MAYER | BROWN

August 22, 2022

Mayer Brown LLP
350 South Grand Avenue
25th Floor
Los Angeles, CA 90071-1503
United States of America

T: +1 213 229 9500
F: +1 213 625 0248

mayerbrown.com

**Dominique Shelton Leipzig**
Partner
[redacted]

## California Chamber of Commerce Comments to Draft California Privacy Rights Act Regulations

## INTRODUCTION

The California Chamber of Commerce (CalChamber) respectfully submits these comments to the California Privacy Protection Agency's (the Agency) July 8, 2022, Notice of Proposed Rulemaking regarding the proposed California Privacy Rights Act (CPRA) regulations. In sum, CalChamber requests the following modifications to the proposed CPRA regulations, which are described in greater detail below in the Comments section:

1. **The Agency Should Postpone Enforcement of the CPRA Because of the Agency's Delay in Finalizing the CPRA Regulations.** Under the CPRA, the dates set for finalizing the regulations (July 1, 2022) and start of enforcement (July 1, 2023) provided a one-year compliance window. The one-year window reflected the time needed for businesses to assess and implement changes necessary to comply with new requirements. Because the Agency has not met the deadline to finalize the regulations, enforcement should be postponed to one year after the CPRA regulations are finalized.

2. **The "Average Consumer" Standard Proposed in Section 7002 Is Contrary to the CPRA and Deviates from the Approach Established in Other Privacy Laws.** We propose revisions to remove the "average consumer" standard and align restrictions on the collection and use of personal information to the language in the CPRA. The CPRA standard evaluates the collection of personal information based on the reasonableness of a business's processing activities and transparency, not the ambiguous expectations of an "average consumer." Moreover, the proposed regulation could shift California from an implied consent based on notice jurisdiction to an opt-in jurisdiction, which is contrary to California law. In addition to deviating from California law, adopting the "average consumer" standard would separate California from the EU's General Data Protection Regulation (GDPR) and other state privacy laws that apply the reasonableness approach set out in the text of the CPRA.

3. **Methods for Honoring Opt-Out Preferences Should Remain Flexible and Facilitate Consumer Choice as Intended by the CPRA.** As proposed, section 7025's mandate that businesses honor opt-out preference signals ***and*** provide an opt-out link contravenes the

CPRA statute, which gives businesses flexibility to choose either option without requiring both. The proposed regulation further contradicts the CPRA by adding that a business is only able to employ opt-out preference signals, without providing the opt-out link, if they do so in a "frictionless manner," a term not used in the CPRA. We propose modifications to rectify this misalignment with the CPRA and to incorporate CPRA requirements intended to facilitate consumer choice, such as the requirement to be free of defaults that presuppose consumer intent, and avoiding conflicts with commonly used privacy settings. These changes encourage consumer choice without removing the flexibility for businesses that the CPRA intended.

4. **The Proposed Requirements for Handling Opt-Outs of Sale and Sharing Should Be Revised To Limit Burdens on Business that Do Not Materially Benefit Consumers.** We propose two changes to section 7026 to address unnecessary requirements. First, we request changes to make clear that section 7026 requires businesses to honor opt-out requests on a going-forward basis. As written, the proposed regulation could create ambiguity around applicability of this requirement. In an abundance of caution, businesses may seek to implement requests retroactively, which would involve a "disproportionate effort," as set forth in section 7001(h), and impose a significant burden on businesses to try to unwind prior data transactions, even though consumers did not previously object to those transactions. Second, businesses should not be required to display consumer preferences on the webpage, as this would unnecessarily clutter the user experience, be technologically difficult to implement, and may lead to confusion. Consumers are sufficiently served by showing the preferences within the privacy settings.

5. **Requirements To Prevent Dark Patterns Should Be Tailored To Address Fraudulent Practices Without Undermining Consumer Choice.** As proposed, section 7004 risks undermining consumer choice with ambiguous and overly restrictive standards, as well as potentially running afoul of First Amendment protections that allow businesses to share truthful and accurate information with consumers. We request that the Agency add reasonable limits and focus on requirements that give businesses flexibility to adopt practical and appropriate methods for informing consumers about their choices, while prohibiting potentially fraudulent practices.

6. **Notice of Collection Requirements Should Be Reasonable To Avoid Becoming Cumbersome and Duplicative.** Draft section 7012 sets out additional requirements for notices of collection when more than one party is involved. We propose modifications to these requirements in line with the CPRA and GDPR to limit cumbersome and duplicative disclosures. First, we urge the Agency to remove the requirement that a business's privacy notice list all third-party names. The CPRA only requires that a business disclose the categories of third parties, which serves the purpose of informing consumers without making the notice unwieldy and imposing unnecessary burdens on businesses. Second, the proposed requirement that all parties involved provide notice should be revised to align

with the GDPR. Under the GDPR, joint controllers allocate responsibilities for compliance amongst themselves, including the obligation to provide a privacy notice. Duplicative disclosures are confusing and run the risk of being tuned out by consumers.

7. **The Agency's Authority To Conduct Audits Should Be Subject To Reasonable Limits.** As drafted, the Agency has broad power to audit a business without evidence of a violation and without any notice to the business. Responding to audits can take resources away from valuable compliance efforts and yield little benefit to consumers when the Agency does not have concrete indications of wrongdoing by the business. Moreover, when the business does not have any notice of an audit, the Agency may obtain an incorrect impression of the business's compliance if the business has not had sufficient time to assemble responses to the Agency's requests. The Agency's audits should be limited to instances where it has sufficient facts to support the audit and are clearly defined in advance; the Agency should also provide the business with 60 days' notice to ensure that the audit can be efficiently managed.

8. **While Organizing Requirements for Service Provider and Contractor Agreements Is Valuable, Any Additional Requirements the Agency Is Seeking To Add Should Be Crafted To Benefit Consumers Without Unduly Burdening Businesses.** As drafted, the regulations create potential confusion and impose overly restrictive contractual requirements unnecessary to achieve the purpose of the CPRA. For example, the draft regulations should be modified to clarify that the CPRA does not apply to entities that process personal information on behalf of non-businesses (e.g., nonprofits and government entities). We also propose modifications to sections 7050, 7051, and 7053 to align the obligations of service providers and contractors with the CPRA statute and to address unnecessarily prescriptive and onerous requirements.

9. **Notice Requirements in Connection with Phone Calls and Smart Devices Should Be Designed To Better Serve Both Consumer Privacy and the User Experience.** Draft section 7013 requires businesses to ensure that consumers encounter a privacy notice while contacting a business over the phone or using a smart device. The notice requirements in connection with phone calls and smart devices should focus on whether consumers can *access* the privacy notice, not whether they will *encounter* the notice on call or smart devices. This will better serve consumer privacy, creating a meaningful opportunity to review the notice, without disrupting the consumer experience.

10. **The Agency Should Accommodate the Possibility of Opt-In Consent for the Use of Sensitive Personal Information and Remove Excessively Restrictive Requirements That Do Not Materially Benefit Consumers.** We propose two modifications to sections 7014 and 7015 regarding the requirements for sensitive personal information. Rather than providing a notice of the right to limit processing, businesses that want to take a more privacy-protective approach should have the option to obtain opt-in consent before processing sensitive personal information for a purpose other than the purposes enumerated

in the statute. This proposal is more privacy protective in honoring consumer choice. Second, the draft requirement that the icon size on the business's website be the same size as others on the page is unduly burdensome to implement in practice. A flexible approach achieves the goals of providing consumers with information without creating an unwieldy standard.

11. **Requirements Related to Responding to Requests To Delete Should Be Reasonable To Achieve the Purposes of the CPRA Without Imposing Resource-Intensive Processes.** We request that the Agency consider removing requirements that (1) businesses, service providers, and contractors provide a detailed explanation regarding why notification would be impossible or involve disproportionate effort and (2) businesses explain to consumers the exemption they are relying on in denying a deletion request. Providing these explanations is time- and resource-intensive. Businesses would struggle to allocate sufficient resources and labor to handle such explanations if required. Moreover, the CPRA does not mandate that businesses provide detailed explanations. Imposing this additional requirement on businesses is not necessary to implement the CPRA.

12. **The Proposed Requirement that Businesses Notify Service Providers and Contractors of a Consumer's Request To Correct Exceeds the Agency's Authority Under the CPRA.** The CPRA does not require that businesses notify service providers and contractors of a consumer's request to correct. We request that the Agency strike this requirement or, in the alternative, add an exception to the draft regulation for when providing notice is impossible or requires disproportionate effort.

13. **The Regulations Should Properly Place the Burden on the Consumer To Make a Specific Request for Information Exceeding the Prior 12 Months, Consistent with the CPRA.** The CPRA does not require a business to automatically provide a consumer personal information beyond the 12-month look-back period. As written, section 7024(h) could create confusion around the time period for which a business must provide data. We propose changes to clarify and align section 7024(h) of the regulations with the CPRA statute, allowing businesses the flexibility to either automatically provide personal information beyond the 12-month look-back period or choose to notify consumers that they can request personal information beyond the 12-month period and comply upon such request.

14. **The Regulations on Requests To Limit the Use or Disclosure of Sensitive Information Should Be Revised To Align with the Text of the CPRA Statute, Avoid Undermining Consumer Choice, and Support Efforts To Combat Crime.** We have proposed a series of modifications to section 7027. First, as drafted, section 7027 sets out requirements that are not aligned with the text of the CPRA statute. We also are concerned with presenting options to consumers that result in a single option being presented more prominently than more nuanced options. This subverts consumer choice and impedes sharing truthful and accurate information. The exception for use to combat malicious, deceptive, fraudulent, or

illegal actions should not be limited to only actions "directed at the business," as proposed. This limits the ability of businesses to aid others that are targets of such actions by disclosing sensitive information needed to stop such actions.

15. **Procedures for Probable Cause Proceedings Should Be Modified To Give Businesses an Opportunity To Respond To Allegations Before Initiating a Proceeding.** Before initiating a probable cause proceeding, businesses should have an opportunity to receive the information underlying the alleged violations and to provide a response, as well as to appeal or request a correction in a decision. This gives the Agency and businesses an opportunity to exchange critical information to fully inform a decision and address any errors in the decision.

## COMMENTS

### 1. The Agency Should Postpone Enforcement of the CPRA Because of the Agency's Delay in Finalizing the CPRA Regulations.

