

From: **Christopher Rosina** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
CC: **Jane Horvath** [REDACTED]
Subject: CPPA Public Comment
Date: 23.08.2022 14:14:13 (+02:00)
Attachments: Apple Inc. Comments on CPRA Proposed Regulations.pdf (17 pages)

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

Dear CPPA,

Attached, please find the public comments of Apple, Inc.

Sincerely,
Chris Rosina

Christopher Rosina
Senior Privacy Counsel
Global Privacy Law and Policy
Apple Inc.
[REDACTED]

COMMENTS OF APPLE INC.
in connection with the California Privacy Protection Agency Rulemaking
regarding the California Consumer Privacy Act of 2018, as amended by the California
Privacy Rights Act

Introduction

At Apple, we believe privacy is a fundamental human right. We greatly appreciate the opportunity to submit comments to the California Privacy Protection Agency (Agency) and the significant, thoughtful effort that it has put forth in drafting updated regulations for the California Consumer Privacy Act (Proposed Regulations).

We stand by our ongoing commitment to protect consumer privacy. We also recognize that safeguards that go beyond the commitments of individual companies sometimes are needed to best protect consumers' rights. Laws and regulations can ensure that individuals understand how their personal information is used and help instill confidence that their privacy will be respected, regardless of the values or business model of the particular company that is collecting or processing their data.

To make the greatest impact, we believe that laws and regulations must not only deter harmful uses of personal information, but also encourage businesses to take privacy-protective paths forward, including by allowing businesses to invest resources in the areas that will have the greatest impact on protecting privacy. We respectfully offer the following comments on the Proposed Regulations through which the Agency can increase privacy protections for consumers, clarify ambiguities, encourage consumer-friendly practices, and help avoid unintended, negative consequences.

First, we encourage the Agency to allow businesses to process rights requests for individuals who use shared devices when it is reasonably clear which individual is using the device. This will help protect members of a household who share accounts and strengthen the privacy rights of individuals who maintain separate user profiles within an account on shared devices.

We also ask the Agency to continue supporting transparency-based approaches and to incentivize straightforward, easy-to-understand notices by permitting businesses to provide links to privacy information.

The Agency also should clarify that the opt-out preference signal obligations apply only to businesses that sell or share personal information. This will reduce potential confusion amongst consumers and incentivize businesses to take privacy-protective approaches for the disclosure of personal information.

Permitting businesses to require authentication for certain consumer requests in instances where consumers maintain accounts also would strengthen privacy protections. Similarly, we encourage the Agency to help reduce instances of fraudulent consumer requests by allowing suspected fraud to be addressed simply by noting that the request could not be verified.

I. *The Agency Should Clarify the Definition of “Household” to Strengthen Privacy Protections for Shared Devices and Permit Businesses to Make Reasonable Determinations Regarding What Data is Household Data.*

Apple believes that all consumers deserve privacy protections, including when they share a device. Whether it’s a shared iPad that family members use to play games from the App Store together, or a HomePod that roommates share to play music in the kitchen, it’s common for single devices to be used by multiple members of a household. To increase consumer privacy, we encourage the Agency to provide additional guidance regarding “household” data and **clarify that businesses may make reasonable determinations regarding whether a device is shared.** We also ask the Agency to **confirm that a business may treat a user’s data as individual personal information, rather than household data,** for purposes of rights requests **when the business can reasonably identify the individual that is using a shared device.**

Although the California Privacy Rights Act (“CPRA”) includes a definition of “household,” it does not make clear how businesses that collect personal information from shared devices should treat information collected from such devices. We appreciate that the definition of “household” is now part of the text of the CCPA and that the definition in the CCPA regulations currently in force (Regulations) may no longer be needed. However, other regulations prescribing how businesses must handle household information, including section 7031 of the Regulations (regarding requests to know or delete household information), were removed alongside it in the Proposed Regulations.

