use of consumers’ personal information.

Another unique factor of the high stakes testing industry is that “consumers” of tests and testing services may be individuals, but in many instances, the rights to use tests and/or testing services are “sold” to businesses (i.e., employers) or professionals (e.g., doctors, psychologists), who then have the responsibility to arrange for the administration of the tests to the actual test takers, either by themselves or by a test delivery vendor. In this context, then, it is equally important to note that, especially for “secure tests” (i.e., those tests whose items must not be made available to test takers in advance of a test administration), the tests themselves are not “sold” in the commercial sense but are provided for use by the customer of the testing services – in this sense, then, ownership of the tests is not conveyed in a commercial “sale.”⁵ Indeed, in many instances, the testing organization

⁴ Indeed, many ATP Members operate international testing programs, meaning that those organizations register and administer tests to test takers outside the U.S. Thus, they must operate in accordance with global privacy laws, especially the General Data Protection Regulation (“GDPR”). In those situations, many ATP Members have attempted to establish a uniform privacy policy that harmonizes the GDPR with the CCPA. It is simply impractical and unrealistic to expect an entity doing business internationally to adopt separate and distinct privacy policies for each country in which it operates (or for each state in the United States).

⁵ Secure tests are granted special copyright protection in the United States under the 1976 Copyright Act. The regulations implementing the Act define (in part) a “secure test” as “a nonmarketed test...” “For these purposes, a test is not marketed if copies are not sold but it is distributed and used in such a manner that ownership and control of copies remain with the test sponsor or publisher.” 37 CFR 202.20(b)(4). See 42 Fed. Reg. 59,302, 59,304 & n.1 (Nov. 16, 1977). The ATP contends that the final regulations must include guidance on an exception addressing the recognition of a business’s IP rights under federal law.

provides “scoring services” to the employer or professional test user – it is often the employer or test user who has the right to decide what personal information is collected and how it is used.

Perhaps because of the complexities inherent in the provision of testing services, the standard practice for most testing organizations is the use of a formal test taker form/agreement to spell out to each individual test taker both his/her rights and responsibilities related to the testing services (e.g., rights to challenge or appeal, retest rules, prohibitions on copying/sharing test items), as well as the information about the business’s privacy policy, which the must acknowledge or accept.⁶ Among the uses of personal information that may be enumerated in such agreements are specific steps taken to ensure that cheating does not occur (e.g., monitoring test administration either physically or electronically). Many testing organizations require the test taker to sign this agreement first when registering online for the test and then again at the test administration before the test taker begins the testing session, which provides evidence that the test taker was given the required notice twice.

Because of the well-documented division of responsibilities among different entities participating in a testing event, the most critical issue in a privacy context is which entity has the responsibility for collecting personal information from test takers and for determining what use(s) are to be made of that information. While the high-stakes test owner may obtain test taker information from one or more of its service providers in the performance of the testing services, the responsibility for compliance with the CCPA/CPRA must fall squarely on the test owner, the entity that makes all of the relevant decisions about what personal information should be collected and what uses it makes of that personal information.⁷ However, as noted, in other instances, it is the test user (e.g., employer, professional, institution) that makes those decision and therefore must be treated as the “covered business” or “controller.”

Equally pertinent to this control issue is the key distinction between test takers’ personal information (e.g., name, address, email address) and the outcome of testing services purchased by test takers – the test results or scores. Although it may be appropriate in some situations to recognize that the answers to test items written down by a test taker are “personal” to that individual, test results/scores are not “collected” information.⁸ Test results/scores are the product of the test services procured by the consumer; they are not information collected from test takers, but are derived outcomes produced by the testing organization using proprietary scoring rubrics.⁹

⁶ The ATP believes that, to the extent that a test taker form/agreement is used by a testing organization as a “point-of-collection notice,” it must meet the requirements of §999.305(a). Nevertheless, no matter how much a business tries to use “plain language” and “avoid legal jargon,” someone can always assert that a document which has legal significance fails to conform. The final regulations should be modified to include language that a notice shall be “reasonably written to achieve the goals” to ensure that a balanced approach is used to evaluate all such documents.

⁷ Some of those responsibilities may be delegated by contract to one or more service providers, who often have the direct relationship with the test takers, such as handling registration of test takers, administering the actual testing services, providing test proctoring services, and/or managing the security of the testing event.

⁸ Even “raw” data provided by a test taker is not always considered to be “personal information” or treated as personal information. In circumstances where the test taker is an employee, where the testing organization’s IP rights must take priority over a person’s test answers, and where another exemption may exist that supports a denial of a request for access to, or deletion of, information collected from the test taker, such test answers are effectively not personal information. These situations are covered in the test taker agreement (*see supra*. fn 5).

⁹ Significantly, this type of derived information is largely unique in the testing industry. Test results/scores are distinguished from consumers’ input on social media services, where an individual’s postings to the platform are then shared in the same manner and context in which they were inputted. Nor are test results/scores remotely similar to derived personal information that is generated in a marketing context, where a person’s buying patterns/behaviors are tracked and used to create a profile that is sold to other marketers. Indeed, the Proposed Regulations (at §999.305(d)), make it clear that such results cannot be “personal information at the time of collection” – obviously, test results/scores do not even exist at the time of collection of the consumer’s personal information related to the testing services. An individual acquires (or obtains) testing services when test scores are the contracted for outcome or product. What a testing organization does with those scores is governed by and disclosed to the test takers in the test taker agreement.

Moreover, the uses of test results/scores are co-extensive with the need of each test taker for the testing services. In other words, if an individual is seeking a license/certificate documenting a particular skill (e.g., in law, medicine, technology), the issuer of that license/certificate is the owner of the test and the outcome is based on the individual's test results/score; similarly, if an individual is seeking a job or a promotion, that decision is made by the employer, based upon various factors, including the individual's test results/scores. Application of overly-prescriptive privacy requirements on the sharing of an individual's test results/scores defeats the very purpose the person has in taking the test in the first place.¹⁰

The ATP has presented this background information on the roles and responsibilities experienced in the assessment/learning industry as a framework within which to address specific Proposed Regulations in the following comments.

Comments on the Proposed Regulations

1. Authorized Agent

The Agency proposes to delete the requirement that an "Authorized Agent" is registered with the Secretary of State, apparently intending that a consumer would be able to authorize anyone to act on their behalf.¹¹ Moreover, Section §7063(b) of the Proposed Regulations regarding "Authorized Agents," states that: "A business shall not require a power of attorney in order for a consumer to use an authorized agent to act on their behalf." We also note that the authorized agent is only required to implement and maintain reasonable security procedures and practices to protect the consumer's personal information (*see* §7063(c)).

The ATP has serious concerns about these revisions because they would make compliance significantly more onerous as the volume of individual rights requests will increase and may also lead to a corresponding increase in fraudulent or spamming-like activities that businesses have already experienced under CCPA from groups that send thousands of requests claiming to be authorized by individuals without providing any proof of authorization. Scores of covered businesses have received and continue to be subject to the onslaught of these requests. Some of these requests are not legitimate requests from individuals but from spam-like organizations and others not acting in good faith. The ATP urges the Agency not to revise the current definition but rather to expand the regulations to impose more obligations for these "authorized agents" to provide proof that they are in fact authorized and are acting legitimately on behalf of individuals. Many testing organizations have been inundated with these illegitimate requests that require significant time and resources to attempt to verify, investigate, and resolve. Proposing to remove the requirement that these "agents" are registered with the Secretary of State will result in businesses being flooded with illegitimate, unwarranted requests.

2. Disproportionate Effort:

The Agency proposes to add a definition of "disproportionate effort" "within the context of a business responding to a consumer request, specifically stating the term: *"means the time and/or resources expended by the business to respond to the individualized request significantly outweighs the benefit provided to the consumer by responding to the request"* (*see* §7063(h)). The Agency has provided some helpful examples of when a covered business's efforts to respond to an individual request would outweigh any harm to the individual to not acting on the request. Nevertheless, the ATP is concerned this revised definition places onerous responsibilities on

¹⁰ This is true regardless of whether the individual pays for the test; in some instances (e.g., employment, training) the employer may have paid for the test. Even when an individual pays for the test, s/he authorizes the test owner to share the results/scores with certain designated recipients (e.g., schools to which the individual is applying, jobs for which the individual is applying, certification bodies from which the individual is seeking a license or certificate). Either way, the need for a decision-maker, or multiple decision-makers, to obtain the test results/scores is precisely the reason why the individual registered for and took that test.

¹¹ Proposed Regulations, §7001(h).

businesses to demonstrate and document this balancing test. Many testing organizations also deidentify the test takers' information after initial use, so an individual cannot be identified – and thus it is no longer personal information (*see infra.* at fn. 14). They do this because they do not use personal information for test-related research and to follow privacy by design principles including data minimization and purpose limitations. When this is the situation, this new requirement unnecessarily burdens these businesses to conduct such a balancing test, when the situation is simply that they do not any longer have the consumer's personal information and should be able to respond as such. Accordingly, the ATP requests that the Agency revise this definition to reflect the reality of these situations.

3. Financial Incentives

The Proposed Regulation would define “financial incentive” as “a program, benefit, or other offering, including payments to consumers, for the collection, retention, sale, or sharing of personal information. *Price or service differences are types of financial incentives*” (§7063(k)). The Agency proposes to add the last sentence in this definition. This addition creates concerns where testing organizations price their products and services differently and may need additional information to process the request (e.g., when an individual wants to obtain an expedited score report, wants to cancel a score, or wants to reschedule a test). Thus, the Agency needs to modify its proposed language so that when a business legitimately differentiates the pricing for its services, it does not fall under this definition.

4. Definition of “First Party”

The proposed new definition of “First party” means the consumer-facing business with which the consumer intends and expects to interact” (*see* §7063(l)). As indicated in the general overview above, ATP Members, specifically test sponsors, regularly use a variety of service providers to deliver tests that interact more directly with consumers but the test itself has the branding of the test sponsor. ATP is concerned that the use of the words “consumer-facing” are inappropriate in the context of the assessment community and are likely to cause confusion amongst consumers/test takers. Instead, the ATP recommends that the Agency should focus on the formal role of the covered business as the controller of personal data, and continue to require that, if the covered business intends to delegate its responsibilities related to consumers to its service providers, it must do so through a legally binding contract which clearly provides what actions the service providers must perform to comply with the CPRA.

5. Restrictions on the Collection and Use of Personal Information

The Agency proposes to add a new requirement in Section 7002, notably a higher standard for consent: “A business shall obtain the consumer’s explicit consent in accordance with Section 7004 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 is collected or processed. The Agency has provided no definition of what would constitute “explicit consent” and therefore, this proposed language is inappropriate. The ATP contends that when a testing organization presents a legally binding agreement to a test taker prior to the testing session, which is tied to a disclosure notice and privacy policy that comply with the CPRA, the test taker’s acceptance (e.g., using a checkbox or digital signature) is legally sufficient to constitute “explicit consent.” Moreover, this is essentially the same process that is already required for a test taker to give affirmative consent to the collection and use of sensitive personal information. Therefore, the proposal to add the word “explicit” to consent should be dropped.