We request that the Agency delay enforcement of the CPRA and the regulations. Under the CPRA, regulations were set to be finalized by July 1, 2022. *See* Cal. Civ. Code § 1798.185(d). The voters intended to provide a one-year compliance window ahead of the July 1, 2023, CPRA enforcement date. *Id.* Postponing enforcement is appropriate here because the Agency has not fulfilled its obligation to finalize the CPRA regulations by the July 1, 2022, deadline, and businesses need sufficient time to revise policies and procedures and implement changes to digital properties.

Indeed, contrary to the Economic Impact Statement released as part of this rulemaking, implementing compliance with the CPRA will not cost $127.50 per business and increase labor requirements by 1.5 hours per business. *See* Economic and Fiscal Impact Statement. Rather, based on a survey of the businesses that are members of CalChamber, all respondents estimated that the costs of implementing CPRA compliance will far exceed the Agency's estimates, to the tune of hundreds of thousands of dollars, if not $5 million or more using *conservative* estimates for larger companies. The respondents indicated that compliance efforts will necessarily involve no fewer than 300 hours, with most respondents providing estimates in the four-digit range and requiring anywhere from one to five new full-time employees per business. At a minimum, compliance legal fees *alone* would far surpass the Agency's estimates. Compliance will require businesses to dedicate considerable time for data identification and mapping, review and revision of data policies and security measures for non-employee data, and implementation of internal training programs, among other programming, record-keeping, and reporting measures.

Businesses are also left in a precarious situation, as they are interested in implementing their CPRA compliance programs as soon as possible but cannot do so because the regulations, which contain critical details and new requirements of the CPRA, are not yet final. Accordingly, we ask the Agency to postpone the enforcement date to one year after the CPRA regulations become finalized.

### 2. The “Average Consumer” Standard Proposed in Section 7002 Is Contrary to the CPRA and Deviates from the Approach Established in Other Privacy Laws (Section 7002).

#### A. Proposed Modifications

We propose the below modifications to section 7002(a). We also propose removing the illustrative examples in section 7002(b) or modifying section 7002(b) to align with these proposed changes to section 7002(a).

(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 used for other ~~disclosed~~ purpose(s) if they are compatible with ~~what is reasonably expected by the average consumer~~ any purpose that is disclosed at the time of collection. A business shall notify the consumer ~~obtain the consumer’s explicit consent~~ in accordance with section 7012~~7004~~ before collecting, using, retaining, and/or sharing the consumer’s personal information for any purpose that is unrelated to or incompatible with the disclosed purpose(s) for which the personal information is collected or processed.

#### B. Reasons for Proposed Modifications

We offer modifications to section 7002(a)–(b) to align with the CPRA and other state privacy laws.

As an initial matter, the “average consumer” standard in section 7002 should be removed. This proposed standard conflicts with the CPRA, which requires the collection of personal information to be “reasonably necessary and proportionate to achieve the purposes for which personal information was collected or processed or for another disclosed purpose that is compatible with the context in which the personal information was collected . . . .” Cal. Civ. Code § 1798.100(c); *see also* 11 CCR § 7003 (providing detailed requirements for disclosures to consumers). The CPRA standard is based on the reasonableness of the business’s processing activities based on transparency, rather than an “average consumer” standard. As a result, the introduction of an “average consumer” standard may create ambiguity for CPRA compliance. A business, consumer, and regulator may have differing views on what an “average consumer” expects, particularly in California, which does not have a homogenous consumer base and has a wide variety of industries. This lack of clarity creates challenges for businesses working to comply with the regulation. It also gives the Agency broad leeway to substitute its own judgment of what is necessary and proportionate. Instead of looking to an “average consumer,” we propose language that aligns with the CPRA and other privacy laws and reduces ambiguity for businesses when assessing their compliance.

Further, this proposed regulation could shift California from an implied consent based on notice to an opt-in jurisdiction, which is contrary to California law. *See* Cal. Civ. Code § 1798.100(a). The CPRA, like other state privacy laws, established that California does not require consumers (except for sale of children's data) to opt-in to data collection and use practices. *See id.* Rather, the CPRA looks to the notice provided to the consumer, and use that is compatible with that notice, to assess whether the collection is permissible. *See id.* (A business shall inform consumers of "[t]he categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes ***that are incompatible with the disclosed purpose*** for which the personal information was collected without providing the consumer with notice consistent with this section.") (emphasis added). As written, draft section 7002 changes the statute by requiring consent based on the expectation of the "average consumer," instead of the context of the collection, including the notice at or before the point of collection to consumers, along with compatible purposes. To avoid this conflict with the CPRA, we recommend that the Agency amend the draft regulation as proposed. Simply put, the disclosed purpose for collecting the consumer's personal information is an important element in setting consumer expectations; there is no need to add an "average consumer" standard that seemingly would allow the Agency to disregard the disclosures that businesses provide to consumers.

Indeed, the GDPR does not take this approach. *See* GDPR, Arts. 5(1)(b), 13 & 14. Other state privacy laws taking effect in 2023 also do not adopt an "average consumer" approach for the purpose limitation doctrine. *See* Va. Code Ann. § 59.1-574(A)(1) ("A controller shall: Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, ***as disclosed*** to the consumer. . . .") (emphasis added); Colo. Rev. Stat § 6-1-1308(c)(3) ("A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to ***the specified purposes*** for which the data are processed.") (emphasis added); Conn. Gen. Stat. § 6(a) ("A controller shall (1) Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, ***as disclosed*** to the consumer.") (emphasis added). Adopting an "average consumer" standard would conflict with these other privacy laws, contrary to the Agency's statement that the proposed regulations are intended to be harmonious with other privacy laws. *See* Notice of Proposed Rulemaking at 7 ("Finally, the proposed regulations take into consideration privacy laws in other jurisdictions and implement compliance with the CCPA in such a way that it would not contravene a business's compliance with other privacy laws, such as the General Data Protection Regulation (GDPR) in Europe and consumer privacy laws recently passed in Colorado, Virginia, Connecticut, and Utah. In doing so, it simplifies compliance for businesses operating across jurisdictions and avoids unnecessary confusion for consumers who may not understand which laws apply to them.").

**3. Methods for Honoring Opt-Out Preferences Should Remain Flexible and Facilitate Consumer Choice as Intended by the CPRA (Section 7025).**

A. Proposed Modification

(b) A business that elects to honor an opt-out preference signal pursuant to Civil Code section 1798.135(b) 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 platform, technology, or mechanism shall have the capability to clearly indicate the consumer's opt-out choice in a manner that complies with Section 7004, including accurately identifying the user as a California resident and disclosing any technical limitations of the mechanism.

(3~~2~~) 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~~ to the consumer that align with Section 7004, 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 as defined under California law. ~~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 is not required to collect additional information to link the user to other accounts.

(5) The platform, technology, or mechanism that sends the opt-out preference signal shall have the capability to allow a consumer to clearly represent the consumer's intent and be free of defaults constraining or presupposing that intent.

(6) The platform, technology, or mechanism that sends the opt-out preference signal shall ensure that the opt-out preference signal is consumer-friendly, clearly described, and easy to use by a reasonable consumer.

(7) The platform, technology, or mechanism that sends the opt-out preference signal shall ensure that the opt-out preference signal does not conflict with other commonly used privacy settings or tools that consumers may employ.

(c) When a business that elects to honor an opt-out preference signal pursuant to Civil Code section 1798.135, subdivision (b) collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b):

. . .

(3) 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~~ may ignore the opt-out preference signal, if it notifies ~~but my notify~~ the consumer of the conflict and provides 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, or if the customer does not respond to the business within seven calendar days of receiving the notice from the business, 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).

(4) If the opt-out preference signal conflicts with the consumer's participation in a business's financial incentive program that requires the consumer to consent to the sale or sharing of personal information, the business ~~shall~~ may notify the consumer that processing the opt-out preference signal would withdraw the consumer from the financial incentive program and ask the consumer to affirm that they intend to withdraw from the financial incentive program. If the consumer affirms that they intend to withdraw from the financial incentive program, the business shall process the consumer's request to opt-out of sale/sharing. If the consumer does not affirm their intent to withdraw, or if the customer does not respond to the business within seven calendar days of receiving the notice from the business, 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).

(5) A business shall not interpret the absence of an opt-out preference signal after the consumer previously sent an opt-out preference signal as consent to opt-in to the sale or sharing of personal information.

(6) The business ~~should~~may display whether or not it has processed the consumer's opt-out preference signal. For example, the business may display on its 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.

(7) Illustrative examples follow.

(A) Caleb visits Business N's website using a browser with an opt-out preference signal enabled. Business N collects and shares Caleb's browser identifier for cross-contextual advertising, but Business N does not know Caleb's identity because he is not logged into his account. If Business N recognizes opt-out preference signals, upon receiving the opt-out preference signal, Business N shall stop selling and sharing Caleb's browser identifier for cross-contextual advertising, but it would not be able to apply the request to opt-out of the sale/sharing to Caleb's account information because the connection between Caleb's browser and Caleb's account is not known to the business.

(B) Noelle has an account with Business O, an online retailer who manages consumer's privacy choices through a settings menu that recognizes opt-out preference signals. Noelle's privacy settings default to allowing Business O to sell and share her personal information with the business's marketing partners. Noelle enables an opt-out preference signal on her browser and then visits Business O's website. Business O recognizes that Noelle is visiting its website because she is logged into her account. Upon receiving Noelle's opt-out preference signal, Business O shall treat the signal as a valid request to opt-out of sale/sharing and shall apply it to her device and/or browser and also to her account and any offline sale or sharing of personal information. Business O may inform Noelle that her opt-out preference signal differs from her current privacy settings and provide her with an opportunity to consent to the sale or sharing of her personal information, but it must process the request to opt-out of sale/sharing unless Noelle instructs otherwise.

. . .

~~(D) Ramona participates in Business P's financial incentive program where she receives coupons in exchange for allowing the business to pseudonymously track and share her online browsing habits to~~

~~marketing partners. Ramona enables an opt-out preference signal on her browser and then visits Business P's website. Business P knows that it is Ramona through a cookie that has been placed on her browser, but also detects the opt-out preference signal. Business P may ignore the opt-out preference signal, but must notify Ramona that her opt-out preference signal conflicts with her participation in the financial incentive program and ask whether she intends to withdraw from the financial incentive program. If Ramona does not affirm her intent to withdraw, Business P may ignore the opt-out preference signal and place Ramona on a whitelist so that Business P does not have to notify Ramona of the conflict again.~~

. . .