By removing all of the household-related provisions, the Proposed Regulations could leave individuals’ privacy rights exposed in some situations and could even spur exploitation by bad actors. Additionally, an individual should not be denied their privacy rights solely because they may let another individual use one of their devices. For example, a group of roommates may have house guests who request music from a HomePod linked to one user’s Apple Music Account. This should not remove the HomePod owner’s ability to request data related to their use of the HomePod.

Given the above, the Proposed Regulations should permit businesses to make reasonable determinations regarding whether a device is shared based on the generally accepted use of a product and the information the business has collected regarding a device (e.g., the location where a service was accessed).

The Proposed Regulations also should permit businesses to treat personal information as linked to an individual (rather than as household data) where the business reasonably can link personal information to a specific user's account.

For example, an Apple Music subscriber may share an Apple Music Family subscription with other individuals in their iCloud family, which each family member accesses through a shared MacBook. Each family member signs in with their own Apple ID to access the subscription, listen to songs of interest to them, and receive personalized recommendations for content they might enjoy, separate from any content their family members may listen to and enjoy, while not requiring that they all maintain separate subscriptions. In cases such as these—i.e., where it's possible to identify the individual using a shared device (in this case because of the Apple ID they use to log in and gain access to a family account)—businesses should be allowed to respond to rights requests that are submitted by that user with information relevant to that particular user (rather than treating it as household data), even if that information is collected and processed on a shared device, like a single MacBook.

II. *Apple Strives to Provide Consumers with Genuine Comprehension of its Data Processing Practices, and We Encourage the Agency to Continue Supporting Transparency-Based Approaches.*

Apple has long focused on providing users with first-rate transparency and understands that transparency is of paramount importance to providing great products and services. We believe that consumers should know how businesses—including Apple—will collect, use, and disclose personal information that consumers entrust to businesses. Indeed, this is why Apple goes to great lengths not only to meet legal requirements regarding transparency, including requirements outside of the U.S., but adopting best practices that affirmatively help users comprehend how Apple uses their personal information.

Moreover, the CCPA and CPRA share a common foundation: that consumers should be informed about the ways in which businesses will collect, use, and disclose their personal information. Both laws eschewed the requirement that businesses obtain consumer consent or otherwise justify processing on specific legitimate bases in favor of a framework that entrusts the decision of whether processing activities are acceptable to the consumers, themselves, by ensuring that businesses provide appropriate information about their practices. **We encourage the Agency to continue supporting transparency-based approaches as it develops new regulations.**

Apple has been at the forefront of providing consumers with easy-to-digest information that clearly explains how Apple uses their personal information. This information allows users to understand and reasonably to expect the ways in which we process their personal information. Some examples of the ways in which we aim for genuine comprehension by our users include: (i) clear disclosures; (ii) the Data & Privacy Icon; (iii) layered notices; (iv) detailed notices when Apple devices are first loaded; and (iv) using common formatting.

Clear privacy disclosures. Apple discloses its privacy practices and user choices in plain language. These disclosures are presented both through just-in-time product-specific notices¹ that are accompanied by our Data & Privacy Icon (discussed below) and the Apple Privacy Policy² that applies across our business. All of our disclosures are designed with comprehension in mind and prioritize providing the information that consumers need to know to make an informed decision. These disclosures help set consumer expectations about how Apple processes personal information. A screenshot of the product-specific notice for Apple Music & Privacy is available in Appendix, Exhibit C.

Data & Privacy Icon. Apple has been on the forefront of using iconography to support comprehension amongst consumers. One of our innovations in this area was adopting our Data & Privacy Icon (the “Icon”) to signal to users that the disclosures relate to the processing of their personal information and to avoid concerns about transparency fatigue. A screenshot of the Icon is available in Appendix, Exhibit B.