6. Notice at Collection of Personal Information.

The ATP agrees that only businesses that control the collection of a consumer’s personal information are required to provide a notice at collection. However, the Proposed Regulations in Section 7012 add complex and redundant notice requirements. We urge the Agency to modify its proposal so that a business can meet this requirement by linking directly to its privacy policy that meets the requirements of Section 7011. In Section 7011,

businesses are already required to provide privacy policies that would include the same information, so including another lengthy notice actually inhibits the goal of making it easier for the consumer to understand the business' personal information collection and purposes and adds more complex requirements for businesses. Moreover, as noted earlier, many ATP Members have already developed global privacy programs that follow existing notice and privacy policy requirements. This proposed additional notice requirement only adds unnecessary burdens for businesses and is redundant.

The ATP also objects to the proposed requirement for employers in Subsections (j) and (k) – the CCPA does not currently apply to employment related personal information collected by employers and it is premature to anticipate any legislative change. These subsections would add requirements that are inconsistent with the existing law. We understand that the Agency states this provision would sunset if additional legislation is not passed; however, that approach is antithetical to proper regulatory process, and will cause serious confusion among employers. Thus, this requirement should not be included in the Proposed Regulations at this time.

Moreover, if a request for access to a test taker's personal information involves any actual disclosure of the testing organization's IP, the test taker would not be entitled to access such IP and the business will screen out all such IP from what is made available to test taker.¹² Although we submit that federal patent, trademark, copyright, and trade secret rights are easily understood as potential "conflicts" with a consumer's right to access, the Proposed Regulations fail to provide any explicit guidance in this area. To avoid confusion on this important point, the ATP recommends that the final regulations should provide details for how a business is permitted to deny some or all of a request when its federal IP rights conflict with the consumer's right to access.¹³ See discussion of the impact of a testing organization's IP (*supra.* at p. 4).

7. Notice to "Limit the Use of My Sensitive Personal Information."

The ATP supports the proposed exception that a business using sensitive personal information should not be required to provide notice to limit the use of sensitive personal information when it has disclosed that such information is only for specific purposes aligned with Section 7027 (*see* Section 10, *supra.*). As we have described earlier, many testing organizations readily disclose to every test taker that the use of sensitive personal information is fundamental to their provision of assessment services and to ensure that the test is fair and valid. Equally important, businesses in the assessment industry are collecting sensitive personal information to provide assessment services which test takers have contracted for (or submitted to contractually), to comply with legal and regulatory requirements, and to ensure fairness and validity to test takers in the performance of testing services.¹⁴

¹² The protection of the testing organization's IP is also consistent with the usual terms contained in the test taker agreement, so every test taker will have been put on notice about this restricted access. As discussed in fn. 6, *supra*, test results/scores are likely to be considered by the testing organization to be at least in part covered IP, which will result in denial/partial denial of requests that would entail disclosure of the testing organization's IP.

¹³ Except in the case of trade secrets, a business that owns other IP assets will have evidence of those rights issued by the respective governmental body. The final regulations should merely require the business to provide publicly available information to justify its denial of the request.

¹⁴ Testing organizations use sensitive test taker information that has been anonymized and aggregated to conduct research on building test norms based on various test taker populations, such as age or gender (i.e., the standard of performance on a test, as established by testing a large group of people and analyzing their scores; in norm-referenced testing, subsequent test takers' scores are compared with the test norm to estimate the position of the tested individuals in a predefined population with respect to the competency, skill or trait being

However, for the proposed notice in Section 7014, the ATP submits that a business that is using sensitive personal information consistent with Section 7027 should NOT be required to repeat the statements in their privacy policies a second time – the consumer/test taker engaging with a testing organization can readily read and understand the “specific purposes” laid out in the privacy policy for the permitted purposes for collection (and not for any purposes other than those in Section 7027), as described above (*supra.* at p. 9, Comment 6). Thus, this additional requirement is repetitive and unnecessary.

8. Business Practices for Handling Consumer Requests

a). Although the ATP understands and appreciates the Agency’s efforts to help businesses operationalize consumer requests, we believe a number of the proposals to amend Article 3, Sections 7020-7028 would add significant unnecessary complexity and confusion for businesses and consumers alike. In the assessment industry, as described above *supra.*, at pp. 4-5, a service provider in many instances is the first point of contact for a consumer when and if CCPA and the CPRA amendments are applicable. Thus, it is critical to recognize that in the assessment industry, where a testing organization often uses one or multiple service providers, the data controller must provide a clear delegation of responsibility for compliance, including for handling consumer requests; however, the ATP strongly recommends that the final regulations should require that only the controller should have the responsibility and obligation to resolve any test taker request, no matter if it uses a service provider as the first point of contact.

b). Beyond the basic requirement for a covered business (or controller) to decide any consumer request, the ATP also notes that as proposed in Section 7022 “Requests to Delete,” a covered business would only be in compliance with consumer deletion requests if it “permanently and completely erasing the personal information on the consumer.” As shown above, testing organizations often de-identify test takers’ personal information by anonymizing it and aggregating it for research purposes, whether that is to conduct norming studies or to improve future versions of the test. The ATP recommends that the Agency provide use cases to confirm and clarify these situations.

c). The CCPA makes it clear that a business is free to collect, use, retain, sell, or disclose consumer information that is de-identified or aggregated. *See* Cal. Civ. Code §1798.140(o)(2). The ATP submits it would be helpful for the final regulations specifically to provide examples explaining appropriate uses of such information, including uses in testing, where anonymous personal information has been de-identified and is then aggregated so that no information identifying the consumers is shared or disclosed (*see* fn. 14). Most often, testing organizations include disclosure of such research uses of some personal information on an anonymous and aggregated basis in the test taker agreement, so that they do not have to go back to test takers a second time with a new notice.

measured). As for regulatory requirements, testing organizations providing testing services to employers must be able to enable test user employers/customers to produce evidence to the EEOC or a court showing that use of a specific test did not result in discriminatory outcomes or disparate impact on job applicants or employees in protected categories. *See Uniform Guidelines on Employee Selection Procedures*, adopted by the US Equal Employment Opportunity Commission in 1978, found at 29 C.F.R. § 1607; the *Uniform Guidelines* also have been adopted and applied by the US Department of Justice and US Department of Labor, plus other federal and state agencies, as well as followed by numerous courts including by the US Supreme Court, *see, e.g., Ricci v DeStefano*, 557 U.S., 557 (2007). Another example of the need for a testing organization to retain test taker personal information is to be able to defend itself from test taker claims of violating the Americans with Disabilities Act (*see* 42 U.S.C. § 12189).

d). The ATP strongly supports the Proposed Regulations that permit businesses, service providers, and contractors to delay the deletion of personal information if the requested personal information is archived or in backups. However, the ATP requests additional guidance from the Agency to clarify when it generally should be considered appropriate to keep archived data, which we contend could exist for a multitude of reasons (e.g., to resolve test scoring/reporting challenges, on behalf of testing customers who request extended retention). We recommend that businesses be permitted to archive/backup when they provide a legitimate, documented purpose for doing so. As indicated in Section 7022(d) “If a business, service provider, or contractor stores any personal information on archived or backup systems, it may delay compliance with the consumer’s request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or is next accessed or edited for a sale, disclosure, or commercial purpose.”

e). The ATP again urges that the Agency should impose fewer burdens on businesses, service providers, and contractors with regard to consumers’ “Request to Correct.” In Section 7023 (b), “a business may deny a consumer’s request to correct if it determines that the contested personal information is more likely than not accurate based on the totality of the circumstances.” A long list of factors is provided to help businesses make this determination. However, testing organizations have been encountering requests made in bad faith or that actually represent attempts to circumvent testing fairness and validity procedures. Of particular concern is Subsection (2) that indicates “If the business is not the source of the personal information and has no documentation to support the accuracy of the information, the *consumer’s assertion of inaccuracy* may be sufficient to establish that the personal information is inaccurate.” For the use of assessments to issue certifications and credentials, and other services offered by ATP Members, scores, results, reports, inferences, etc. based on the consumer’s responses, acts, or writings may come from service providers or contractors who are a critical element in the assessment or credentialing process. To permit a mere “consumer assertion” to control the decision to delete personal information would have potentially devastating consequences on a testing organization’s assessments and related products and services. The ATP is very concerned that the business must “rebut” the test taker’s/consumer’s assertions which go to the very heart of the testing psychometric process, developed by and under the professional control of the testing organization, even if it is carried out by a service provider. The proposal would place an extremely onerous and complex burden on the testing organization to overcome a mere “assertion” and we urge the Agency to remove it from the Proposed Regulations.

f). Similarly, the ATP is very concerned about the obligations imposed on businesses in Section 7023 (f)(4) of the Proposed Regulations related to a consumer’s request to correct about a consumer’s health: “if a business rejects a request to correct concerning a consumer’s health, *the right of a consumer to provide a written addendum to the business with respect to any item or statement regarding any such personal information that the consumer believes to be incomplete or incorrect.* The proposal would limit such an addendum to 250 words per alleged incomplete or incorrect item and shall clearly indicate in writing that the consumer requests the addendum to be made a part of the consumer’s record. The ATP objects to this requirement. For example, when a health-related assessment is involved, the test results/outcomes are NOT personal information supplied by the individual test taker, but rather are derived by the testing organization (or the clinician using the test) – it is not appropriate to enable the test taker to challenge test results that are fundamental to the need for the test; this is akin to saying a student may challenge the score on a math test by alleging that the actual results should be different. The second example showing the error of the proposed regulation occurs when the test taker has provided information to support a request for an accommodation; in this case, the testing organization has provided a fixed process by which a test taker is permitted to appeal an adverse decision about whether an accommodation is granted. It would be wholly inappropriate for the Agency to use the Proposed Regulation to intrude into those Americans with Disabilities Act (“ADA”) issues.

g). The ATP supports subsection (h) that permits businesses to deny fraudulent or abusive requests, “if it has a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive.” The business shall inform the requestor that it will not comply with the request and “shall provide an explanation why it believes the request is fraudulent or abusive.” However, Subsection (j), which requires a business to provide all of the consumer’s PI to show what was corrected, is unnecessary and repetitive. This requirement would be very burdensome and resource intensive for businesses, especially where testing organizations, along with its service providers, may process voluminous information on any one consumer for valid test administration purposes – and it again risks exposing a test taker’s PI to another avenue of disclosure. To require such extensive disclosure is incredibly burdensome and, to the extent, the organization has already responded to the consumer’s “right to know” request, it is repetitious.

h). For Subsection 7024 “Right to Know,” the ATP supports directing the consumer to the business’ privacy policy when the consumer’s identity cannot be verified. A testing organization is already required to include detailed descriptions of categories of information collected, the purpose, etc. in its Privacy Policy, so a consumer can easily understand its privacy practices.

i). The ATP objects to Subsection (h) because this provision would require a business to provide records for longer than 12 months from the request date unless it can show the request causes an impossible or disproportionate effort. Requiring a covered business to provide a “detailed explanation” about why it cannot meet this requirement is yet another complex and onerous burden to meet, especially in light of the voluminous requests many testing organizations have been receiving.