~~(e) Civil Code section 1798.135, subdivisions (b)(1) and (3), provides a business the choice between (1) processing opt-out preference signals and providing the "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links or an alternate opt-out link; or (2) processing opt-out preference signals in a frictionless manner in accordance with these regulations and not having to provide the "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links or an alternate opt-out link. It does not give the 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 signals, though it may do so in a non-frictionless manner. If a business processes opt-out preference signals in a frictionless manner in accordance with subsections (f) and (g) of this regulation, then it may, but is not required to, provide the above-referenced links.~~

~~(f) Except as allowed by these regulations, processing an opt-out preference signal in a frictionless manner as required by Civil Code section 1798.135, subdivision (b)(1), means that the business shall not:~~

~~(1) Charge a fee or require any valuable consideration if the consumer uses an opt-out preference signal; or~~

~~(2) Change the consumer's experience with the product or service offered by the business. For example, the consumer who uses an opt-out preference signal shall have the same experience with regard to how the business's product or service functions compared to a consumer who does not use an opt-out preference signal.~~

~~(3) Display a notification, pop-up, text, graphic, animation, sound, video, or any interstitial content in response to the opt-out preference signal. A~~

~~business's display of whether or not the consumer visiting their website has opted out of the sale or sharing their personal information, as required by subsection (c)(2), shall not be in violation of this regulation. The business may also provide a link to a privacy settings page, menu, or similar interface that enables the consumer to consent to the business ignoring the opt-out preference signal with respect to the business's sale or sharing of the consumer's personal information provided that it complies with subsections (f)(1) through (3).~~

(~~e~~g) A business meeting the requirements of Civil Code section 1798.135, subdivision (b)(1) is not required to post the "Do Not Sell or Share My Personal Information" link or the alternative opt-out link.~~ if it meets all of the following additional requirements:~~

~~(1) Processes the opt-out preference signal in a frictionless manner in accordance with the CCPA and these regulations.~~

~~(2) Includes in its privacy policy the following information:~~

~~(A) A description of the consumer's right to opt-out of the sale or sharing of their personal information by the business;~~

~~(B) A statement that the business processes opt-out preference signals in a frictionless manner;~~

~~(C) Information on how consumers can implement opt-out preference signals for the business to process in frictionless manner;~~

~~(D) Instructions for any other method by which the consumer may submit a request to opt-out of sale/sharing.~~

~~(3) Allows the opt-out preference signal to fully effectuate the consumer's request to opt-out of sale/sharing. For example, if the business sells or shares personal information offline and needs additional information that is not provided by the opt-out preference signal in order to apply the request to opt-out of sale/sharing to offline sales or sharing of personal information, then the business has not fully effectuated the consumer's request to opt-out of sale/sharing. Illustrative examples follow.~~

~~(A) Business Q collects consumers' online browsing history and shares it with third parties for cross-contextual advertising purposes. Business Q also sells consumers' personal information offline to marketing partners. Business Q cannot fall within the exception set~~

~~forth in Civil Code section 1798.135, subdivision (b)(1) because a consumer's opt-out preference signal would only apply to Business Q's online sharing of personal information about the consumer's browser or device; the consumer's opt-out preference signal would not apply to Business Q's offline selling of the consumer's information because Business Q could not apply it to the offline selling without additional information provided by the consumer, i.e., the logging into an account.~~

~~(B) Business R only sells and shares personal information online for cross-contextual advertising purposes. Business R may use the exception set forth in Civil Code section 1798.135, subdivision (b)(1) and not post the "Do Not Sell or Share My Personal Information" link because a consumer using an opt-out preference signal would fully effectuate their right to opt-out of the sale or sharing of their personal information.~~

B. Reasons for the Proposed Modification

We propose modifying section 7025 to align the regulation with the plain language of the CPRA statute, which creates flexibility for how businesses may honor opt-out of sale or sharing requests and ensures consumers make informed opt-out choices.

Initially, the Agency has exceeded its authority by directly contravening the CPRA statute and making it mandatory for businesses to honor opt-outs through both a "Do Not Sell or Share My Personal Information" link and opt-out preference signals. *See* Section 7025(e) ("Even if the business posts the above-referenced links, the business must still process opt-out preference signals, though it may do so in a non-frictionless manner."). Under the CPRA, voters approved giving flexibility to businesses to not provide an opt-out link if they allow consumers to exercise their opt-out rights through a preference signal. *See* Cal. Civ. Code § 1798.135(b)(1). The Agency has contradicted this requirement by making it mandatory to honor opt-out preference signals, even if an opt-out link is provided, and by adding the caveat that, for businesses to only honor opt-out preference signals instead of providing the opt-out link, they must do so in a "frictionless manner," a term that is not substantiated in the CPRA and difficult to comply for businesses with a limited online presence.

Indeed, the Agency's draft regulation is also inconsistent with what was envisioned when drafting the CPRA. For example, when Alastair Mactaggart, Ashkan Soltani, and CalChamber's representative, Dominique Shelton Leipzig, were negotiating the opt-out preference signal requirements under the CPRA, the Global Privacy Control was developed as an alternative to the "Do Not Sell or Share My Personal Information" link to give flexibility for businesses. CalChamber members also had extensive discussions with Alastair Mactaggart where it was confirmed that the opt-out preference signal provisions were intentionally drafted to offer that option. The Agency has reduced this flexibility under section 7025, which CalChamber seeks to correct through the above modifications.

Next, not all businesses are alike and able to honor the same type of opt-out preference signals. We propose the modifications to section 7025(b) in the spirit of providing flexibility for businesses to address opt-out preference signals in a manner that is compatible with their technical abilities. For example, when a signal is an HTTP header field enabled through a browser extension, a business should not be required to collect additional information from a consumer in an attempt to link the signal to other accounts. Without such limitations, a business could unintentionally violate the rule merely because it did not receive the signal in a form that the business could process. This would be the same as holding a business liable for failing to honor an opt-out request sent to an email account that the business cannot access. The proposed modification is intended to avoid such a scenario. These revisions will help businesses with their already-onerous task of complying with the CPRA and avoid unintended consequences, because it will incentivize opt-out preference signal providers to develop alternative forms of signals to meet different technological capabilities of businesses.

Moreover, the proposed regulations should be amended to incorporate CPRA requirements for opt-out preference signals, such as being free of defaults that presuppose consumer intent, being clearly described and easy to use, and ensuring the opt-out signal does not conflict with other commonly used privacy settings. *See* Cal. Civ. Code § 1798.185(a)(19). The Agency should not ignore these statutory requirements and the complexity of implementing an opt-out choice preference signal. The Agency should also take a consistent approach to transparency and informed user choice in the context of opt-out preference signals and its implementation of other CPRA requirements. Accordingly, at a minimum, the provider of an opt-out preference signal should be required to disclose the limits of any signal, the potential conflicts with other privacy settings, and the specific definition of sale and sharing of data under the CPRA.

Additionally, the proposed regulations should permit businesses to honor consumers' business-specific privacy choices that conflict with an opt-out preference signal. Sections 7025(c)(3)–(4) address conflicts between a consumer's business-specific privacy settings and opt-out signals with a regulatory presumption that a consumer would choose the universal opt-out. This exceeds the spirit of the CPRA, which is premised on consumer choice and control, and supplants the Agency's choice for the consumers. Section 7025(c)(3) creates an overly burdensome requirement for businesses when consumer preference signals create conflicts. Businesses would either have to build new mechanisms that detect conflicts, honor the signal when a conflict is present, and then permit businesses to seek consent to re-enable choices that consumers have already made. This forces businesses to clear up the confusion created by the opt-out mechanism. As a result, the proposed regulations would effectively override the statutory specifications for the opt-out signals to notify consumers about the effect of the opt-out, creating even more confusion and degrading the consumer experience. The Agency's regulations should put consumers in control of their choices, not the Agency.

**4. <u>The Proposed Requirements for Handling Opt-Outs of Sale and Sharing Should Be Revised To Limit Burdens on Businesses that Do Not Materially Benefit Consumers (Section 7026)</u>.**

A. <u>Proposed Modification</u>

*i. Preferred Approach*

(a) A business that sells or shares personal information shall provide two or more designated methods for submitting requests to opt-out of sale/sharing. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the personal information that it sells to or shares with third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of sale/sharing. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow.

(1) A business that collects personal information from consumers online, the business may ~~shall, at a minimum,~~ allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal and through an interactive form accessible via the "Do Not Sell My Personal Information" link, the alternative opt-out link, or the business's privacy policy.

. . .

(f) A business shall comply with a request to opt-out of sale/sharing by:

…

~~(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.~~

~~(3) Notifying 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, that the consumer has made a request to opt-out of sale/sharing and directing them 1) to 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 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.~~

~~(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 "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.~~

*ii. Alternative Approach*

(a) A business that sells or shares personal information shall provide two or more designated methods for submitting requests to opt-out of sale/sharing. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the personal information that it sells to or shares with third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of sale/sharing. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow.

(1) A business that collects personal information from consumers online, the business may ~~shall, at a minimum,~~ allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal and through an interactive form accessible via the "Do Not Sell My Personal Information" link, the alternative opt-out link, or the business's privacy policy.

. . .

(f) A business shall comply with a request to opt-out of sale/sharing by:

. . .

~~(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.~~

(2~~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.

(3~~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.

### B. Reasons for Modification

The proposed regulations could imply an interpretation that the regulations require businesses to apply opt-outs retroactively. The CPRA makes clear that opt-out requests apply only on a going-forward basis after the business receives the request from the consumer. *See* Cal. Civ. Code § 1798.120(d) ("A business that has received direction from a consumer not to sell or share the consumer's personal information. . . shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from selling or sharing the consumer's personal information *after its receipt of the consumer's direction.*") (emphasis added). As currently drafted, the regulations call into question whether an opt-out request must be conveyed to all third parties and limit use of previously sold or shared personal information. If the regulations were to be improperly interpreted to apply retroactively, this could involve a "disproportionate effort" as defined under draft regulation 7001(h). It would allow a consumer to revoke a business's previously received right to share or sell that consumer's personal information, instead of applying it on a going-forward basis. To comply, businesses would have to unwind prior data transactions to implement the opt-out requests across all downstream partners. This could be a complicated and burdensome process for businesses to ensure compliance, especially when dealing with third parties. Our proposed modifications address this issue by making clear that businesses need only apply opt-out requests on a going-forward basis as received. This change limits the burden on businesses. CPRA already requires notice of sharing or selling at the time of the collection of data; since the consumer had not elected to opt-out at the initial time of collection, the consumer knew and implicitly consented to the sale or sharing. For this reason, the business was well within its rights to share or sell the consumer's personal information.