Layered notices. The Apple Privacy Policy was designed to enhance user comprehension through an internationally accepted best practice of layered notices. Layered notices start with a simple and straightforward summary of what personal information is at issue, the business’s reason for collecting and processing it, and a link to the fuller policy. This method is consistent with California’s dual interests in providing consumers with disclosures that are in “plain” and “straightforward” language, while assuring that the consumer is still presented with the relevant privacy disclosures for a product or feature at or before the point of personal information collection. The Apple Privacy Policy serves as the first layer in our approach to layered-notice transparency, with more detailed notices—as described below in more detail—presented to users on a product or service-specific basis.

Detailed notices appearing as you first engage with Apple devices. Apple designs the start-up experience on a new Apple device to welcome all consumers regardless of language or ability, and we include detailed disclosures about our processing of personal information to create a carefully curated start-up experience. These disclosures are a key method through which we inform new and existing Apple users of our Privacy Policy and relevant product-specific information. For example, in the Apple Music privacy disclosure, we describe the information that Apple collects about users’ Apple Music activity, how Apple receives information from a user’s cloud library to identify and unlock songs that are also available in Apple Music, and how long Apple retains records of the songs that users play.³ We also refer users to the Apple Privacy Policy, where they can find additional information regarding Apple’s information

¹ You can find a list of our product-specific notices at <https://www.apple.com/legal/privacy/data/>. See also <https://developer.apple.com/app-store/user-privacy-and-data-use/> (for developer guidance regarding designing just-in-time privacy notices). Relevant screenshots are included in Appendix, Exhibit A.

² <https://www.apple.com/legal/privacy/en-ww/>.

³ See Apple Music & Privacy, available at: <https://www.apple.com/legal/privacy/data/en/apple-music/>. Relevant screenshots are included in Appendix, Exhibit C.

practices.⁴ This practice of providing users with both product-specific disclosures and the general Apple Privacy Policy creates the layered notice effect discussed above, which promotes transparency and user comprehension.

Common formatting. Apple has adopted a consistent format for privacy-related disclosures, leveraging, in particular, the Icon to draw attention to the disclosures regarding the processing of personal information. By providing a consistent experience, Apple users can understand exactly how their personal information will be processed when they interact with each Apple product or service.

Apple takes pride in being able to surprise and delight its users with new, innovative products and services. We also understand that consumer trust is a fundamental element of our business success, particularly in an age where trust in business is so low. We disclose that fact in our privacy notices, thereby ensuring that our customers will know about, understand, and expect the ways in which we use their data.

III. *Businesses Should Be Able to Direct Consumers to Support Pages Explaining How to Delete Portions of Their Personal Information, Rather Than Including Lengthy Instructions for All Products and Services.*

Apple is deeply committed to transparency and supports efforts to ensure that consumers are informed of the control they have over their data. Accordingly, we agree with the principle, advanced in the Proposed Regulations, that, where a business offers granular options for data deletion, consumers should be made aware of those options prior to deleting all of their data.

However, the second part of the requirement in proposed subsection 7022(h)—that businesses providing consumers the ability to delete select categories of personal information in contexts *other than* responding to a deletion request must “direct them to how they can do so”—could undermine transparency and make it more difficult for consumers to exercise this greater degree of control over their data. Instead, **businesses should be permitted to provide consumers with links to support pages and other resources, rather than providing a detailed explanation of how to delete each type of information from each product or service in the deletion process.**

At Apple, we offer consumers a wide range of options for deletion. These include (among many others) the ability to delete individual browsing history items in Safari, the ability to delete individual songs in the Apple Music Library, and the ability to reset an individual identifier that helps personalize the information you receive with Apple News.⁵ A requirement to provide, in Apple’s privacy policies and disclosures, step-by-step instructions for consumers to delete all

⁴ See *id.*

⁵ See Apple News & Privacy, available at: <https://www.apple.com/legal/privacy/data/en/apple-news/>. Relevant screenshots are included in Appendix, Exhibit D.

of their various kinds of data across all of Apple’s different products and services would add numerous pages to those documents and render them less accessible for consumers.