In this regard, as we described in the beginning of our comments, the Agency should be aware that there have been increasing requests, including ones that are often misguided and disingenuous attempts by some vendors, researchers, and graduate students, to exercise their individual rights in ways that flood testing organizations with requests not only about the test taker’s “right to know” but also for deletion, copies, etc. There has been a significant uptick in these types of requests, which have already become an overwhelming burden for testing organizations.¹⁵ In fact, there is apparently no cut-off date for when a business needs to go back to provide available personal information. For testing organizations, where individuals may test several times over extended periods of time, such a proposed regulation would require looking back well beyond one year, covering multiple testing events. It is equally possible that application of the proposed regulation would be inconsistent with the testing organization’s existing retention policy for test takers’ personal information. Accordingly, the ATP urges the Agency to remove both the requirement that businesses must provide a detailed description about why the request was denied beyond lack of verification, and that businesses should be required to look back beyond 12 months for any individual’s personal information. While the ATP believes that no business should be required to respond to requests for more than a one-year period of time, at a minimum, the Agency should modify its proposal to require the individual requester to identify the specific time frame within which the person is seeking information if it is outside of one year’s records, so the business is able to focus its response on a clearly defined time period.

9. Section 7025 Opt-out Preference Signals and Section 7026 Opting out of Sale/Sharing

In general, testing organizations are NOT selling or sharing consumers’ personal information – their use of PI is internal (e.g., research to establish test norms or to improve the tests themselves) or is shared with service providers under contract in the performance of testing services. However, in some instances, a testing organization may use data analytics service providers to assist with operations of their websites and testing platforms. In these instances, the business would have an agreement with an analytics service provider and this still would not

¹⁵ See, IAPP article on these requests and compliance concerns: [Why some data subject request services create compliance concerns \(iapp.org\)](https://iapp.org).

constitute any “sale” or “sharing” of personal information so long as the contract limits any use of PI by the service provider beyond the purposes disclosed by the controller.

Moreover, some testing organizations may include on their websites’ social media widgets where a user can click on these to share information about the business’s products and services or to communicate with other interested individuals/groups. In these circumstances, the consumer/test taker chooses to interact with those third-party sites and, generally speaking, the business notifies consumers in its privacy policy that any third-party links are subject to that third party’s privacy policy and notices. We recommend that the Agency provide additional use case examples in the Proposed Regulations that confirm that these situations are exempt from the opt-out and notice requirements.

10. Section 7027. Requests to Limit Use and Disclosure of Sensitive Personal Information.

The ATP supports Section 7027 of the Proposed Regulation that businesses are not required to provide these notices, nor honor requests to limit use and disclosure of sensitive personal information when used in accordance with the allowed purposes indicated in Subsection (1). ATP Members, as noted earlier, use sensitive personal information for test administration and other purposes that generally are reasonably expected by their customers and test takers and for the other purposes specified in Subsection (1). The ATP also believes that there are other legitimate purposes for use of sensitive personal information that may not be listed in this Subsection, including to prevent fraud, to ensure fairness in testing, to respond to government or law enforcement orders, etc. (e.g., to comply with the EEOC *Uniform Guidelines [see fn. 14, supra.]*, in response to growing data requirements under various Diversity, Equity, and Inclusion initiatives). Accordingly, the ATP requests that the Agency should add to this subsection (1) another category for purposes where the covered business can use its reasonable discretion to use sensitive data and also to allow for its legitimate purposes, including legal bases, related to the provision of its products and services.

11. Article 4 Service Providers, Contractors, and Third Parties

Section 7050 indicates that service providers that would otherwise be subject to the CPRA/CCPA but that are providing services to nonprofit organizations and government agencies, are exempt under these Proposed Regulations. The ATP supports this clarification to make clear that providing services to nonprofits or government agencies are NOT subject to the CPRA/CCPA. As we have noted, testing organizations often provide testing services/processing to nonprofit organizations (e.g., test sponsors) and government agencies (e.g., state school districts, state and local employers) and they have structured their compliance programs with the understanding that these organizations are not subject to the CCPA requirements. The ATP submits it would be useful for the Agency to provide some examples for clarity to prevent misunderstandings of this exemption.

In Section 7051 “Contract Requirements for Service Providers and Contractors” the Proposed Regulations prescribe extensive provisions that businesses must include in their contracts with their service providers and contractors. Testing organizations generally conduct significant and sufficient due diligence with service providers/contractors and based on that information, delegate privacy (and associated security) responsibilities under their contracts. However, the ATP objects to specific prescriptive due diligence the Agency would require of a business under the Proposed Regulations; instead, a business should be allowed greater flexibility with respect to its due diligence efforts that align with the facts and circumstances of its relationship with a particular service provider or contractor, especially if that relationship is well-established and has allowed both entities to build an agreed process/protocol for how they interact. For smaller businesses, for example, conducting an automatic annual audit where the testing organization has no evidence of any auditable issues could be a serious burden resulting in significant additional costs, which would be passed along to consumers.

Related to Section 7052 “Third Parties,” the ATP has concerns specifically with the requirement that businesses flow down requirements to the third party when the business receives a consumer request to delete or opt out of the sale/sharing, as the third party is required in subsection (c) to recognize the opt out signal. While the ATP supports the requirement for third parties to recognize the opt out signals from consumers, we do not believe

that testing organizations generally have any reason to provide sensitive personal information to third parties, where the “flow-down” privacy requirements of Section 7053 would come into play. Thus, this proposal creates an unnecessary burden on businesses and from a practical standpoint it is nearly impossible to effectuate a flow-down of privacy requirements because testing organizations have little leverage over many of these third parties (e.g., social media links for test takers’ use). Indeed, most testing organizations only use analytics providers to better operate their test delivery platforms and for website operations, although they may provide links to their own social media pages where test takers can access resources and convene with peers, and where members of the testing community can interact. They do not intend for these third parties to use personal information for their own purposes and certainly do not want any personal information used for any targeted ads or marketing for the third parties and their other customers. The ATP recommends that the Agency should revise the Proposed Regulations so they directly address such third-party vendors who misuse consumers’ personal information obtained from consumers through links from a business’s website for their own purposes to target ads, marketing or other purposes that are not directly related to the intended, contracted testing services purpose.

12. Section 7304. Agency Audits.

The ATP urges the Agency to limit its auditing power by providing more objective criteria so businesses understand the requirements and can prepare for such audits. The majority of ATP members take their compliance with the CCPA very seriously and they will need to understand when the Agency can conduct an audit and what records or systems will be audited with more specificity. Such information will enable businesses to have the proper personnel on site to comply with the audit requests, and to respond to questions in a cooperative manner. For example, the ATP submits that the Agency should adopt audit guidelines that give businesses advance notice of an audit, except in the most egregious situations. Moreover, audits should only occur when there is strong evidence of noncompliant activities and should not be based solely on consumer complaints.

CONCLUSION

On behalf of the international testing and learning industry, the ATP has provided comments on the Proposed Regulations for implementing the CPRA. We have focused on a variety of unique circumstances that are common in the assessment industry which should be considered by the Agency. Additionally, we note that many testing organizations are smaller/medium-sized businesses that would be compelled to comply with more complex, onerous requirements. Together, we believe these reasons justify modification of the Proposed Regulations when balanced against the rights of individual test takers as consumers.

In summary, our recommendations center on providing a more practical, flexible approach for these Proposed Regulations, taking into consideration specific circumstances of testing organizations. These include: (1) recommendations that requirements for authorized agents and third parties should be expanded and businesses are not themselves compelled to ensure third party compliance other than through contractual language; (2) a more practical approaches avoiding burdensome, repetitive requirements, including more flexibility for covered businesses to document the effort and due diligence of services providers and third parties; (3) modifying the definition of financial incentives that reflect legitimate prices differences; (4) greater focus on the actual businesses that control the processing of personal information instead of a first party definitional approach; (5) removal of unnecessary requirements related to explicit consent for new purposes, realistic requirements related to privacy policies and notices (for personal information and for sensitive personal information); (6) not allowing as non-rebuttable those consumer assertions and addendums related to their data; and (7) not including premature requirements related to employee data. Moreover, the ATP contends that the Agency needs to remove practices that could result in the disclosure of personal information unnecessarily and that could lead to harm to consumers, such as requiring that a covered business provide “all of the consumer’s personal information” to show

what was corrected and further requiring going beyond 12 months for a “look back” period related to consumers’ information requests. This and other requirements are contrary to well established privacy principles and are onerous requirements on smaller covered businesses. Furthermore, we recommend that the Agency limit its audits of covered businesses and provide more objective criteria for such audits to allow businesses, such as those in the testing industry, to continue their good faith efforts of compliance.

We also recommend that the Agency provide more use cases to clarify the appropriate use of personal information by covered businesses, including: (1) related to IP rights and the rejection of consumer requests; (2) showing how deidentification and archiving of data meets consumers’ deletion requests; (3) how the use of analytics and social media service providers for businesses’ analytics and customer services purposes falls under the service provider requirements and is exempt from the “opt out of sharing” notice requirements; and (4) adding more examples of service providers working with nonprofits and government agencies as being exempt from these requirements.

Thank you for your attention to the important issues raised by the ATP on behalf of the global assessment industry about the Proposed Regulations implementing the CRPA by affected testing organizations located both within and outside of California. The ATP would be pleased to answer any questions the Agency may have in response to these comments, including to do so in a virtual or face-to-face meeting. For any follow up, please contact our General Counsel at the email address shown below.

Sincerely,

ASSOCIATION OF TEST PUBLISHERS

William G. Harris, Ph.D.
 CEO
 601 Pennsylvania Ave., NW
 South Bldg., Suite 900
 Washington D.C. 20004

Alina von Davier, Ph.D.
 Chair of the ATP Board of Directors
 Chief of Assessment
 Duolingo
 5900 Penn Ave.
 Pittsburgh, PA 15206

Alan J. Thiemann
 General Counsel

Alan J. Thiemann and Donna McPartland
 Han Santos PLLC
 225 Reinekers Lane
 Suite 410
 Alexandria, VA 22314
 [REDACTED]

From: **Boudreau, Sarah** [REDACTED]
To: **info@CPPA** <info@cpga.ca.gov>
Subject: 8/24-8/25 CPPA Board Meeting
Date: 22.08.2022 20:17:59 (+02:00)

WARNING: This message was sent from another CA Gov Agency: [REDACTED]. Please use caution opening attachments.