In the alternative, if language on notice to third parties is retained, this section should be revised as proposed. This includes applying to only third parties to which a business has sold or shared a consumer's personal information and adding a disproportionate effort standard. We also have proposed deleting section 7026(f)(2), because the requirements appear entirely subsumed by 7026(f)(3), rendering it redundant.

Section 7026(f)(4) also requires a business to provide a means by which a consumer can confirm that the business has processed their opt-out request. This is a new requirement that extends beyond the statutory requirements. We recommend that, if a business is required to display a preference, it should have the option to show a preference within the privacy settings. A business should not be required to display a consumer's preference on the webpage, as this would unnecessarily clutter the user experience, be technologically difficult to implement, and may lead to confusion.

Finally, we propose modifications to section 7026(a) to align with the plain language of the CPRA statute that gives businesses the flexibility to honor opt-out of sale or sharing requests and ensures consumers make informed opt-out choices, as further described above.

### 5. Requirements To Prevent Dark Patterns Should Be Tailored To Address Fraudulent Practices Without Undermining Consumer Choice (Section 7004).

A. Proposed Modifications

(a) Except as expressly allowed by the CCPA and these regulations, businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles.

(1) Easy to understand. The methods shall use language that is easy for consumers to read and understand. ~~When applicable, they shall comply with the requirements for disclosures to consumers set forth in section 7003.~~

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

(A) A business's process for submitting a request to opt-out of sale/sharing shall not unreasonably 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 number of steps for submitting a request to opt-out of sale/sharing is measured from when the consumer clicks on the “Do Not Sell or Share My Personal Information” link to completion of the request.~~ The number of steps for submitting a request to opt-in to the sale of personal information is measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request.~~

…

~~(C) A website banner that serves as a method for opting out of the sale of personal information that only provides the two choices, “Accept All” and “More Information,” or “Accept All” and “Preferences,” is not equal or symmetrical because the method allows the consumer to “Accept All” in one step, but requires the consumer to take additional steps to exercise their right to opt-out of the sale or sharing of their personal information. An equal or symmetrical choice would be “Accept All” and “Decline All.”~~

(C~~D~~) A choice where the “yes” button is more prominent (i.e., materially larger in size ~~or in a more eye-catching color~~) than the “no” button is not symmetrical, but colors can be used to aid the consumer’s choice (e.g., green for “yes” and red for “no”).

(D~~E~~) A choice where the option to participate in a financial incentive program is selected by default or featured more prominently (i.e., materially larger in size ~~or in a more eye-catching color~~) than the choice not to participate in the program is neither equal nor symmetrical.

(1) Avoid language or interactive elements that are not clear and conspicuous and are intentionally confusing to the consumer. The methods should not use double negatives. Toggles or buttons must clearly indicate the consumer’s choice. ~~Illustrative example follows.~~

~~(A) Giving the choice of “Yes” or “No” next to the statement “Do Not Sell or Share My Personal Information” is a double negative and a confusing choice for a consumer.~~

~~(B) Toggles or buttons that state “on” or “off” may be confusing to a consumer and may require further clarifying language.~~

~~(C) Unintuitive placement of buttons to confirm a consumer’s choice may be confusing to the consumer. For example, it is confusing to the consumer when a business at first consistently offers choices in~~

~~the order of Yes, then No, but then offers choices in the opposite order — No, then Yes — when asking the consumer something that would benefit the business and/or contravene the consumer's expectation.~~

(1) 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.

~~(A) When offering a financial incentive, pairing choices such as, "Yes" (to accept the financial incentive) with "No, I like paying full price" or "No, I don't want to save money," is manipulative and shaming.~~

(A~~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~~.

(B~~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. By contrast, where the use of personal information is compatible with a requested good or service, the business need not offer a separate option. For example, using a consumer's geolocation information to find the closest gas station is compatible with a mobile app that assists consumers in finding prices at local gas stations.

(5) Easy to execute. The business shall not add unreasonable ~~unnecessary~~ burden or friction to the process by which the consumer submits a CCPA request. Methods should be tested to ensure that they are functional and do

not undermine the consumer’s choice to submit the request. Illustrative examples follow.

(A) Upon clicking the “Do Not Sell or Share My Personal Information” link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out of sale/sharing.

~~(B) Circular or broken links, and nonfunctional email addresses, such as inboxes that are not monitored or have aggressive filters that screen emails from the public, may be in violation of this regulation.~~

(B~~C~~) Businesses that require the consumer to unnecessarily wait on a webpage as the business processes the request may be in violation of this regulation.

## B. Reasons for Proposed Modifications

Proposed section 7004(a) risks undermining consumer choice because the standards contained therein are ambiguous, subjective, and overly restrictive. It also contravenes the First Amendment protection allowing businesses to share truthful and accurate information with consumers. Our proposed modifications are not intended to undermine the purpose of section 7004, which is to ensure that consumers are presented with methods to submit rights requests and give consent without encountering “dark patterns.” Instead, we propose modifications to add reasonableness limitations and focus the requirements on design practices that give businesses the flexibility to adopt practical and appropriate methods, while not engaging in what can be fraudulent practices. These modifications are consistent with California’s other consumer protection laws aimed to prevent fraudulent activities. *See, e.g.*, Cal. Bus. & Prof. Code § 17200 (defining unfair competition as including “unfair, untrue or misleading advertising”). Our modifications are also intended to give businesses flexibility to inform consumers regarding the implications of their decisions, such as the impact of opting out or choosing an option. Consumer choice is not meaningful if consumers’ access to information is needlessly restricted. Accordingly, the Agency should revise the draft regulations to appropriately tailor the provisions targeting dark patterns.

Initially, section 7004(a)(2)’s requirement for symmetry should be based on a reasonable effort to achieve symmetry rather than having perfect symmetry. Perfect symmetry may not be possible in all contexts and could undermine consumer choice by restricting information or options. The illustrative example in section 7004(a)(2)(A), for instance, prohibits the process for submitting an opt-out request from involving more steps than a request to opt-in. However, there are instances where an additional step is necessary to provide a consumer with complete information about the impact of an opt-out request. As drafted, this extra step would be improper even if it is reasonable and likely helpful to consumers so that they can make informed decisions. To remedy this, we propose stating that businesses cannot "unreasonably" require additional steps. This will give businesses the opportunity to inform consumers regarding the disadvantages of opting out.

Similarly, section 7004(a)(2)(C) mandates an all-or-nothing approach for website banners that seek to allow consumers to exercise their rights. Yet, by limiting consumers to "accept all" or "deny all," consumers cannot fully exercise their rights. A consumer may oppose the use of data for certain purposes and not others. The proposed regulation also does not allow consumers to exercise their rights in an informed manner, because it suggests that a "More Information" option is not permitted. This proposed regulation will not allow consumers to tailor consents based on their individual preferences. Thus, the Agency's all-or-nothing approach for symmetry does not protect consumers. Rather, it deprives consumers of options and the information they would need to make informed decisions.

Further, the proposed modifications to section 7004(a)(3)-(4) are intended to prevent intentionally misleading designs, rather than strict requirements that may be unwieldy or unintentionally undermine consumer choice. Additionally, we suggest changes to focus on misleading or deceptive architecture. The First Amendment protects a business's ability to share truthful and accurate information with consumers. *See, e.g.*, *Central Hudson Gas & Electric v. Public Service Commission*, 447 U.S. 557 (1980). As written, section 7004(a)(4), in particular, could impinge on a business's communication of truthful information about the effect of an opt-out request. Consumer choice is not informed if consumers' access to information is needlessly restricted. Accordingly, the Agency should revise the draft regulations to appropriately tailor these provisions to address actual dark patterns, not restrict the flow of information.

Finally, we propose that section 7004(a)(5) be subject to a reasonableness standard to allow appropriate flexibility and avoid excessive penalization of businesses. The illustrative example in section 7004(a)(5)(B) demonstrates how this section could be applied in an overly burdensome manner. This example could be interpreted to mean that any broken link or nonfunctional email address creates liability, even though such failures happen despite robust practices to prevent them. These ordinary and isolated technical failures should not be the basis for liability. Adding a reasonableness standard (as opposed to one based on unnecessary burden or friction) remedies this issue.

## 6. Notice of Collection Requirements Should Be Reasonable To Avoid Becoming Cumbersome and Duplicative (Section 7012).

### A. Proposed Modifications

#### *i. Preferred Approach*

(e) A business shall include the following in its notice at collection:

. . .

~~(6) If a business allows third parties to control the collection of personal information, the names of all the third parties; or, in the alternative, categories of the third parties' business practices.~~

(f) If a business collects personal information from a consumer online, the notice at collection may be given to the consumer 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) and includes headings to assist a consumer with finding this information. ~~Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain the required information, so that the consumer is required to scroll through other information in order to determine the categories of personal information to be collected and/or whether the business sells or shares the personal information collected, does not satisfy this standard.~~

(g) Third Parties that Control the Collection of Personal Information. When more than one business may control the collection of a consumer's personal information, the businesses shall in a transparent manner determine their respective responsibilities for compliance with these regulations, which includes determining which business or businesses will provide notice at collection in accordance with the CCPA and these regulations. The businesses shall be accountable for their respective compliance with their designated responsibilities. This arrangement will appropriately reflect the respective roles and relationships of the businesses to consumers. The nature of the relationship shall be made available to consumers.

~~(1) For purposes of giving notice at collection, more than one business may control the collection of a consumer's personal information, and thus, have an obligation to provide a notice at collection in accordance with the CCPA and these regulations. For example, a first party may allow another business, acting as a third party, to control the collection of personal information from consumers browsing the first party's website. Both the first party that allows the third parties to collect personal information via its website, as well as the third party controlling the collection of personal information, shall provide a notice at collection.~~

(1) This subsection shall not affect the first party's obligations under the CCPA to comply with a consumer's request to opt-out of sale/sharing. If a consumer makes a request to opt-out of sale/sharing with the first party, both the first party and third parties controlling the collection of personal information shall comply with sections 7026, subsection (f), and 7052, subsection (a).