Moreover, businesses may simply choose not to offer such granular deletion options and instead may take an all-or-nothing approach to deletion in an effort to avoid the related compliance obligations. Consequently, subsection 7022(h)’s “direction” requirement ultimately could deprive consumers of certain privacy choices.

To avoid these outcomes, we propose revising subsection 7022(h) as follows:

§ 7022(h)

*In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information as long as a single option to delete all personal information is also offered and more prominently presented than the other choices. A business that provides consumers the ability to delete select categories of personal information (e.g., purchase history, browsing history, voice recordings) in other contexts, however, must inform consumers of their ability to do so and direct them to how they can do so. **For the purposes of this section, businesses may direct consumers to how they can delete select categories of personal information by providing them with a link to a support page or other resource that explains consumers’ data deletion options.***

IV. The Agency Should Confirm that Opt-Out Preference Signal Requirements Apply Only to Businesses That Sell or Share Personal Information.

As currently drafted, the requirements for opt-out preference signals have the potential to confuse consumers, especially in cases where a consumer expects to receive a communication regarding their use of an opt-out signal but the business does not sell or share personal information.

For example, the Proposed Regulations state in part that:

§ 7025(c)(6)

The business should display whether or not it has processed the consumer’s opt-out preference signal.

Our understanding is that the Agency expects only businesses that sell or share personal information to provide such communication to consumers. A business that does not sell or share a consumer’s personal information does not need to provide such confirmation to a consumer both because the business is not engaging in any conduct—selling or sharing personal information—to which the right to opt-out applies and because the preference signal would not result in changes to how the business processes the consumer’s information. However, a consumer who does not receive a communication regarding the opt-out signal from

such a business might become confused and lose confidence in a business's privacy protections.

We therefore request that the Agency **confirm expressly that businesses that do not sell or share personal information do not have to respond to, acknowledge, or otherwise engage with opt-out preference signals under section 7025 of the Proposed Regulations.** Including such language also would increase incentives for businesses not to sell or share personal information and would encourage them to direct resources towards other compliance initiatives.

We propose the following clarification language for the Agency's consideration:

§ 7025(f)

A business that does not sell or share personal information is not obligated to process any opt-out preference signal. The obligations under this section apply only to businesses that sell or share personal information.

V. *Businesses Should Be Allowed to Require Authentication for Requests to Limit the Use and Disclosure of Sensitive Personal Information and Should Not Be Required to Disclose that Requests Were Rejected Because They Were Fraudulent.*

Apple supports consumers' right to limit the use and disclosure of their sensitive personal information (right to limit). However, we are concerned that the Proposed Regulations' prohibition on requiring verifiable consumer requests for requests to limit, as well as the requirement that a business explain to requestors why it believes certain requests are fraudulent, may create new privacy and security risks to consumers. In particular, we are concerned that these requirements will increase the number of fraudulent requests and make it easier for bad actors to circumvent anti-fraud controls. For these reasons, we urge the Agency: **(A) to allow a business to require authentication for requests to limit submitted by consumers that maintain accounts with the business; and (B) to allow fraudulent requests to be addressed by permitting the business to respond noting simply that the request could not be verified.**

A. *For Users That Maintain Accounts with the Business, Businesses Should Be Allowed to Require Authentication for Requests to Limit the Use and Disclosure of Sensitive Personal Information.*

Proposed subsection 7027(e) prohibits businesses from requiring a verifiable consumer request for a request to limit. For companies (such as Apple) that have account registration capabilities and invest in ensuring their systems are secure, this prohibition would lower the bar for making changes to a user's account and increase privacy and security risks to consumers.

Currently, Apple requires users to be authenticated—including via multi-factor authentication, if the user has this feature enabled—before they may make any changes to their accounts. This requirement protects our users by ensuring that unauthorized users do not have access to their personal information. But under subsection 7027(e), where such changes involve a request to limit the use or disclosure of the consumer’s sensitive personal information to the purposes specified in subsection 7027(l), Apple and other businesses would not be able to adhere to their normally high security standard of requiring that the user be authenticated before making any changes to the account. This could endanger consumers’ sensitive personal information by resulting in increased instances of fraudulent requests.