Good afternoon,

I'm reaching out on behalf of some of Assemblyman Kiley's constituents who expressed some concerns with the CPPA and the work being done to add additional regulations to the CCPA and CPRA. We wanted to pass along their thoughts ahead of this week's board meeting:

- California's ever-changing privacy laws are creating confusion, uncertainty, and compliance problems for consumers and the business community. Businesses were hit with extraordinary challenges during the pandemic and are now navigating inflation and increased fuel and energy costs. The state is now adding more costs, requirements, and uncertainties on business operations.
- In the economic and fiscal impact statement, the CPPA has estimated initial compliance for a small business to be \$128 and increased labor hours for 1.5 hours. We are highly concerned that the compliance statement is severely understating the burden on small businesses. The cost for one hour of consultation to determine privacy compliance needs alone would exceed the estimate put forth by the agency. Examples of costly and burdensome compliance measures could include hiring consultants, lawyers, staff, updates to technology systems, and increased labor needed to respond to consumer data requests, and to prepare for cybersecurity audits and risk assessments.
- There is already a long laundry list of economic pressures and government mandates getting piled onto the backs of small business owners - historic inflation, minimum wage and compensation increases, higher gas prices, regulatory mandates from the CA Air Resources Board scoping plan, and new COVID health requirements and sick leave, just to name a few.

Thank you!

Sarah Boudreau

Legislative Director
Office of Assemblyman Kevin Kiley
6th Assembly District
Office: (916) 319-2006

From: **Ferrell, Peter** <[REDACTED]>
To: **Regulations** <Regulations@cpga.ca.gov>
Subject: CPPA Public Comment
Date: 22.08.2022 21:41:35 (+02:00)
Attachments: NEMA - CPPA Comments - FINAL.pdf (2 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Mr. Soublet,

Please see attached NEMA's comments regarding the CPPA's current rulemaking. Please let me know if you have any questions or require additional information.

Sincerely,

Peter Ferrell
Manager, Connectivity and Data Policy
National Electrical Manufacturers Association
1300 17th Street North, Suite 900
Arlington, VA 22209-3801
[REDACTED]





National Electrical Manufacturers Association

The association of electrical equipment
and medical imaging manufacturers
www.nema.org

August 23, 2022

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

RE: *Notice of Proposed Rulemaking; July 8, 2022*

Submitted via regulations@coppa.ca.gov

To Whom It May Concern:

The National Electrical Manufacturers Association (“NEMA”) is the leading U.S. trade group representing nearly 325 electrical equipment and medical imaging manufacturers that are at the forefront of helping the nation successfully transition to an electrified, connected, and decarbonized economy. Specifically, more than 65 electroindustry companies employ roughly 25,000 employees who produce this important equipment within the State of California. NEMA appreciates the opportunity to provide comments to the California Privacy Protection Agency’s (“CPPA”) proposed rules implementing the California Privacy Rights Act (“CPRA”) amendments to the California Consumer Privacy Act.

For years, NEMA has promoted the design, development, and adoption of so-called “smart buildings” as well as for the increased operational performance and efficiency of buildings in general. Buildings consume 70% of all electricity and 40% of primary energy in the United States; existing technologies such as lighting, energy-efficient motors, variable-speed drives, integrated building controls, and automation systems can reduce building energy consumption by 50% - 70% on average¹. Enabling a building to use these technologies effectively, efficiently, and safely relies on its ability to collect data properly but easily, mainly generated through sensors.

The type of information and data collected through sensors depends on the operational goals of a structure’s management and/or owner. (Energy efficiency, noted above, can be one such goal.) Not all data necessary to achieve a goal is sensitive or personal; the use of aggregated and anonymized data can help optimize a building’s operational technologies, mechanisms, and hardware. However, buildings are acquiring more and more information through the incorporation of Internet of Things (IoT) devices, wireless networks, and other data platforms². Such information can be more granular and specific to an individual; allowing managers to cater to the preferences of tenants, employees, guests, and consumers generally.

NEMA applauds the CPPA’s effort to put forth rules to protect consumers from the exploitative and harmful consequences of data mismanagement, insecurity, and improper handling. However, we urge the agency to be flexible in its rulemaking. In its pursuit to safeguard the collection and handling of personal and sensitive information, CPPA rules should not be so rigid as to disincentivize technological innovation

¹ <https://www.nema.org/directory/nema-councils/high-performance-buildings-council>

² <https://www.nema.org/news-trends/ei/view/enabling-ai-within-smart-buildings>

or dissuade managers and/or owners from incorporating high-performance technologies and systems in their buildings.

Section 7002: Restrictions on the Collection and Use of Personal Information.

The CPRA text allows businesses to collect and use both personal information and sensitive personal information if it is “*necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods and services.*”³ In Sections §1798.140(e)(2), (4), (5) and (8), the legislative text states how such consumer information can be used, so long as the purpose for collecting such information is disclosed.

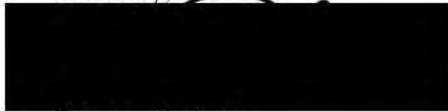
High-performance and smart buildings, by their very design and definition, are expected to collect and process information in seamless and creative ways, which makes them appealing to consumers and help attract capital investment. However, the CPPA’s proposed regulations state that a business “*shall obtain the consumer’s 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.*”⁴

NEMA is concerned that under this proposed rule, the ‘explicit consent’ requirement could significantly deter building managers and/or owners from pursuing high-performance and smart building technologies. For example, luxury hotels, casinos, and convention centers are designed purposefully to enhance an individual’s experience; in many ways consumers and guests expect these buildings to be cutting-edge and interactive, especially through IoT devices like a cellphone. A strict prohibition on collecting personal information and sensitive personal information without explicit consent may place many modern facilities such as these out-of-compliance, since they are intended to seamlessly collect data.

Again, the electroindustry encourages the CPPA to consider the broad ramifications of applying a strict opt-in standard, including on business goals and outcomes. Consumer data should be collected, handled, and processed in a responsible and secure manner. NEMA believes rules can be crafted which incentivize good business behavior while being flexible and allowing for technological innovation and integration.

NEMA thanks the CPPA for the opportunity to submit comments to these proposed rules and looks forward to working with the agency in forthcoming rulemakings. Should you have any questions, please contact me.

Sincerely,



Spencer Pederson
Vice President, Public Affairs

Endnotes

³ <https://cpra.gtlaw.com/cpra-full-text/>

⁴ https://cppa.ca.gov/regulations/pdf/20220708_text_proposed_regs.pdf

From: **Lior J. Strahilevitz** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
Subject: CPPA Public Comment
Date: 22.08.2022 21:42:30 (+02:00)
Attachments: CPRA Public Comment - UChicago NorthwesternU.pdf (7 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

To the CPPA:

Attached please find a Comment on the proposed CPRA regulations from a team of scholars affiliated with the University of Chicago and Northwestern University.

Thank you,

Lior Strahilevitz



Aug 22, 2022

Before the
California Privacy Protection Agency,
State of California

CPRA Public Comment

Thank you for the opportunity to provide comments on the proposed regulations of the California Privacy Rights Act. We are academic researchers associated with the University of Chicago and Northwestern University who focus on privacy. We draw on our collective experience in computer science and law to encourage the California Privacy Protection Agency to resist watering down the strong and sensible protections established by the proposed regulation. We also offer some concrete suggestions to enhance transparency, efficiency, and clarity in the regulations. We recognize the importance of the proposed regulation not only for the protection of Californian’s privacy but also as a model for other jurisdictions.

1. General Support of the Proposed Draft

First, we commend the Agency for expanding the regulatory provisions that protect consumer privacy. There are a number of changes that we feel the Agency included that will significantly improve consumer privacy. We highlight a subset of these changes here. Defining and including Sensitive Personal Information (SPI) as a new category of personal information to be protected similar to the European Union’s Special Category Data under Article 9 of GDPR. The Agency opted to expand on the EU’s category to include additional sensitive consumer data like text messages and emails, further protecting consumers from unwanted surveillance. The Agency expanded the rights to know/access/opt-out given to consumers by the CCPA to now also include not just the selling of consumer data but also the sharing of consumer data. We strongly support this change, as the unsolicited sharing of personal information can be as much of a violation of privacy as selling it. The CPRA also includes new rights not included in the CCPA such as the right to rectify incorrect information and the rights to access information about the use of personal data in automated decision making (‘profiling’) and to opt-out of

automated decision making. Lastly, the Agency added necessary provisions that specify obligations for third parties/contractors/service providers, filling potential gaps in the consumer data life cycle.

2. Standardized Access and Site Location

As Internet researchers, we are familiar with the large differences in approaches to policy that platforms use. The language adopted, navigability, and accessibility to establish these policies are all a matter of variance by platform. We recognize the provisions that enforce Ease of Understanding, Symmetry, Straightforward Language, Ease of Execution, and Providing Instructions, but we suggest the Agency considers including a clause approximating Easy to Find. Easy To Find is crucial for usability since prior research has shown, for instance, that even when privacy options are available to users, if they cannot find them, they are often unused. Even further, the Agency could enforce a standardized location for information and disclosures. For example, all information relevant to these regulations could be accessible from [www.\[platform\].com/privacy](http://www.[platform].com/privacy). Standardizations such as this one would make it easier for consumers to exercise their rights, agencies to perform auditing, researchers to study platform practices and policies, and allow companies to not have to make all new decisions from a blank slate. Further, without such standardizations, companies may continue to bury their options in a variety of settings forcing consumers to intuit their way through sometimes unintuitive settings (some unintuitive interfaces may still not be considered full-on dark patterns). The Agency may also consider going even further to smoothen the transition for company compliance, such as providing compliance guidelines like the guidelines provided by the FTC or EU.

3. Section 7002's Connection to Consumer Expectations Improves Transparency and Predictability in the Law

The proportionality principle embedded in Section 7002 is a beneficial approach for privacy regulation. Proportionality is a concept that is central to various domains of domestic data privacy law. See, e.g., Christopher Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* (2007); Margot E. Kaminski, *Privacy and the Right to Record*, 97 *Boston Univ. L. Rev.* 167 (2017); Lior Jacob Strahilevitz, *Reunifying Privacy Law*; 98 *Cal. L. Rev.* 2007 (2010). Proportionality has become central to the GDPR approach to regulating personal data in Europe as well. See Miriam Kohn, *Clearview AI, TikTok, and the Collection of Facial Images in International Law*, 23 *Chi. J. Int'l L.* 195 (2022). It is also at the core of the duty of loyalty contained in the proposed federal privacy law.

The proposed regulation provides very helpful clarification about how firms and regulators will conduct proportionality analysis by incorporating consumer expectations. What kinds of collection, use, retention, and sharing data is expected by an average consumer is an empirical question. Fortunately, it is one that scholars have studied in great depth and with increasing sophistication. See, e.g., Kirsten Martin & Helen Nissenbaum, *Privacy Interests in*

Public Records: An Empirical Examination, 31 Harv. J. L. & Tech. 111 (2017); Roseanna Sommers & Vanessa K. Bohns, The Voluntariness of Voluntary Consent: Consent Searches and the Psychology of Compliance, 128 Yale L.J. 162 (2019); Lior Jacob Strahilevitz & Matthew B. Kugler, Is Privacy Policy Language Irrelevant to Consumers?, 45 J. Legal Stud. S69 (2016). Empirical researchers have coalesced around best practices, including the need for the replication of research results and the formulation of expectation questions to respondents in a neutral way.