~~(2) A first party that allows another business, acting as a third party, to control the collection of personal information from a consumer shall include in its notice at collection the names of all the third parties that the first party allows to collect personal information from the consumer. In the alternative, a business, acting as a third party and controlling the collection of personal information, may provide the first party information about its business practices for the first party to include in the first party's notice at collection.~~

~~(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 at the physical location(s) where it is collecting the personal information.~~

~~(4) Illustrative examples follow.~~

~~(A) Business F allows Business G, an analytics business, to collect consumers' personal information through Business F's website. Business F may post a conspicuous link to its notice at collection, which shall identify Business G as a third party authorized to collect personal information from the consumer or information about Business G's information practices, on the introductory page of its website and on all webpages where personal information is collected. Business G shall provide a notice at collection on its homepage.~~

~~(B) Business H, a coffee shop, allows Business I, a business providing wi-fi services, to collect personal information from consumers using Business I's services on Business H's premises. Business H may post conspicuous signage at the entrance of the store or at the point-of-sale directing consumers to where the notice at collection for Business H can be found online. Business H's notice at collection shall identify Business I as a third party authorized to collect personal information from the consumer or include information about Business I's practices in its notice. In addition, Business I shall post its own notice at collection on the first webpage or other interface consumers see before connecting to the wi-fi services offered.~~

~~(C) Business J, a car rental business, allows Business M to collect personal information from consumers within the vehicles Business K rents to consumers. Business J may give its notice at collection, which shall identify Business K as a third party authorized to collect personal information from the consumer or include information~~

~~about Business K’s practices, to the consumer at the point of sale, i.e., at the rental counter, either in writing or orally. Business K may provide its own notice at collection within the vehicle, such as through signage on the vehicle’s computer dashboard directing consumers to where the notice can be found online. Business K shall also provide a notice at collection on its homepage.~~

*ii. Alternative Approach*

(e) A business shall include the following in its notice at collection:

. . .

(6) If a business allows third parties to control the collection of personal information, ~~the names of all the third parties; or, in the alternative, information about~~ the categories of the third parties’ the business allows to control the collection of personal information ~~business practices~~.

(f) If a business collects personal information from a consumer online, the notice at collection may be given to the consumer 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). ~~Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain the required information, so that the consumer is required to scroll through other information in order to determine the categories of personal information to be collected and/or whether the business sells or shares the personal information collected, does not satisfy this standard.~~

(g) Third Parties that Control the Collection of Personal Information. This subsection shall not affect the first party’s obligations under the CCPA to comply with a consumer’s request to opt-out of sale/sharing. If a consumer makes a request to opt-out of sale/sharing with the first party, both the first party and third parties controlling the collection of personal information shall comply with sections 7026, subsection (f), and 7052, subsection (a).

(1) For purposes of giving notice at collection, more than one business may control the collection of a consumer’s personal information, and thus, have an obligation to provide a notice at collection in accordance with the CCPA and these regulations. For example, a first party may allow another business, acting as a third party, to control the collection of personal information from consumers browsing the first party’s website. Both the first party that allows the third parties to collect personal information via its website, as well as the third party controlling the collection of personal information, shall

provide a notice at collection. The third party may provide the notice at collection on its own webpage pursuant to Civil Code section 1798.100, subdivision (a) and need not provide the notice on the first party's website.

(2) A first party that allows another business, acting as a third party, to control the collection of personal information from a consumer shall include, in its notice at collection, the categories of third parties with whom the first party ~~names of all the third parties that the first party~~ allows to collect personal information from the consumer. In the alternative, a business, acting as a third party and controlling the collection of personal information, may provide the first party information about its business practices for the first party to include in the first party's notice at collection. Whether the first party includes the third party's information in the first party's notice at collection will not affect the third party's obligations or compliance under this subsection.

(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.

(4) Illustrative examples follow.

~~(A) Business F allows Business G, an analytics business, to collect consumers' personal information through Business F's website. Business F may post a conspicuous link to its notice at collection, which shall identify Business G as a third party authorized to collect personal information from the consumer or information about Business G's information practices, on the introductory page of its website and on all webpages where personal information is collected. Business G shall provide a notice at collection on its homepage.~~

(A~~B~~) Business H, a coffee shop, allows Business I, a business providing wi-fi services, to collect personal information from consumers using Business I's services on Business H's premises. Business H may post conspicuous signage at the entrance of the store or at the point-of-sale directing consumers to where the notice at collection for Business H can be found online. Business H's notice at collection shall identify Business I as a third party authorized to collect personal information from the consumer or include information about Business I's practices in its notice. In addition, Business I shall post its own notice at collection on the first webpage or other interface consumers see before connecting to the wi-fi services offered.

(B~~C~~) Business J, a car rental business, allows Business K to collect personal information from consumers within the vehicles Business J rents to consumers. Business J may give its notice at collection, which shall identify Business K as a third party authorized to collect personal information from the consumer or include information about Business K's practices, to the consumer at the point of sale, i.e., at the rental counter, either in writing or orally. Business K may provide its own notice at collection within the vehicle, such as through signage on the vehicle's computer dashboard directing consumers to where the notice can be found online. Business K shall also provide a notice at collection on its homepage.

### B. Reasons for Proposed Modifications

We propose two options for modifying section 7012(e)-(g) to reduce confusion and unnecessary burdens that likely will result under the draft requirements.

Initially, the requirement in section 7012(f) that businesses link to specific sections of their privacy policy should be removed. This requirement will only result in businesses having to provide several different links to specific sections of the privacy policy to satisfy the notice at collection requirement. Allowing businesses to provide a link to their privacy policy that contains the required information and clear headers will allow for a less cumbersome consumer experience.

We also note that sections 7012(e) and (g) should be revised to better address the realities when multiple businesses control data collection to avoid multiple notices to consumers. As written, the section mandates duplicative disclosures and cumbersome mechanisms for these disclosures. More disclosures do not always benefit consumers as this can result in information overload or disclosures becoming white noise that consumers ignore. The benefit is further limited when consumers do not have a direct relationship with the third-party businesses providing notice.

Moreover, the draft regulations are contrary to the statutory text of the CPRA by requiring a list of third-party names. The CPRA only requires describing the ***categories*** of third parties, not their names. *See* Cal. Civ. Code §§ 1798.110(a)(4); 1798.115(a)(2); 1798.130(a)(3)(B)(ii); 1798.130(a)(4)(B). This requirement will also undermine the value of privacy policies by requiring lengthy and confusing language. The list of third-party names may have limited utility to consumers and impact the usability of the privacy policy. In fact, the requirement to provide a list of third parties in a business's privacy policy may conflict with confidentiality provisions in contracts. Indeed, some businesses guard the names of certain parties, such as data security providers, because this provides them with a competitive advantage. The proposed regulation will interfere with these businesses' ability to keep this information confidential without significantly bolstering consumers' rights.

Lastly, to achieve the purposes of the CPRA, only one party should provide notice that describes the categories of third parties with which personal information is shared. Our first proposed approach achieves this. This proposal also aligns the regulations with the GDPR, which allows joint controllers to "determine their respective responsibilities for compliance with" the GDPR, including the obligation to provide a privacy notice. *See* GDPR, Art. 26. If the Agency declines to adopt this proposal, we recommend that the Agency consider the second proposal. This alternative would at least mitigate issues related to disclosing names of all third parties and would adopt a reasonableness standard for notices provided at physical locations.

## 7. The Agency's Authority To Conduct Audits Should Be Subject to Reasonable Limits (Section 7304).

### A. Proposed Modification

(a) Scope. The Agency may audit a business, service provider, contractor, or person to determine compliance with any provision of the CCPA.

(b) Criteria for Selection. The Agency may conduct an audit to investigate possible violations of the CCPA if there are articulable facts leading to a reasonable belief that the business's collection or processing of personal information presents significant risk to consumer privacy or security. ~~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.~~

(c) Audits ~~may be announced or unannounced as determined~~ shall only be conducted upon no less than 60 days' notice by the Agency.

(d) Failure to Cooperate. A subject's failure to cooperate during the Agency's audit may result in the Agency issuing a subpoena, seeking a warrant, or otherwise exercising its powers to ensure compliance with the CCPA.

(e) Protection of Personal Information. Consumer personal information disclosed to the Agency during an audit shall be maintained in compliance with the Information Practices Act of 1997, Civil Code section 1798, et seq.

(f) Prior to initiating an audit, the Agency must approve by majority vote a written order stating the scope of the audit. The audit may not exceed the scope of the written order and shall be limited to the CCPA provision or regulation that the Agency reasonably believes was or is being violated.

(g) A business may request a hearing before an Administrative Law Judge to determine the propriety and scope of a written order commencing an audit.

B. Reasons for the Proposed Modification

Section 7304 should be modified to place reasonable limits on the conduct of Agency audits.

First, the proposal that the Agency may conduct audits to investigate possible violations without limits is unreasonable. Responding to audits can be incredibly burdensome for businesses to manage, even when a business has not violated the law. We encourage the Agency to exercise discretion in focusing audits on businesses where there are sufficient facts supporting a belief that a business's activities create a risk to consumer privacy or security in violation of the CCPA. This allows the Agency to use its resources in an efficient manner without burdening businesses with fishing expeditions. We have proposed modifications to align with this approach.

Second, the Agency's proposal that audits may be conducted without any advanced notice neither benefits the objectives of its investigations nor businesses. In advance of an audit, a business needs time to prepare so that it can provide an informed response to any inquiries by the Agency. A business will also need to coordinate with their privacy leaders and stakeholders to ensure their availability during the audit to provide responses to the Agency based on the actual practices of the business. For example, if there is an unannounced audit, the relevant persons within the business may be on vacation, traveling, or otherwise unavailable to provide appropriate answers to the auditors. As a result, the Agency may end up speaking to individuals within the business that do not have the relevant information, which may lead to a misunderstanding regarding the business's actual compliance with the CPRA. For this reason, we propose that the Agency provide at least 60 days' advance notice before conducting an audit so that the business has sufficient time to prepare and ensure the availability of appropriate persons to guide the Agency regarding the business's compliance program.