To guard against this increased risk of fraudulent requests, **the Agency should revise subsection 7027(e) to clarify that, where a consumer maintains an account with a business, the business may require the consumer to log into the account to submit a request to limit. The Agency should also revise the definition of “verify” in subsection 7000(jj) to expressly include requests to limit.** We suggest possible revisions below:

§ 7027(e)

*A business shall not require a verifiable consumer request for a request to limit, **except that where a consumer maintains an account with a business, the business may require the consumer to log into the account to submit a request to limit.** A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer to whom the request should be applied. However, to the extent that the business can comply with a request to limit without additional information, it shall do so.*

§ 7000(jj)

*“Verify” means to determine that the consumer making a request to know or request to delete, request to correct, ~~or~~ request to know, **or request to limit** is the consumer about whom the business has collected information, or if that consumer is less than 13 years of age, the consumer’s parent or legal guardian.*

B. Businesses Should Not Be Required to Disclose that Requests Were Rejected Because They Were Fraudulent.

Subsection 7027(f) would require businesses to disclose when requests to limit are rejected because they are believed to be fraudulent and to explain the reasons for that belief. Specifically, proposed subsection 7027(f) provides: “If a business has a good-faith, reasonable, and documented belief that a request to limit is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide to the requestor an explanation why it believes the request is fraudulent.”

This requirement is likely to increase privacy and security risks to consumers by making it easier for bad actors to circumvent anti-fraud controls. Requiring a business to

explain the reasons why it believes a request is fraudulent would provide bad actors with a blueprint as to how the business detects fraud and, consequently, how to avoid being detected in the future. And, as bad actors continue to learn the fraud indicators to avoid over time, they will get better at submitting requests and eventually evade businesses' fraud detection measures, altogether.

To avoid this increased risk to consumer privacy and security, **subsection 7027(f) should be revised to require only that businesses inform requestors that their requests were denied because they could not be verified.** Such a requirement would serve to provide transparency for legitimate requestors whose requests were erroneously denied, without helping to create increasingly sophisticated bad actors with a heightened ability to circumvent anti-fraud controls. We therefore propose the following revision to subsection 7027(f):

§ 7027(f)