A great virtue of the empirical approach is that it enables regulated firms to anticipate the content of government regulation and enforcement. That is, if firms are uncertain about the application of proportionality review to an emerging technology they are considering employing, they can, at a moderate cost, employ the tools that disinterested academic researchers have been using to assess the expectations of their customers, or consumers generally. Some privacy-invasive practices are consistent with consumer expectations and others are sharply inconsistent with them, and firms' business practices and user-interfaces can alter those expectations. See Sara Katsanis et al., A Survey of U.S. Public Perspectives on Facial Recognition Technology and Facial Imaging Data Practices in Health and Research Contexts, 16 (10) PLOS One (Oct. 14, 2021); Matthew B. Kugler, From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms, 10 U.C. Irvine L. Rev. 107 (2019). Making the expectations of an average consumer an important part of the regulatory inquiry permits firms to engage in profitable practices that leverage the economic value of consumers' data. But it requires these firms to be highly transparent about what they are doing so that consumers who object to those practices can make an informed decision to take their business elsewhere.

This is not to say that a firm that conducts surveys and experiments to assess the relationship between a particular business practice and consumer expectations is in the clear and can claim a safe harbor under the regulation. Firms that employ hired guns with social science training to produce biased, self-serving survey and experiment results should not be permitted to engage in unnecessary and disproportionate privacy-invasive practices. Rather, if a firm conducts a serious and fair-minded investigation of consumer expectations before launching a product or engaging in a new practice and determines that its contemplated actions are consistent with most consumers' expectations, it is quite likely that the same results will be obtained months or years later when a regulatory entity evaluates consumer expectations. That is because citizens' privacy expectations tend to be stable over time. See Matthew B. Kugler & Lior Jacob Strahilevitz, The Myth of Fourth Amendment Circularity, 84 Univ. Chi. L. Rev. 1747 (2017). The proposed regulations' expectations-based approach thus makes the content of the law transparent and relatively easy to anticipate. Under Section 7004(a)(4)(C) of the proposed regulation, this tie to consumer expectations also enhances transparency and predictability in the definition of dark patterns.

Well-run firms already invest in learning what their customers want and expect. The proposed regulation provides further legal compliance incentives for firms to understand their current and potential customer base. Coupled with the CPRA's disclosure obligations, this increases the efficiency of the market in sorting consumers across companies.

4. Section 7004's Symmetry in Choice Approach is Appealing

There is little question that dark patterns are proliferating online. See Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Paloma & Alberto Bacchelli, *UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception*, Proceedings of the CHI Conference on Human Factors in Computing Systems (2020); Arunesh Mathur, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty & Arvind Narayan, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Sites*, Proceedings of the ACM Human-Computer Interaction Conference (2019). There is also a growing empirical literature examining the effects of dark patterns on consumer choice. See, e.g., Colin M. Gray et al., *End User Accounts of Dark Patterns as Felt Manipulation*, ACM Computer-Human Interactions Conference Proceedings (2021); Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 *J. Legal Anal.* 43 (2021); Stefan A. Mager & Johann Kranz, *On the Effectiveness of Overt and Covert Interventions in Influencing Cookie Consent: Field Experimental Evidence*, 42nd International Conference on Information Systems (2021); Midas Nouwens et al., *Dark Patterns after the GDPR: Scraping Consent Pop-up Ads and Demonstrating their Influence*, CHI Conference Proceedings (2020). These studies reveal that particular dark pattern techniques successfully manipulate consumers into purchasing goods or services that they do not wish to purchase, retaining subscriptions that they prefer to cancel, or surrendering personal information that they prefer to keep private. See Luguri & Strahilevitz, *supra* and Nouwens et al., *supra*. Dark patterns further engender feelings of frustration as consumers feel manipulated. See Gray et al, *supra*.

The dark pattern examples identified in the regulation are among the most pernicious techniques currently employed in e-commerce. For example, the use of double-negatives is highly effective in manipulating consumers, with consumers often signing up for services they believe they have rejected. Nagging, obstruction, visual interference, confirmshaming, default terms, and fine print have been demonstrated to be quite effective at convincing consumers to sign up for dubious services without sparking a substantial consumer backlash, as long as the techniques are used subtly and in moderation. See Luguri & Strahilevitz, *supra*. The proposed regulations' examples provide helpful context for market participants who are trying in good faith to comply with the law.

While dark patterns are a broad phenomenon, the asymmetry present in user interfaces often indicates the presence of a dark pattern. Thus, a company may permit customers to sign up for a subscription in one click but require customers to mail a letter via snail mail or navigate

through multiple screens to cancel. That structure will rarely be accidental, and even if the asymmetry results from an innocent design mistake, its ongoing effects should be obvious. Hence Section 7004's emphasis on symmetry of choice is wise.

To be sure, there will be instances in which it is appropriate for a firm to introduce some modicum of friction. For example it would make sense for an email provider to ask "Are you sure?" before deleting a customer's account and all of their emails, provided confirmshaming and other one-sided techniques are not employed. Such a screen reduces the probability that an unwanted outcome will result from an errant click. But a firm can avoid any concerns about liability for introducing such friction by introducing a symmetrical "are you sure?" prompt at the account creation stage. Beyond that clarification, we offer several suggestions to improve the proposed regulation's symmetry in choice framework.

First, we recommend expressing Section 7004(a)(2) in terms of consumer effort as well as the number of steps necessary to opt in or out of sharing. A choice architecture that allows users to opt out of the sale of their personal information through two clicks on pages that require a typical consumer to read 1000 words of text and allows users to opt in to the sale of their personal information through two clicks on pages that require a typical consumer to read 100 words of text is not symmetrical. Consumer effort includes both the number of screens a consumer has to click through and the time it will take a typical consumer to read the materials pertinent to making a well-informed choice. Symmetry in choice should permit regulators to evaluate friction introduced in interface design from the perspective of both the number of steps necessary to make a choice effective and the time required for a typical consumer to do so.

Second, we recommend clarifying that symmetry of choice principles are applicable to Section 7026(j)'s discussion of CCPA opt-outs. It is asymmetrical for firms to ask consumers who have opted out of personal information sharing to opt-in every twelve months if those firms do not also ask consumers who have opted in to personal information sharing whether they wish to opt out every twelve months. It would be symmetrical for firms to either respect any initial consumer choice until the customer affirmatively requests a different choice or to provide every consumer with an annual decision about whether to continue or change their current choice.

Third, special care should be taken when constraining firms' choice of default terms. Section 7004(a)(2)(E) provides that a "choice where the option to participate in a financial incentive program is selected by default . . . is neither equal nor symmetrical." Default terms are inevitable in some instances so as to ensure that consumers are not overwhelmed with an excessive number of choices. A firm that implements a default term that is demonstrably desired by the majority of its customers or potential customers has not employed a dark pattern. For example, many credit card issuers provide their customers with 1% cash back on all card purchases. A credit card issuer that enables cash back by default (or that makes cash back a

mandatory condition of participating in the card program) rather than forcing customers to affirmatively opt-in to receiving cash back should not be construed as having violated Section 7004(a)(2)(E). Empirically sound customer surveys along the lines of those described in our discussion of Section 7002 can help firms establish that particular default provisions are desired by most of their customers and therefore permissible.

5. Kid Friendly: 7070-7072

Sections 7070-7072 pertain to the special provisions for consumers under the age of 16. We stress the importance of protecting privacy related to vulnerable populations such as children. The provisions say little about how the options or disclosures should be presented to children. We recognize that Section 7004 requires consent language to be easy to understand, but we submit that language for children may require additional consideration. If information is required to be given to children, it needs to be in a way that is understandable to them, as children may not understand the same language that is directed for adults.

* * *

As platforms mine consumer data to increase user engagement and financial gain, the CCPA and CPRA can serve as important sources of protection for Internet users. The Agency can aid users by raising awareness about privacy and the dark patterns used to undermine it, providing more rights to consumers, and keeping companies accountable through enforcement and audits. As research suggests, correcting the asymmetry in privacy choices and enforcing better privacy defaults are likely to significantly increase consumer privacy. Meaningful regulation is necessary to protect consumer autonomy and welfare. We are available to assist the Agency towards the goal of protecting user privacy amidst the dominant economic systems commodifying consumer data.

Respectfully submitted,

Marshini Chetty
Assistant Professor, Department of Computer Science, University of Chicago

Matthew Kugler
Associate Professor of Law, Northwestern University

Brennan Schaffner
Graduate Student, Department of Computer Science, University of Chicago

Lior Strahilevitz
Sidley Austin Professor of Law, University of Chicago Law School



Contact:

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

From: **Rachel Michelin** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
CC: **Ryan Allain** [REDACTED]
Subject: CPPA Public Comment
Date: 22.08.2022 21:43:25 (+02:00)
Attachments: CalRetailers CCPA Reg comments.docx.pdf (9 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

On behalf of the members of the California Retailers Association, please find our comments and concerns regarding the proposed regulations related to consumer privacy.

If you have any questions or would like to discuss in more detail, please do not hesitate to reach out to me directly.

Rachel

Rachel Michelin

President & CEO
1121 L Street, #607
Sacramento, CA 95814
P:916/443-1975



[REDACTED]
@CRAgovtaffairs



August 22, 2022

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

VIA Email: regulations@coppa.ca.gov.

Dear Members of the Committee:

On behalf of the California Retailers Association please see our comments related to the California Consumer Privacy Act Regulations and the formal rulemaking process to adopt regulations to implement the Consumer Privacy Rights Act of 2020 (CPRA).

We have general comments we would like considered as you navigate the rule making process. Specifically:

- **Privacy Request Notifications to Service Provider/Third Party/Contractors.** There are various notification requirements between a business provider and its service provider, contractor, and third party upon a data subject request (e.g., delete, correct, opt out). The draft regs provide no exemption from providing notification even if a business knows a service provider is not going to delete the data due to an exemption or has already purged the data per a short retention schedule. The notification requirement propagates personal information unnecessarily and goes against the data minimization principle.
- **Explanation Related to Fraudulent/Abusive Requests.** The draft rule requires the business to explain in detail why it denied a request because it is fraudulent or abusive. It increases security concerns if a business is required to disclose its fraud detection measures to the potential fraudster who may use the information to circumvent the business's verification system.
- **Professional or Employment-Related Information Should Be Defined to Mean the Personnel File.** Initially, the Agency should clarify that "professional or employment-related information" under the CPRA (Cal. Civ. Code § 1798.140(v)(1)(I)) means an employee's personnel file consistent with employees' and employers' understanding of the type of data they are generally entitled to receive and disclose in response to access requests. For clarity and consistency, the Agency should consider providing examples of the type of data that is considered part of the personnel file based on guidance provided by the Division of Labor Standards Enforcement: Categories of records that are generally considered to be "personnel records" are those that are used or have been used to determine an

employee's qualifications for promotion, additional compensation, or disciplinary action, including termination. The following are some examples of "personnel records" (this list is not all inclusive):

1. Application for employment
2. Payroll authorization form
3. Notices of commendation, warning, discipline, and/or termination
4. Notices of layoff, leave of absence, and vacation
5. Notices of wage attachment or garnishment
6. Education and training notices and records
7. Performance appraisals/reviews - 3 - 8. Attendance records See California Department of Industrial Relations, Personnel Files and Records.

https://www.dir.ca.gov/dlse/faq_righttoinspectpersonnelfiles.htm

If the CPRA's definition of "professional or employment-related information" fails to align with employment laws, employees and employers will equally be confused about their respective rights and obligations under the law. Until January 1, 2023, both employees and employers know what obligations and rights exist regarding employee data (e.g., access, retention, correction, and non-discrimination), as described above. However, when the CPRA becomes operational, unless the Agency closely aligns "professional or employment-related information" with existing employment laws, current clarity will disappear. For example, certain data generated during the course of employment, such as business emails, PowerPoint decks, data regarding the company's intellectual property, financial spreadsheets, feedback submitted on behalf of other employees, etc., is not employee personal information; rather, it is company data (collectively, Company Data). Extending CPRA rights to Company Data would not be in the employees' interests because it does not involve their personal employment history and records and could potentially reveal the personal information of other employees if, for example, business emails to and from several employees reveal personal details about one employee's life or views regarding a supervisor or other co-workers.