## 8. **While Organizing Requirements for Service Provider and Contractor Agreements Is Valuable, Any Additional Requirements the Agency Is Seeking To Add Should Be Crafted To Benefit Consumers Without Unduly Burdening Businesses (Sections 7050, 7051, and 7053).**

A. Proposed Modifications

*i. Section 7050*

(a) A business that provides services to a person or organization that is not a business~~, and that would otherwise meet the requirements and obligations of a "service provider" or "contractor"~~ under the CCPA and these regulations~~,~~ shall not be subject to the obligations of a "business" under ~~be deemed a service provider or contractor with regard to that person or organization for purposes of~~ the CCPA and these regulations with respect to its processing of personal information for that person or organization. However, such a business is not under an obligation to enter into a “service provider” or “contractor” agreement that complies with the CCPA and these regulations with the person or organization that is not a business. For example, a cloud service provider that provides services to a non-profit organization ~~and meets the requirements and obligations of a service provider under the CCPA and these regulations, i.e., has a valid service provider contract in place, etc.,~~ shall ~~be considered a service provider even though it is providing services to a non-business~~ not be required to honor consumer rights requests under the CCPA and these regulations. The cloud service provider is also not obligated to be bound by contractual terms applicable for “service providers” or “contractors” under the CCPA and these regulations, because it is processing personal information for a non-business.

(a) A service provider or contractor shall not retain, use, or disclose personal information obtained in the course of providing services except:

. . .

(2) For the ~~specific~~ business purpose(s) and service(s) set forth in, and in compliance with the written contract for services required by the CCPA and these regulations.

. . .

(4) For internal use by the service provider or contractor to build or improve the quality of its services, provided that the service provider or contractor does not use the personal information to directly perform services on behalf of another person. Illustrative examples follow.

(A) An email marketing service provider can send emails on a business’s behalf using the business’s customer email list. The service provider could analyze those customers’ interactions with the marketing emails to develop or improve its services and offer those improved services to everyone. But the service provider cannot use the original email list to directly send marketing emails on behalf of another business.

. . .

(c) ~~A service provider or contractor cannot contract with a business to provide cross-contextual behavioral advertising.~~ Per Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but those services shall not combine the personal information of consumers who have opted out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or from its own interaction with consumers. ~~A person who contracts with a business to provide cross contextual behavioral advertising is a third party and not a service provider or contractor.~~ Illustrative examples follow.

(1) Business S, a clothing company, hires a social media company as a service provider for the purpose of providing Business S's advertisements on the social media company's platform. The social media company can serve Business S by providing non-personalized advertising services on its platform based on aggregated or demographic information (e.g., advertisements to women, 18-30 years old, that live in Los Angeles). The social media company can also use a customer list provided by Business S to serve Business S's advertisements to Business S'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 ~~identify users on the social media company's platform to serve advertisements to them~~.

*ii. Section 7051*

(a) The contract required by the CCPA for service providers and contractors shall:

. . .

(2) Include the required terms for such contracts under Civil Code 1798.100, subsection (d)(1). ~~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) 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).~~

. . .

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

. . .

~~(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.~~

…

~~(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.~~

…

(d~~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, where the business knows or has reason to believe that a violation of the CCPA and these regulations occurred, but the business never enforces the terms of the contract, ~~nor exercises its rights to assess, audit or test the service provider’s or contractor’s systems~~ it 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.

### *iii. Section 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, where the business knows or has reason to believe that a violation of the CCPA and these regulations occurred but the business never enforces the terms of the contract 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.

### B. Reasons for Proposed Modifications

We appreciate the Agency organizing the provisions required for contracts with service providers and contractors in one location, considering that these requirements are distributed in different parts of the CPRA. However, as drafted, sections 7050 to 7053 will unduly burden businesses when contracting and overseeing service providers and contractors without providing benefits for consumers. We encourage the Agency to consider revising sections 7050 to 7053 to address these concerns.

First, we recommend modifying section 7050(a) to more directly address the purpose of this subsection per the Agency's Initial Statement of Reasons, which is to avoid "entities that process personal information on behalf of non-profit and government entities in accordance with a written contract [not to] be required to comply with consumer requests even when those nonprofits and government entities in ultimate control of the information are not required to do so." *See* Initial Statement of Reasons at 49. We have modified subsection (a) to make this point clear and to avoid other unintended effects of the Agency's proposed language, such as making a business acting as a service provider to a non-business (e.g., the State of California) implement a contract with the non-business that meets all of the terms of the CPRA and these regulations. This places undue and unintended burdens not only on service providers and contractors, but also on non-profits and governmental entities that are not within the scope of the CPRA.

Second, we recommend that section 7050(b)(4)(a) clarify that a service provider or contractor is still considered to be using personal information for internal purposes as long as it is not directly using the personal information to service another person. This is important because a service provider or contractor may generally improve its services based on personal information obtained from one business, which may benefit another person indirectly. This modification is necessary to draw that distinction and to avoid any unnecessary consequences of improving the services of service providers and contractors.

Third, we propose revising section 7050(c) to remove the verbiage regarding cross-context behavioral advertising and other restrictions. These issues are already dealt with in sufficient specificity in the statute. *See* Cal. Civ. Code § 1798.140(e)(6). Additionally, these restrictions are problematic, because they do not reflect that businesses that operate as service providers for one function may operate as a third party with respect to another function.

Fourth, we propose modifying section 7051 to address overly prescriptive requirements for contracts that are not present in the CPRA statute. Under the proposed section 7051(a)(2), a business is required to "identify the specific business purpose(s) and service(s) for which the service provider or contractor is processing personal information." This is a new requirement added by the Agency, which is not in the CPRA. The concept is carried over into proposed section 7051(a)(3) regarding various prohibitions, which also are to be tied to "the specific business purpose(s) and service(s) identified in subsection (a)(2)." This, too, is a new requirement added by the Agency and is not found in the CPRA. Small businesses, which may not even have internal legal staff to help write or review contracts, should not be placed in a position to violate the CCPA because their contracts do not contain specific listings of business purposes (a defined term under the CCPA) and services. As well, it will create an enormous burden on businesses that seek to prepare uniform data protection agreements as part of negotiating, in some instances, hundreds, if not thousands, of contracts with their service providers and contractors. The Agency should instead rely on the contract requirements already enumerated in CPRA for agreements between a business and its service provider, contractor, or third party. *See* Cal. Civ. Code § 1798.100(d)(1). The additional requirements in proposed section 7051 are overly prescriptive and do not further protect consumer privacy in any meaningful way. These provisions, which go beyond the plain text of the CPRA, also call into question the Economic Impact Statement released as part of this rulemaking. Any business would be hard-pressed to customize contracts as called for by these proposals while also limiting its *total* CPRA compliance costs to $127.50 and increased labor requirements by 1.5 hours.

Fifth, we request that the Agency remove the five-business day deadline for a service provider or contractor to provide notice under section 7051(a)(8). This specific deadline is not included in the CPRA. *See* Cal. Civ. Code § 1798.100(d)(4). Businesses should be able to determine a deadline that makes sense based on their business and contract. Indeed, because of the Agency's delay in publishing the draft CPRA regulations, many businesses have already begun the process of amending their contracts to address the new requirements for service providers and contractors based on the plain text of the CPRA statute. By including this additional requirement, businesses will have to redo these negotiations to address this unforeseen provision.

Sixth, we propose removing the section 7501(a)(10) requirement that contracts contain a provision obligating a business to inform a service provider or contractor of consumer requests. Businesses are unlikely to have this explicitly stated in existing agreements with service providers or contractors as there is no such requirement under the CPRA. As a result, these businesses may have to update many existing contracts to add this term. Mandating a contractual provision on this is unnecessary to achieve obligations under the CPRA.

Seventh, we propose removing section 7051(c) from the CPRA regulations because it is unnecessary. The CPRA statute already provides the requirement for there to be an agreement or written contract between the parties. *See* Cal. Civ. Code §§ 1798.100(d); 1798.140(j)(1); 1798.140(ag)(1). The effect of not having an agreement or written contract, but otherwise having a mutual understanding with your service provider or contractor, should be assessed on a case-by-case basis to see if it is truly a “sale” under the CPRA.

Lastly, as written, sections 7051(e) and 7053(e) potentially establish a requirement for businesses to conduct due diligence and audits of service providers, contractors, and third parties, even though there is no reason to believe that these parties are violating the CCPA or CPRA. The CPRA is clear 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.” *See* Cal. Civ. Code § 1798.140(ag)(1)(D) (emphasis added); *see also* Cal. Civ. Code § 1798.140(j)(1)(C) (permitting, but not requiring, audits). Thus, contrary to the plain text of the CPRA, the Agency is potentially making audits and diligence a mandatory requirement irrespective of the circumstances of the processing. Critically, requiring businesses to conduct audits and due diligence, even when there is no reason to suspect wrongdoing, will impose a significant burden on small businesses that do not have the resources to audit all of these suppliers on a routine basis. This will. in turn. divert resources that small businesses need for their general privacy compliance obligations. The proposed modification addresses this issue by requiring a business to know or have reason to know that there is a violation of the law before conducting diligence or an audit.

## 9. Notice Requirements in Connection with Phone Calls and Smart Devices Should Be Designed to Better Serve Both Consumer Privacy and the User Experience (Section 7013).

A. Proposed Modification

(e) A business that sells or shares the personal information of consumers shall provide the notice of right to opt-out of sale/sharing to consumers as follows:

…

(3) A business shall also provide the notice to opt-out of sale/sharing in the same manner in which it collects the personal information that it sells or shares. Illustrative examples follow.

…

(B) A business that sells or shares personal information that it collects over the phone shall inform consumers of the notice and where it can be accessed ~~provide notice orally~~ during the call when the information is collected.

(C) A business that sells or shares personal information that it collects through a connected smart device ~~(e.g., smart television or smart watch)~~ shall provide notice in a manner that ensures that the consumer ~~will encounter~~ can access the notice while using the smart device.

…

(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.

B. Reasons for the Proposed Modification

We have proposed a modification to section 7013(e) to ensure consumers can exercise choice by being able to determine the method for accessing the notice while contacting a business over the phone or using a smart device to better reflect how smart devices operate.

To foster consumer privacy, the emphasis in this section should be placed on whether a consumer can *access* the privacy notice during the call or while using the smart device, not whether they will *encounter* the notice on the smart device. Accessing the notice recognizes the importance of providing the consumer an opportunity to thoughtfully review the notice; conversely, merely encountering the notice does not ensure any meaningful opportunity to review and can interfere with the consumer's user experience on the smart device. For instance, a notice prompt on a smart watch every time a consumer opens a watch app would distract from the consumer's intended use of the smart device. In terms of telephone calls, consumers may not find it beneficial to listen to a notice of opt-out of sale/sharing and would prefer to read it themselves.