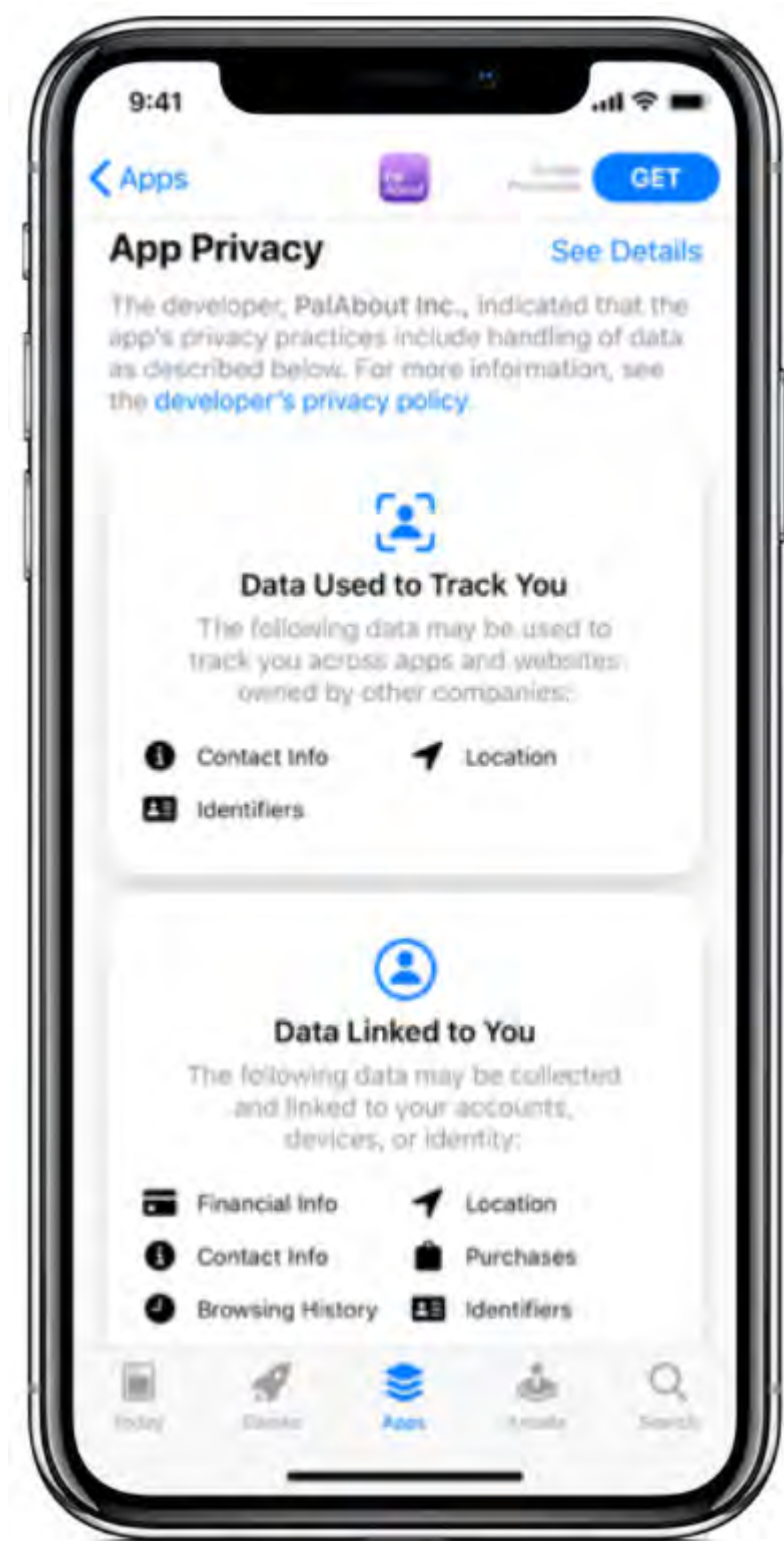
If a business has a good-faith, reasonable, and documented belief that a request to limit is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request ~~and shall provide to the requestor an explanation why it believes the request is fraudulent~~ because the request could not be verified.