In addition, providing employees access to Company Data could be detrimental to the employer's interest because such records may contain company trade secrets and proprietary information, which fall outside the CPRA's scope. See Cal. Civ. Code § 1798.145(a)(1) & (b). Further, requiring an employer to disclose Company Data in response to an access request imposes significant time and resources constraints because the volume of data involved in an employee request could be akin to an e-discovery request in litigation, which can often eclipse more than \$100,000 in a single-plaintiff employment lawsuit. Companies could be forced to retain outside e-discovery vendors for each access request because of the volume of data involved, which would increase employers' costs, be of little benefit to employees, and further drive businesses out of California.

This would translate into fewer jobs and opportunities for Californians. Accordingly, to avoid creating such confusion and concerns for both employees and employers, the Agency should define "professional or employment-related information" to mean the personnel file as defined by the Division of Labor Standards Enforcement, which is consistent with existing employment rights and obligations.

Below are California Retailer's comments on specific sections:

Article 1. GENERAL PROVISIONS

§ 7001. Definitions.

7001(c): Deletes requirement for authorized agent to register. Retailers are concerned this could lead to a proliferation of agents with no way for consumers or companies to confirm legitimacy, deal with abusive practices (e.g., sending notices to every company indiscriminately, leading to proliferation of requests). **Retailers ask for clarity.**

7001(h): Defining disproportionate effort is helpful. Retailers ask for consideration on adding the data is used for legal, compliance **or security** purposes (add "security"). We also ask for consideration on changing "significantly higher" to "higher."

7001(k): Definition of financial incentives. Retailers ask for consideration on references related to making a price or service differentials as financial incentive.

§ 7002. Restrictions on the Collection and Use of Personal Information.

In their current form, the draft regulations create confusion for businesses concerning the relevant notice and choice standards for certain processing and whether such processing is permissible in any case. Specifically, the statute permits advertising activities, including those that would constitute a "share" or a "sale," provided the business offers appropriate disclosures and offers and honors an opt-out for these activities.

The draft regulations, however, state that (a) processing, even for "disclosed purposes," is limited to what an average consumer would expect; and (b) any processing that is "unrelated or incompatible with the purpose(s) for which the personal information was collected or processed" requires the consumer's explicit consent. *Section 7002(a)*. This language introduces ambiguity as to whether targeted advertising is, in fact, permissible with appropriate notice and opt out, or instead is only permissible with a consumer's opt-in consent or even entirely impermissible.

In preparing compliance plans for CPRA, retailers request clarifying that this is permissible with appropriate notice and opt out. This change would avoid undermining otherwise compliant activities, which are clearly permitted by the statute, that retailers rely upon to run their businesses, reach their customers, and attract new ones.

Proposed Revisions:

Option A: Strike Section 7002(a) of the Draft Regs in its entirety since the concept is addressed in 1798.100(c) of the statute.

Option B: Revise Section 7002(a) of Draft Regs as follows:

*A business's collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purpose(s) for which the personal information was collected or processed. To be reasonably necessary and proportionate, the business's collection, use, retention, and/or sharing must be consistent with what an average consumer would expect when the personal information was collected **or**. ~~A business's collection, use, retention, and/or sharing of a consumer's personal information may also be for other disclosed purpose(s) if they are compatible with~~ **the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes what is reasonably expected by the average consumer. If a business discloses information about***

*sales or sharing it engages in as required by these regulations and the CCPA, then the associated processing is subject to the obligations related to such activities set forth in these regulations and the CCPA and does not require explicit consent. A business shall obtain the consumer's explicit consent in accordance with section 7004 before collecting, using, retaining, and/or sharing the consumer's personal information for any purpose that is **not disclosed to the consumer and is unrelated or incompatible with the purpose(s) for which the personal information collected or processed.***

Option C: Revise Section 7002(a) of Draft Regs as follows:

7002(a): A business's collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purpose(s) for which the personal information was collected or processed. ~~To be reasonably necessary and proportionate, the business's collection, use, retention, and/or sharing must be consistent with what an average consumer would expect when the personal information was collected.~~ A business's collection, use, retention, and/or sharing of a consumer's personal information may also be for other disclosed purpose(s) if they are compatible with ~~what is reasonably expected by the average consumer~~ the context in which the personal information was collected. A business shall obtain the consumer's explicit consent in accordance with section 7004 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.

7002(b)(1): Business A provides a mobile flashlight application. **Depending on the circumstances,** Business A should not collect, or allow another business to collect, consumer geolocation information through its mobile flashlight application without the consumer's explicit consent because the collection of geolocation information is incompatible with the context in which the personal information is collected, i.e., provision of flashlight services. The collection of geolocation data ~~may is not be within the reasonable expectations of an average consumer, nor is it~~ reasonably necessary and proportionate to achieve the purpose of providing, **improving, or adding features to** a flashlight function.

§ 7003. Requirements for Disclosures and Communications to Consumers.

7003(c): We ask for a revision that clarifies the "need to be same prominence" as COMPARABLE links. An example, if a privacy notice is in the footer, it should be as prominent as other links there. It might not be as prominent as other links in the body of the site. We just want to ensure specific context is considered.

§ 7004. Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent.

This section contains prescriptive requirements related to tracking the number of consumers 'clicks' and what the Agency considers dark patterns. Conceptually, symmetry in choice and requiring the path for a consumer to exercise a more privacy-protective option not be longer than the path to exercise a less privacy-protective option is straightforward. However, the example provided in 7004(a)(2)(A) may be concerning in practice.

- The example indicates a business's process for submitting a request to opt-out of sale/sharing shall not require more steps than that business's process for a consumer to opt-in to the sale of personal information after having previously opted out.
- The issue of concern is consumers visiting retail sites via different devices. Retailers would not know whether that consumer has opted out and thus opt in is the default.

Retailers are either asking for clarity from the Agency, on how retailers can implement a process for opt outs and opt ins to be symmetrical or delete.

- Also, the mention of dark patterns here is unusual. In certain sections, the description and definition of what the Agency deems a dark pattern is very clear; however, in other sections the examples are too broad or subjective such as the reference to “more eye-catching color”. We ask for consistency and clarity.
- The entire subsection of 7004(4) is concerning and problematic. Retailers want to explain to consumers how choices will affect them. One example: If someone asks to have their info deleted, they will lose their loyalty points which may be worth hundreds of dollars. They also may lose their ability to later create a profile using the same email address. It’s important that retailers be able to tell them what will happen if they make certain choices. And retailers should be able to convey benefit choices in a non-deceptive way (see specific comments below).

7004(a)(2): Symmetry in choice. The path for a consumer to exercise a more privacy-protective option shall not be ~~longer more burdensome~~ than the path to exercise a less privacy-protective option.

7004(a)(4): Avoid manipulative language or choice architecture. The methods should not use language or wording that ~~guilts, or shames threatens or misleads~~ the consumer into making a particular choice ~~or bundles consent~~ so as to subvert the consumer’s choice.

(B) Requiring the consumer to click through ~~false or misleading~~ reasons why submitting a request to opt-out of sale/sharing is ~~allegedly~~ a bad choice before being able to execute their choice to opt-out is manipulative. ~~and shaming~~.

(C) It is manipulative to bundle choices so that the consumer is only offered the option to consent to using personal information for reasonably expected purposes together with purposes that are incompatible to the context in which the personal information was collected. For example, a business that provides a location-based service, such as a mobile application that posts gas prices within the consumer’s location, shall not require the consumer to consent to incompatible uses (e.g., sale of the consumer’s geolocation to data brokers) together with the expected use of providing the location-based services, which does not require consent. This type of choice architecture is manipulative because the consumer is forced to consent to incompatible uses in order to obtain the expected service. The business should provide the consumer a separate option to consent to the business’s use of personal information for unexpected or incompatible uses.

ARTICLE 2. NOTICES REQUIRED DISCLOSURES TO CONSUMERS

§ 7011. Privacy Policy

7011(e)(3)(J): We ask for consideration in deleting that the method to contact with questions needs to reflect the “primary manner” in which the business interacts with consumers. We suggest using the term “one of the primary ways” or something similar.

§ 7012. Notice at Collection of Personal Information.

7012(e)(5): We ask for clarification on the meaning – is the intent that retailers must include the link to the opt-outs in the consent notice? If so, we are concerned that will make notices very long. We suggest allowing retailers to specify to consumer they use the alternative opt-out link as referenced in section §7015.

§ 7013. Notice of Right to Opt-Out of Sale/Sharing of and the “Do Not Sell or Share My

Personal Information” Link.

7013(f): Retailers are concerned having to link to specific sections could be burdensome, particularly because links break. We respectfully request an option to offer consumers a page with descriptive links that will take them where they want to go for various options.

7013(e)(3)(B): Asking for clarification as it would seem to require notices on the phone even if that’s not the primary way you interact.

ARTICLE 3. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS

§ 7022. Requests to Delete.

7022(c): This would require a service provider to tell retailers if it was too hard to tell third parties to delete data (with a detailed explanation) and then retailers would need to tell the consumer. This could become very burdensome, and not helpful to consumers. We question how will giving a detailed reason helps consumers if there really is nothing the consumer can do? We suggest limiting to sensitive data only.

7022(f): There is now a requirement for a “detailed explanation” v. a description why a business is denying a request to delete. This seems to add additional burdens without a lot of benefit and could potentially make responses more complex.

§ 7023. Requests to Correct

7023(c): (*Suggested change*) - A business that complies with a consumer’s request to correct shall correct the personal information at issue on its existing systems and implement measures to ensure that the information remains corrected. The business shall also instruct all service providers and contractors that maintain the personal information at issue in the course of providing services to the business to make the necessary corrections in their respective systems **unless such notification proves impossible or involves disproportionate effort**. Service providers and contractors shall comply with the business’s instructions to correct the personal information or enable the business to make the corrections and shall also ensure that the information remains corrected.

7023(i): This would require retailers to give source of data, even if the retailer is not the source of incorrect data. The result would be retailers have to map all data sources, which may not be possible for older data.