Lastly, section 7013(h) should apply to personal information collected after the notice requirement goes into effect under the CPRA. We propose modifications to this section to align this requirement.

## 10. The Agency Should Accommodate the Possibility of Opt-In Consent for the Use of Sensitive Personal Information and Remove Excessively Restrictive Requirements That Do Not Materially Benefit Consumers (Sections 7014 and 7015).

### A. Proposed Modification

*i. Section 7014*

We propose inserting a new subsection (b) under section 7014 (with the subsections that follow the current subsection (a) renumbered) that will state the following:

(b) A business is not obligated to provide a notice of right to limit if it obtains the consumer’s explicit consent to process his or her sensitive personal information and, at the time of consent, discloses how the consumer may withdraw their consent in a manner consistent with the applicable provisions in sections 7003 and 7004.

### *ii. Section 7015*

(b) A business that chooses to use an alternative opt-out link shall title the link, “Your Privacy Choices” or “Your California Privacy Choices,” and shall include the following opt-out icon to the right or left of the title. The link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business’s internet homepages. ~~The icon shall be approximately the same size as any other icons used by the business on its webpage.~~

### B. Reasons for the Proposed Modification

We recommend making minor modifications to sections 7014 and 7015 to provide both consumer choice and more flexibility to businesses.

First, we suggest that the regulations permit businesses to obtain opt-in consent *prior* to processing sensitive personal information for a purpose other than those enumerated in the statute, and provide consumers with a mechanism of withdrawing consent, in lieu of providing a notice of right to limit. This approach would be more privacy-protective by honoring consumer choice.

Second, as currently written, section 7015(b) would require an alternative opt-out link to be an icon that is the same size as other icons on a business’s website. In effect, section 7015(b) could require opt-out links and icons to be the same size as the business’s logo on its homepage. It also requires businesses to develop and define icons for each specific page on a website, which will require a different size icon for each page of a website. The burden of this requirement outweighs any value to the consumer. Thus, we recommend, at a minimum, removing the requirement that “[t]he icon shall be approximately the same size as any other icons used by the business on its webpage.” This will help address this unintended consequence. The better and more consumer-friendly approach is to permit businesses to use a clearly labeled alternative opt-out link, such as when labeled “Your Privacy Choices.” This will provide consumers with a clear link for reviewing and making privacy choices while giving businesses a straightforward and less burdensome way to develop a link across a single website.

**11.** **Requirements Related To Responding To Requests To Delete Should Be Reasonable To Achieve the Purposes of the CPRA Without Imposing Resource-Intensive Processes (Section 7022).**

A. Proposed Modification

(b) A business shall comply with a consumer's request to delete their personal information by:

(1) Permanently and completely erasing the personal information from its existing systems except archived or back-up systems, deidentifying the personal information, or aggregating the consumer information;

(2) 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

(3) Notifying all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information unless this proves impossible or involves disproportionate effort. ~~If a business claims that notifying some or all third parties would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot notify all third parties. The business shall not simply state that notifying all third parties is impossible or would require disproportionate effect.~~

(c) A service provider or contractor shall, upon notification by the business, comply with the consumer's request to delete their personal information by:

…

(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.~~

. . .

(f) In cases where a business denies a consumer's request to delete in whole or in part, the business shall do all of the following:

(1) Provide to the consumer a ~~detailed~~ explanation of the basis for the denial, including any conflict with federal or state law, or exception to the CCPA, ~~or factual basis for contending that compliance would be impossible or involve disproportionate effort~~, unless prohibited from doing so by law;

(2) Delete the consumer's personal information that is not subject to the exception;

(3) Not use the consumer's personal information retained for any other purpose than provided for by that exception; and

(4) Instruct its service providers and contractors to delete the consumer's personal information that is not subject to the exception and to not use the consumer's personal information retained for any purpose other than the purpose provided for by that exception.

B. Reasons for the Proposed Modification

We propose modifications to section 7022 to remove requirements for businesses, service providers, and contractors to provide consumers a detailed explanation regarding why deletion would be impossible or involve disproportionate effort.

As an initial matter, it is not uncommon for businesses to have hundreds, if not thousands, of service providers and contractors. If every consumer request to delete required a business to provide, or to receive from its service providers or contractors, a detailed explanation regarding why downstream notification would be impossible or involve disproportionate effect, the business would struggle to allocate sufficient resources and labor to handle its CPRA compliance efforts. Additionally, ensuring an accurate chain of communication to third parties may not be feasible in the digital marketplace. Similarly, as an operational matter, it is unreasonably burdensome to require a business to provide tailored and detailed explanations regarding the exemption it is relying on in denying a deletion request, in whole or in part. Critically, the Agency's proposed requirements for detailed explanations goes beyond the CPRA statute, which contains no such obligation. *See* Cal. Civ. Code § 1798.105.

Thus, for these reasons, we request the Agency to limit section 7022 to what is required under the CPRA and adopt our proposed modifications.

**12. The Proposed Requirement that a Business Notify Service Providers and Contractors of a Consumer's Request To Correct Exceeds the Agency's Authority Under the CPRA (Section 7023).**

A. Proposed Modification

*i. Preferred Approach*

(b) In determining the accuracy of the personal information that is the subject of a consumer's request to correct, the business shall take commercially reasonable efforts to correct the inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information. ~~consider the totality of the circumstances relating to the contest personal information.~~ A business may deny a consumer's request to correct if it determines that correction is not required under this subdivision ~~the contested personal information is more likely not accurate based on the totality of the circumstances~~.

(1) For purposes of this subdivision "nature of the personal information and the purposes of the processing of the personal information" includes whether the information is or was factual.

~~(1) Considering the totality of the circumstances includes, but is not limited to, considering:~~

~~(A) The nature of the personal information (e.g., whether it is objective, subjective, unstructured, sensitive, e.g.).~~

~~(B) How the business obtained the contested information.~~

~~(C) Documentation relating to the accuracy of the information whether provided by the consumer, the business, or another source. Requirements regarding documentation are set forth in subsection (d).~~

(1~~2~~) 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.

(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 in its systems. ~~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. 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.~~

. . .

(f) In responding to a request to correct, a business shall inform the consumer whether or not it has complied with the consumer's request. ~~If the business denies a consumer's request to correct in whole or in part, the business shall do the following:~~

~~(1) Explain the basis for the denial, including any conflict with federal or state law, exception to the CCPA, inadequacy in the required documentation, or contention that compliance proves impossible or involves disproportionate effort.~~

~~(2) If a business claims that complying with the consumer's request to correct would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot comply with the request. The business shall not simply state that it is impossible or would require disproportionate effort.~~

. . .

(i) Where 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 may~~shall749338220.2~~ provide the consumer with the name of the source from which the business received the alleged inaccurate information.

~~(j) Upon request, a business shall disclose all the specific pieces of personal information that the business maintains and has collected about the consumer to allow the consumer to confirm that the business has corrected the inaccurate information that was the subject of the consumer's request to correct. This disclosure shall not be considered a response to a request to know that is counted towards the limitation of two requests within a 12-month period as set forth in Civil Code section 1798.130, subdivision (b).~~

*ii. Alternative Approach*

(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 in its systems. 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.

. . .

(f) In responding to a request to correct, a business shall inform the consumer whether or not it has complied with the consumer's request. ~~If the business denies a consumer's request to correct in whole or in part, the business shall do the following:~~

~~(1) Explain the basis for the denial, including any conflict with federal or state law, exception to the CCPA, inadequacy in the required documentation, or contention that compliance proves impossible or involves disproportionate effort.~~

~~(2) If a business claims that complying with the consumer's request to correct would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot comply with the request. The business shall not simply state that it is impossible or would require disproportionate effort.~~

. . .

(i) Where 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~~ may provide the consumer with the name of the source from which the business received the alleged inaccurate information.

. . .

~~(j) Upon request, a business shall disclose all the specific pieces of personal information that the business maintains and has collected about the consumer to~~

~~allow the consumer to confirm that the business has corrected the inaccurate information that was the subject of the consumer's request to correct. This disclosure shall not be considered a response to a request to know that is counted towards the limitation of two requests within a 12-month period as set forth in Civil Code section 1798.130, subdivision (b).~~

B. Reasons for the Proposed Modification

To start, the Agency should strike the "totality of the circumstances" standard and related provisions from section 7023(b). This standard would create an onerous burden on a business's legal department to get involved in each request to conduct this analysis. Instead, the Agency should align the standard for determining accuracy of information with other data protection laws, such as the GDPR, to facilitate a consistence compliance approach for businesses and consumers. *See, e.g.*, GDPR, Art. 5(1)(d). The Agency should also clarify that the scope of the request to correct under this section necessarily excludes inferences, probabilistic data, and marketing-related information generally.

As to section 7023(c), the Agency exceeds its authority by requiring a business to notify service providers and contractors of a consumer's request to correct because there is no such requirement under the CPRA statute. Indeed, if the intent was to have such a requirement, it would have been included under the CPRA, as drafted in the right to delete. *Compare* Cal. Civ. Code § 1798.106 (no requirement to notify service providers and contractors), *with* Cal. Civ. Code § 1798.105(c)(1) ("A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records, notify any service providers or contractors to delete the consumer's personal information from their records, and notify all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information unless this proves impossible or involves disproportionate effort."). Alternatively, the Agency should adopt a more flexible standard that allows businesses not to provide notice to service providers or contractors if it would be impossible or require disproportionate effort. Our proposed modifications are important because section 7023 would impose significant operational burdens on businesses and require them to coordinate corrections with service providers and contractors in all instances, even when the processing of the personal information may not be germane to the business's direct interactions with consumers.

Lastly, the Agency should delete section 7023(j). In addition to creating an operational burden on businesses, the regulation is duplicative of existing access and transparency requests in section 7024. We would also request the Agency to modify section 7023(f) as proposed, for the reasons explained under Section 7 of this letter.

## 13. The Regulations Should Properly Place the Burden on the Consumer To Make a Specific Request for Information Exceeding the Prior 12 Months, Consistent with the Statute (Section 7024(h)).

### A. Proposed Modifications

*i. Section 7024(h)*

(h) In response to a request to know, a business shall provide all the personal information it has collected and maintains about the consumer on or after January 1, 2022 or all the personal information it has collected and maintained about the consumer during the 12-month period preceding the business's receipt of the request. The business may provide all the personal information it has collected and maintained about the consumer on or after January 1, 2022 that is beyond the 12-month period preceding the business's receipt of the request, unless doing so proves impossible or would involve disproportionate effort, or, alternatively, the business shall notify the consumer that they can also request the personal information beyond the 12-month period preceding the business's receipt of the request. The~~at~~ information shall include any personal information that the business's service providers or contractors obtained as a result of providing services to the business. If a business claims that providing personal information beyond the 12-month period would be impossible or would involve disproportionate effort, the business shall provide the consumer a ~~detailed~~ explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot provide personal information beyond the 12-month period. The business shall not simply state that it is impossible or would require disproportionate effort.

### B. Reasons for the Proposed Modification

The Agency should revise section 7024(h) to align with the allocation of responsibilities between the consumer and the business already provided under the CPRA. *See* Cal. Civ. Code § 1798.130(a)(2)(B). Under the statute, a consumer "may" request personal information beyond the 12-month period. However, the proposed regulations create ambiguity as to whether businesses are required to automatically provide personal information beyond the 12-month period by requiring that the business "shall" provide such personal information without specifying whether the consumer has requested this personal information. Also, the reference to January 1, 2022 in the statute was to make clear that there is no obligation to provide personal information collected prior to that time. But, under the text proposed, for a request received in December 2027 (as an example), the business would seemingly have to provide all information collected and maintained going back to January 1, 2022. The regulations should accurately allow businesses the flexibility to automatically provide the personal information beyond the 12-month period or to notify consumers of their ability to request personal information beyond the 12-month period upon the consumers' specific requests and also use the reference to January 1, 2022 for the purpose laid out in the statute.

**14. The Regulations on Requests To Limit the Use or Disclosure of Sensitive Information Should Be Revised To Align with the Text of the CRPA Statute, Avoid Undermining Consumer Choice, and Support Efforts To Combat Crime (Section 7027).**

A. Proposed Modification

(h) A business that uses or discloses sensitive personal information for the purpose of inferring characteristics creates a heightened risk of harm for the consumer. The purpose of the request to limit is to give consumers meaningful control over how their sensitive personal information is collected, used, and disclosed. It gives the consumer the ability to limit the business's use of sensitive personal information to that which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, with some narrowly tailored exceptions, which are set forth in subsection (l).

(i) In responding to a request to limit, a business may present the consumer with the choice to allow specific uses for the sensitive personal information as long as a single option to limit the use of the personal information is ~~more prominently~~ also presented ~~than the other choices~~.

…

(l) The purposes for which a business may use or disclose sensitive personal information without being required to offer consumers a right to limit are as follows. A business that only uses or discloses sensitive personal information for these purposes is not required to post a notice of right to limit.

…

(3) To resist malicious, deceptive, fraudulent, or illegal actions ~~directed at the business~~ and to prosecute those responsible for those actions, provided that the use of the consumer's personal information is reasonably necessary and proportionate for this purpose. For example, a business may use information about a consumer's ethnicity and/or the contents of email and text messages to investigate claims of racial discrimination or hate speech.

B. Reasons for the Proposed Modification

Initially, we propose modifying section 7027(i), which requires that the single option be presented more prominently than other choices. Doing so would subvert consumer choice and unnecessarily impede the sharing of truthful and accurate information with consumers. In addition, adopting such a standard would contradict section 7004 by directing unreasonable asymmetry in choice architecture in this instance. The presentation of specific use cases/options for consumers should align with the same general choice architecture requirements otherwise proposed by the regulations.

Next, we recommend that the Agency remove from section 7027(l)(3) the limitation that the exception to the right to limit for malicious, deceptive, fraudulent, or illegal actions is only available when such actions are "directed at the business." First, this language is predicated on the assumption that a business would be able to definitively know that such activities are directed at it. Instead, the Agency should promote transparency and working relationships with law enforcement agencies to stop bad acts, regardless of which business it is directed toward or whether it is possible to definitively tell. For example, if a business is aware that there is fraudulent activity directed at another business, the business should be permitted to use sensitive personal information to stop such activity and involve law enforcement if necessary. Limiting the ability of a business to disclose sensitive personal information in section 7027(l)(3) to only instances in which the business can tell that such acts are directed at it would impose unnecessary constraints, and potentially prevent businesses from proactively taking steps to stop crimes, even if possibly directed at other businesses.

## 15. **Procedures for Probable Cause Proceedings Should Be Modified To Give Businesses an Opportunity To Respond To Allegations Before Initiating a Proceeding (Section 7302).**

### A. Proposed Modification

(a) Probable Cause. Under Civil Code section 1798.199.50, probable cause exists when the evidence sufficiently supports a reasonable belief that the CCPA has been violated.

(b) Probable Cause Notice. The Enforcement Division will provide the alleged violator with notice of the probable cause proceeding as required by Civil Code section 1798.199.50.

(c) Probable Cause Report. No probable cause proceeding will take place until at least 30 calendar days after the Enforcement Division provides the following, by service of process or registered or certified mail with return receipt requested, to each alleged violator:

(1) A probable cause report that contains a written summary of the law and evidence that supports the Agency's reasonable belief that there is probable cause that each alleged violation of the CPRA has occurred, as well as a

description of any exculpatory evidence indicating a violation alleged in the report did not occur.

(2) Notification that each alleged violator has the right to respond in writing to the Enforcement Division and the right to be present in person and represented by counsel at the probable cause proceeding.

(d) Response to Probable Cause Report. Not later than 30 calendar days following service of the probable cause report, an alleged violator may submit to the Enforcement Division a written response to the probable cause report. The response should contain a summary of law and evidence that supports a position that the probable cause report fails to establish probable cause that any or all of the alleged violations of the CPRA occurred.

(e~~c~~) Probable Cause Proceeding.

(1) The proceeding shall be closed to the public unless the alleged violator files, at least 10 business days before the proceeding, a written request for a public proceeding. If the proceeding is not open to the public, then the proceeding may be conducted in whole or in part by telephone or videoconference.

(2) Agency staff shall conduct the proceeding informally. Only the alleged violator(s), their legal counsel, and Enforcement Division staff shall have the right to participate at the proceeding. Agency staff shall determine whether there is probable cause based on the probable cause notice, probable cause report, and any information or arguments presented at the probable cause proceeding by the parties.

(3) If the alleged violator(s) fails to participate or appear at the probable cause proceeding, the alleged violator(s) waives the right to further probable cause proceedings under Civil Code section 1798.199.50, and Agency staff shall determine whether there is probable cause based on the notice and any information or argument provided by the Enforcement Division.

(f~~d~~) Probable Cause Determination. Agency staff shall issue a written decision with their probable cause determination and serve it on the alleged violator electronically or by mail. ~~The Agency's probable cause determination is final and not subject to appeal.~~

(g~~e~~) Notices of probable cause and probable cause determinations shall not be open to the public nor admissible in evidence in any action or special proceeding other than one enforcing the CCPA.

B. Reasons for the Proposed Modification

Section 7302 should be modified to provide businesses that are subject to a potential enforcement action an opportunity to receive all information that forms the basis of the alleged violations and be given an adequate opportunity to respond in writing in advance of the probable cause proceedings.

For example, the California Public Utilities Commission (CPUC) implements progressive enforcement, characterized as:

> [A]n escalating series of actions, beginning with actions such as a warning letter or notification of violation followed by actions that compel compliance and may result in the imposition of penalties or fines (e.g., the issuance of an enforcement order or filing a civil or criminal action). Progressive enforcement may not be an appropriate enforcement response when violations result from intentional or grossly negligent misconduct, where the impacts on ratepayers or other consumers are widespread, or where impacts to safety are significant.

*See* CPUC Enforcement Policy, R. M-4846 at 4, (November 5, 2020). CPUC enforcement generally begins with a Notice of Violation, giving the entity 30 days to dispute or cure the violation. *Id.* at 8-9. There is the possibility to propose a negotiated settlement, to adopt an Administrative Consent Order, and to follow a Citation and Compliance Program. *Id.* at 10-12. And there is the possibility of an Order to Show Cause why a CPUC action should not be taken. *Id.* at 14.

The proposed modifications are intended to be consistent with this enforcement process and align with the CPRA statute, which requires the Agency to provide at least 30 days' notice before there is a finding of probable cause. *See* Cal. Civ. Code § 1798.199.50. The proposed modifications to section 7302 build on this process to develop a written briefing process in advance of the actual probable cause proceedings. This is also in line with the Fair Political Practices Commission (FPPC), which has a similar probable cause requirement, and includes a lengthy and detailed set of requirements on this point—including requiring a formal probable cause report, allowing for a written response and a reply, after which a probable cause hearing officer determines if there is probable cause to proceed.

Finally, we propose modifications to section 7302 to ensure that an alleged violator can receive detailed allegations and respond in advance of the hearing. We also propose a modification or an appeal right if there is an erroneous probable cause determination, which the current proposed draft does not allow. It is possible that the final determination was based on incorrect law or evidence, leading to further action against the business despite these errors. This proposal is intended to remedy this issue.

In sum, with the above-proposed revisions, the Agency and businesses will have an opportunity to exchange critical information so that any decision regarding probable cause is fully informed and there is an opportunity to address any errors in the decision.

## CONCLUSION

California voters entrusted the Agency with not only protecting personal information, but also ensuring a judicious balance between consumer privacy and business innovation. *See* Cal. Civ. Code § 1798.199.40(l). To ensure this balance, the CPRA grants the Agency a limited authority to enforce the CPRA consistent with its statutory provisions. *See* Cal. Civ. Code § 1798.199.40(b). Throughout this letter, we have identified a number of instances where the Agency has exceeded its authority or made proposals that create undue burdens for businesses without countervailing benefits for consumers. We request that the Agency consider our proposed modifications and ensure that the CPRA regulations align with the statute, as the voters intended.

**Submitted on behalf of the California Chamber of Commerce**

[redacted]

**Dominique Shelton Leipzig,**
**Partner, Cybersecurity & Data Privacy**
**Leader, Global Data Innovation and Ad Tech Privacy & Data Management practices**
**Mayer Brown**
Arsen Kourinian, Partner
Sasha Keck, Associate
Megan Von Borstel, Associate
Britteny Leyva, Associate