7023(j): Retailers question the requirement to show we have corrected the data we have been asked to correct by showing all the data. We suggest changing this to **show only** what was required to be corrected.

§ 7024. Requests to Know.

7024(h): There is an added a requirement that the personal information shown to the customer must include personal information services providers or contractors obtained as a result of providing services to the business. Does that require retailers to every service provider or contractor for personal information? For example, if a retailer does vendor direct shipping, does the retailer have to go to each vendor to ask what data they have?

§ 7025. Opt-Out Preference Signals.

Address Lack of Clarity Concerning Opt-Out Preference Signals and Responses

In their current form, the draft regulations fail to address a critical statutory mandate: that the Agency issue regulations that “define the requirements and technical specifications for an opt out preference signal...” including to ensure that the platform that sends such signals is consumer-friendly, that it clearly represents a consumer's intent, and that the signal does not conflict with other settings. *Section 1798.185(a)(19)*.

Rather than meeting its statutory obligation to address these topics, the draft regulations instead require businesses to honor any opt out preference signal that is “in a format commonly used and recognized” such as “an HTTP header field.” This amorphous standard fails to “define the requirements and technical specifications” for such opt outs, leaving retailers and their advertising partners to guess at what signals they must honor, how to look for such signals, and how to honor them. Businesses need clarity on these important topics before being required to honor these signals. The Agency should pause any enforcement on this topic until it has defined the technical requirements for opt out preference signals.

Other concerns include:

- Inconsistency between CPRA text and §7025(e). The Agency views the global opt-out preference as mandatory, not optional.
- Requirements for honoring and displaying whether or not we processed the consumers opt-out preference signal very prescriptive. Regulations require we display on our website “Opt-Out Preference Signal Honored” when a browser, device, or consumer using an opt-out preference signal visits the website or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.
- The concept of “frictionless manner” is introduced, which provides that businesses refrain from certain activities (charging a fee for using the opt-out, change the consumer’s experience, provide a pop-up or other “interstitial content”) in response to the opt-out preference signal. (§7025(f)).

Proposed Revisions:

- Option A:** Strike Section 7025 of the Draft Regs in its entirety until the Agency acts on its statutory obligation to define the requirements and technical specifications for an opt out preference signal sent by a platform, technology, or mechanism.
- Option B:** Add a new subsection (h) to section 7025 that provides: **(h) The Agency will not enforce this section 7025, nor any provisions of these regulations or the CCPA relating to opt-out preference signals until six months after the Agency has issued final regulations addressing requirements and technical specifications for opt-out preference signals pursuant to Section 1798.185(19), Civil Code.**
- Option C:** 7025 (b): A business shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing:
- (1) The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field.
 - (2) The signal shall have the capability to indicate that the consumer has selected to turn off the opt-out preference signal.**
 - (3) The platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer, whether in its configuration or in disclosures to the public, that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information. The configuration or disclosure does not need to be tailored only to California or to refer to California.

(4) The business's obligation to process a preference signal shall not exceed the technical capability of the platform, technology, or mechanism that sends the opt-out preference signal. For instance, where a signal is in an HTTP header field format, the business shall process the signal only where it is received on a browser.

7025(g)(3): Retailers would likely not be able to be frictionless because we could not effectuate for offline without more info. This means we'd likely still have to have the opt-outs, plus honor the signal. That really undercuts value of exception for many businesses.

Restore Opt-Out Link or Opt-Out Preference Signal Choice

Under the CPRA, businesses are explicitly provided a choice in how they offer opt-outs: either provide a "Do Not Sell/Share" link on their sites behind which consumers can opt out on the business's sites, or honor platform-based opt-out preference signals. *Section 1798.135*. In their current form, the draft regulations take away this choice. Instead, they require retailers and other businesses to honor opt-out platform signals even if they provide a fully compliant opt out link.

The statute offers a reasonable choice that allows retailers and other companies some measure of flexibility, while honoring the wishes of their customers. By purporting to remove this flexibility, the draft regulations create more confusion for retailers and others, particularly given the nascent development of opt out preference signals as a technological solution.

Proposed Revisions: Revise Section 7025 of the Draft Regs as follows:

- Add the following text to the beginning of subsection: (a) This section 7025 applies to any business that (1) collects information from consumers online; (2) engages in sales, sharing, or collection of sensitive personal information; and (3) does not provide "Do Not Sell or Share My Personal Information," "Limit the Use of My Sensitive Personal Information" or alternate opt-out links on the business's internet homepage(s). The purpose of an opt-out preference signal is to provide consumers...
- Omit subsection (e) of section 7025.

§ 7026. Requests to Opt-Out of Sale/Sharing.

7026(f)(3): Notifying all third parties to whom the business has sold or shared the consumer's ~~makes~~ personal information ~~available, including businesses authorized to collect personal information or controlling the collection of personal information on the business's premises~~, that the consumer has made a request to opt-out of sale/sharing and directing them ~~1) to comply with the consumer's request unless such notification proves impossible or involves disproportionate effort and 2) to forward the request to any other person with whom the third party has disclosed or shared the personal information during that time period~~. In accordance with section 7052, subsection (a), those third parties ~~and other persons~~ shall no longer retain, use, or disclose the personal information unless they become a service provider or contractor that complies with the CCPA and these regulations.

7026(i): For an authorized agent to submit a do not sell/share request, they have to provide signed written permission. Without more authorized agents this could become burdensome/abusive. Authorized agents could submit requests to every company even if person is not customer, and that is in addition to having to honor preference signals.

ARTICLE 4. SERVICE PROVIDERS, CONTRACTORS, AND THIRD PARTIES

§ 7051; 7053. Contract Requirements for Service Providers, Contractors, and Third Parties.

Permit More Flexibility in Agreements with Service Providers and Third Parties

The draft regulations impose extremely prescriptive requirements retailers and other businesses must follow for all their contracts with service providers and third parties. Failure to address all these provisions (ten requirements in service provider agreements and six in contracts with third parties) would subject the business to significant penalties, even for trivial missteps. The statute already addresses core requirements for service provider agreements (see *Section 1798.140(ag)*) and does not instruct the Agency to issue regulations concerning third party agreements. Sections 7051 and 7053 of the draft regulations create an onerous compliance regime for businesses with little to no corresponding protection for consumers.

Proposed Revisions: Strike Sections 7051 and 7053 of the draft regulations in their entirety.

ARTICLE 8. TRAINING, AND RECORD-KEEPING

§ 7102. Requirements for Businesses Collecting Large Amounts of Personal Information.

7102: Retailers should not have to report number of requests not to sell/share to extent came from preference signal.

Thank you for the consideration of our concerns and our suggestions on clarification. If you have any questions or would like additional input, please do not hesitate to reach out to me directly.

Sincerely,



Rachel Michelin
 President & CEO
 California Retailers Association

From: [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
Subject: CPPA Public Comment
Date: 22.08.2022 18:43:23 (+02:00)
Attachments: CardCoalitionCPPAFiled82222.pdf (9 pages)

WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Attached are the comments of the Card Coalition. Thank you for your consideration.

Frank M. Salinger

General Counsel

Card Coalition

[REDACTED]
www.cardcoalition.org

Notice: If received in error, please delete and notify sender. Sender does not waive confidentiality or privilege and use or transmittal of any content is prohibited.

Card Coalition P.O. Box 802 Occoquan, VA 22125-0802 ☎ 703.910.5280



August 23, 2022

California Privacy Protection Agency
ATTN: Brian Soublet, Esquire
2101 Arena Boulevard
Sacramento, CA 95834
Filed via email at regulations@coppa.ca.gov

Re: CPPA Public Comment

Dear Mr. Soublet:

The Card Coalition respectfully submits these comments in response to the Notice of Proposed Rulemaking published on July 8, 2022, to adopt proposed regulations implementing the Consumer Privacy Rights Act of 2020 (CPRA).

Statement of Interest & Policy Concerns

The Card Coalition consists of major national card issuers and related companies interested in state legislative, executive, and regulatory activities affecting the credit card industry and consumers. We are the only national organization devoted solely to the payment card industry and related legislative and regulatory activities in all 50 states.¹

Few industries are as keenly aware of the need to protect our customers' privacy, and we appreciate the opportunity to participate in this important rulemaking.

We are concerned about practical compliance issues which arise when your agency promulgates requirements unique to California without demonstrating privacy challenges that are, in some manner, unique to California. Enhancing consumer privacy protections is a global, transnational, issue and we believe individual states should move cautiously and allow regulated institutions maximum flexibility to respond to ever-evolving challenges.

We begin by expressing alarm that, in many instances, the proposed regulations exceed what is required by the underlying statute—and you will note our comment letter references provisions we believe should be amended to follow the underlying statute. While passage of the CCPA was a significant event and a number of states

¹ To learn more about the Card Coalition and our members, please visit www.cardcoalition.org.

carefully considered enacting comprehensive privacy laws, only five states have done so—most of them less burdensome to business.²

Adding extra-statutory requirements adds needless compliance challenges with little apparent benefit to California consumers. We urge you to adopt our suggested changes.

Specific Areas of Concern

a. Section 7002(a) and explicit consent vs. notice.

Section 7002(a) requires “explicit consent” to collect, use, retain, or share personal information for “any purpose that is unrelated or incompatible with the purpose(s) for which the personal information [was] collected or processed.” To the contrary, Section 1798.100(a)(1) of the statute permits the collection or use of personal information for additional purposes that are incompatible with the disclosed purposes as long as the business notifies the consumer of the additional purposes. The statute requires only notice and the regulations require “explicit consent.” The final regulations should track with the statute and require notice only, not explicit consent.

b. Section 7004(c) and dark patterns.

Section 7004(c) states that a “user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decision-making, or choice, regardless of a business’s intent.” In other words, the Draft Regulations subject businesses to strict liability regarding the development and implementation of their user interfaces.

As a consequence, the CPPA or the Attorney General could initiate an enforcement action against a business that experienced technical, software, hardware, or other technology-related issues that caused accidentally a substantial subversion or impairment of a user’s autonomy, decision-making, or choice. It is common for businesses of all sizes to experience problems with their websites, online user interfaces, and mobile applications.

Moreover, these problems can occur without the business’s negligence, wrong-doing, or intent. Malicious actors, hackers, and other criminal actors can alter or disrupt a business’s online presence despite the business’s use of state-of-the-art security measures.

A business should not be punished for something it did not intend or cause nor could have prevented. The regulations should drop the strict liability in exchange for a more-

² California, Colorado, Connecticut, Utah, and Virginia.

measured approach that considers the business’s intent, knowledge, and other relevant factors, such as information security practices.

In the alternative, if the CCPA chooses to retain strict liability, it should establish a safe harbor provision that protects businesses from liability for violations that could not have been prevented or expected.

(c) Section 7011(e) and privacy policy required content.

Section 7011(e) requires a business’s privacy policy to include content not mentioned in the statute. For example, Section 7011(e)(1) requires “a comprehensive description of the business’s online and offline practices regarding the collection, use, sale, sharing, and retention of personal information.”

The statute doesn’t mention any requirement that the privacy policy contain a “comprehensive description” of a business’s “online and offline practices.” The regulations should track with the statute and provide additional guidance or clarity, not create unanticipated requirements with undefined terms such as “comprehensive description.”

(d) Section 7012(f) and notice at collection online.

Section 7012(f) requires a business that collects personal information online to provide the notice at collection by providing a “link that takes the consumer directly to the specific section of the business’s privacy policy that contains the information required in subsection (e)(1) through (6).”

The section continues by stating that directing the consumer to the beginning of the privacy policy or to any other section without the required information will not satisfy the notice at collection requirement. We believe this requirement is overly prescriptive and impractical to put in place.

The notice at collection must contain a link to the privacy policy. Additionally, the notice at collection is more tailored to the products or services requested by the consumer. Should every notice at collection have different links to different sections of the privacy policy?

We recommend this requirement be scrapped.

(e) Section 7012(g) and third parties controlling the collection of personal information.

Section 7012(g) introduces a new concept not seen in the statute regarding third parties who “control” the collection of personal information, and the imposition of an

obligation for such third parties to deliver their own privacy notice at collection. This section goes beyond the statute, creating new obligations not previously contemplated. We recommend deleting this section as the concerns expressed should be appropriately addressed by the service provider, contractor, and third party contractual requirements and related restrictions.

(f) Section 7012(e)(6) and names of third parties.

Section 7012(e)(6) requires a business that allows third parties to control the collection of personal information to include in the notice at collection, “the names of all third parties; or, in the alternative, information about the third parties’ business practices.”

We note the underlying statute requires *only* disclosure of “categories” of third parties, never names or business practices, including the privacy policy, the notice at collection, and in response to the right to know/access.

We believe the regulations should track with the statute requiring categories of third parties, not names or business practices.

(g) Section 7012(e)(4) and data retention periods.

Section 7012(e)(4) requires the notice at collection to include the “length of time the business intends to retain each category of personal information,” or if that is impossible, the “criteria used to determine the period of time” the personal information will be retained.

Prescriptive data retention notice requirements are difficult to comply with because of the various and numerous factors that could come into play, such as duration of the relationship with the consumer, duration of the transaction, legal requirements, or in anticipation of defending against legal claims or litigation. Further, different types of data may have different retention periods, some required by statute.

We recommend this provision should be stricken or, at a minimum, be amended to allow greater flexibility.

(h) Section 7013(e) and notice of right to opt-out of sale/sharing.

Section 7013(e) requires a business that “sells or shares” to provide a notice of right to opt-out of “sale/sharing.” Under the current CCPA statute and CCPA AG Regulations, a business that does not “sell” personal information is not required to post a “Do Not Sell My Personal Information” link.

Under the draft regulations, if a business “shares” but does not “sell” personal information, the regulations require a business to post a “Do Not Sell or Share My Personal Information” link or the alternative link.

If a business “shares” but does not “sell,” or vice versa, the business should be able to post the relevant link and not both links. For example, the business that does not “sell” but “shares” should be permitted to post a “Do Not Share My Personal Information” link without the inclusion of “sale.”

(i) Sections 7022(b) and (d) and archived or backup systems.

Section 7022(b)(1) requires businesses to delete a consumer’s personal information from its existing systems except “archived or back-up systems,” seemingly indicating that requests to delete do not trigger a requirement to delete personal information on archived or back-up systems.

To the contrary, Section 7022(d) states that a business that stores any personal information on archived or back-up systems “may delay compliance with the consumer’s request” until the archived or back-up system is “restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose.”

For clarification, is the proposed Regulation saying that a business is never required to delete personal information stored on archived or back-up systems (as long as it stays on such archived or back-up systems), or a business has a requirement to delete personal information on archived or stored systems; however, that requirements isn’t triggered unless, or until, a business activates that system or accesses, sells, discloses, or uses such data for a commercial purpose?

Additionally, does the term “access” include *de minimus*, temporary, or transient access for maintenance, information security, fraud, system improvement, and other purposes that do not require length or permanent access nor use or disclosure of personal information outside of the limited purposes mentioned? We urge the CPPA to clarify these issues.

(j) Section 7023(f)(3) and notifying others about accuracy of personal information.

Section 7023(f)(3) requires a business that has denied a consumer’s request either in whole or in part, to notify the consumer that, upon her request, the business will “note both internally and to any person with whom it discloses, shares, or sells the personal information” that the consumer has contested the accuracy of the personal information, unless the request is fraudulent or abusive.

This requirement goes beyond the underlying statute by requiring a business to notify both internally and to any person with whom it discloses, shares, or sells the personal information that the consumer has requested correction, despite the request having been denied. Assuming the denial is lawful, why should a business have to contact external parties to inform them of a denied request to correct? There is nothing for the external parties to do with this information. We urge the CPPA to clarify these issues.

(k) Section 7025 and opt-out preference signals.

Section 7025 states that a “business shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing” in conflict with the statute pursuant to Section 1798.135(b)(1), which states that a business that complies with subdivision (a) (providing opt-out links on a business’s website), does not have to comply with Section 1798.135(b)(1).

In other words, the statute gives businesses the choice of whether they want to honor universal opt-out preference signals, but the draft regulations require businesses to both provide opt-out links on their websites and to honor universal opt-out preference signals.

First, the draft regulations directly conflict with the underlying statute. The draft regulations should track with the statute, permitting businesses the option to honor universal opt-outs.

Second, the draft regulations do not address the technical limitations in honoring universal opt-out preference signals. At this time, there is no universal opt-out preference signal capable of effectively communicating a consumer’s opt-out preferences to all websites, online platforms, or mobile applications. At a minimum, the CPPA should provide (perhaps in an appendix) the technical specifications for a recognized opt-out signal or signals. Otherwise a business will not know what it is supposed to be watching for. But the better course is to follow, not expand the statute, and reaffirm that universal opt-preference signals should be an optional method to honor opt-outs.

(l) Section 7026(f)(2) and downstream notification of consumer opt-out requests to all third parties.

Section 7026(f)(2) requires a business to notify all third parties to whom the business has sold or shared a consumer’s personal information of a consumer’s request to opt-out of sale/sharing and to forward the consumer’s opt-out request to “any other person with whom the person has disclosed or shared the personal information.”

Both requirements go beyond the requirements of the statute and would be technically challenging at the device level (whether in connection with a one-off device interaction or in response to a global privacy control).

Furthermore, the requirement to forward a consumer's request to any person with whom the person has disclosed or shared the information fails to take into consideration lawful disclosures to service providers, contractors, law enforcement, government agencies, or disclosures to other businesses or individuals pursuant to an explicit request or direction from the consumers to make the disclosure.

We believe these requirements should be dropped as, along with lacking statutory authority, are operationally difficult or likely impossible due to technological and practical limitations.

(m) Section 7027 and requests to limit use and disclosure of sensitive personal information.

Section 1798.121(d) of the CPRA states that “[s]ensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer, is not subject to this Section [Section 1798.121 on requests to limit use and disclosure of sensitive personal information], as further defined in regulations...and shall be treated as personal information for purposes of all other sections of this Act, including Section 1798.100.”

Notably, the draft regulations do not clarify when sensitive personal information is considered collected or processed for purposes other than inferring characteristics about a consumer.

According to the statute, collecting or processing sensitive personal information for purposes other than inferring characteristics about a consumer is exempt from the right to limit the use and disclosure of sensitive personal information. However, the draft regulations ignore this exemption and any collection or processing of sensitive personal information is subject to the right to limit use and disclosure. We urge the CCPA to amend the regulations to track the statute.

(n) Section 7027 and use of sensitive personal information.

In a number of sections, the Regulations contravene and narrow the scope of the statutory language, effectively disregarding Section 1798.121(a)-(b), which permit a business to use a consumer's sensitive personal information for uses that are “necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services,” even after receipt of a consumer's request to limit.

While the Regulations attempt to define permissible uses of Sensitive Personal Information in Section 7027(l), the seven use cases listed most certainly do not encompass all those uses of Sensitive Personal Information that may be “necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services.”

The impact of this overreach by the Regulations has significant adverse effect. As an example, in Section 7014(h), the Regulations purport to impose a springing consent requirement with respect to any use, outside the seven limited uses defined by Section 7027(l), of Sensitive Personal Information collected at a time when a business did not have a notice of right to limit posted.

As a notice of right to limit is not required until January 1, 2023, any personal information collected prior to January 1, 2023, absent consumer consent, may not be used for any purpose other than one of the seven purposes defined by Section 7027(l). Similarly, in Section 7027(g)(1), the Regulations require that, upon receipt of a request to limit, a business must cease to use and disclose Sensitive Personal Information for any purpose other than the 7 purposes listed in Section 7027(l); a restriction that conflicts with the language in 7027(a) and in 1798.121(a)-(b) that allows uses that are “necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services.”

These inconsistencies are problematic for constructing a compliance program. The above notwithstanding, the seven use cases identified in 7027(l) fail to contemplate a use of Sensitive Personal Information to comply with a legal or regulatory obligation or otherwise address any use case that relates to uses of employee information.

(o) Section 7051(a)(2) and Section 7053 and business purpose disclosures in service provider/contractor/third party contracts.

Section 7051(a)(2) requires businesses identify, in each service provider or contractor agreement, the specific business purpose for which personal information is disclosed, which goes beyond the statute’s obligations and beyond the contractual remediation that businesses undertook in complying with the CCPA. The draft regulations would require an impractical amount of additional contract remediation to update executed contracts with this information. Section 7053 of the draft regulations require the same information for third party agreements, which goes beyond the statute’s requirements and is an impractical task.

(p) Sections 7051(e) and 7053(e) and due diligence.

Section 7051(e) and Section 7053(e) states that “[w]hether a business conducts due diligence of its” service providers, contractors, or third parties “factors into whether the business has reason to believe” the service provider, contractor, or third party is using personal information in violation of the CCPA/CPRA.

Furthermore, both provisions cite an example where a business that never enforces the terms of its contract nor exercises its rights to audit or test might not be able to rely on the defense that it did not have reason to believe that the service provider, contractor, or third party intended to use the personal information in violation of the CCPA. These

Card Coalition P.O. Box 802 Occoquan, VA 22125-0802 ☎ 703.910.5280


provisions go beyond the statute and shifts service provider, contractor, and third party liability to the business.

Moreover, the provisions do not discuss what level of due diligence is required to prevent this shifting of liability. We suggest striking these provisions or amending and clarifying them such that businesses know what level of due diligence is required to prevent the shifting liability.

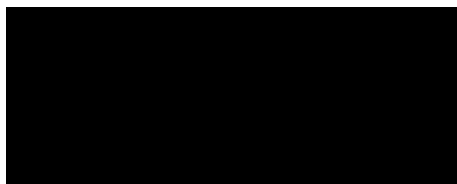
*

The Card Coalition appreciates the opportunity to share our views on and would be pleased to discuss our specific concerns outlined above. Thank you for your consideration.

Respectfully submitted,



Toni A. Bellissimo
Executive Director



Frank M. Salinger
General Counsel