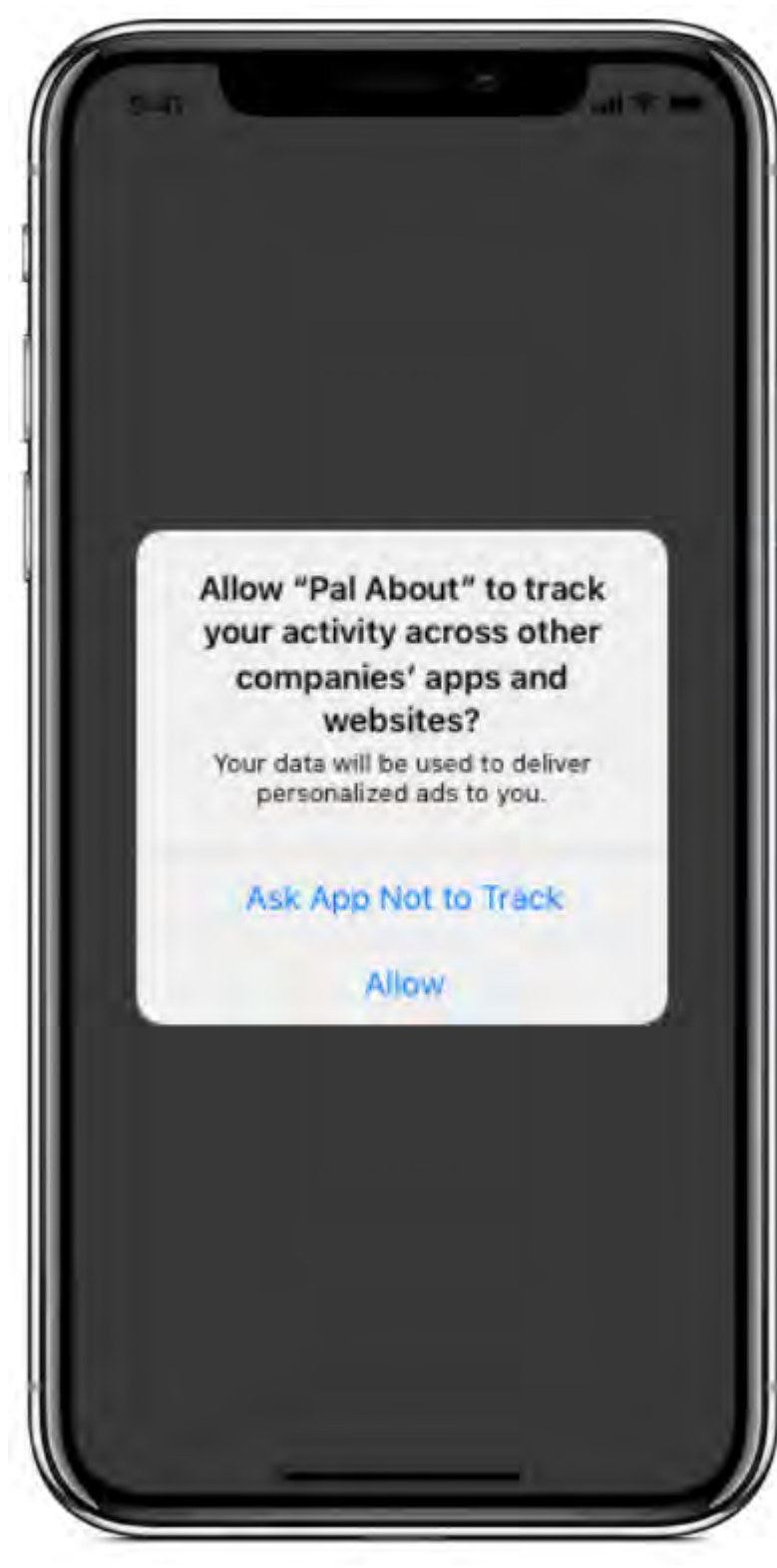
Respectfully,



Jane Horvath
Chief Privacy Officer, Apple Inc.

APPENDIX TO COMMENTS OF APPLE INC.

Exhibit A

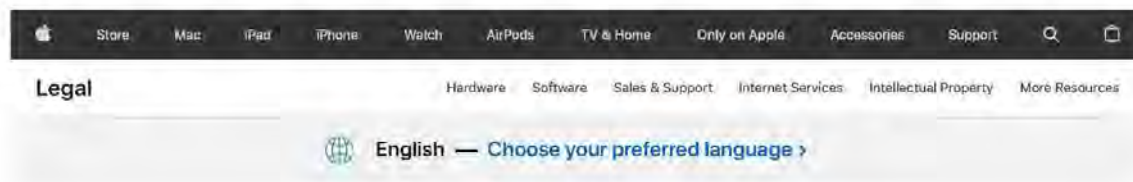


Source: Apple, "User Privacy and Data Use", available at: <https://developer.apple.com/app-store/user-privacy-and-data-use/>.

Exhibit B

Source: See *generally*, Apple, "Privacy Control", available at: <https://www.apple.com/privacy/control/>.

Exhibit C



Apple Music & Privacy

Apple Music is designed to protect your information and enable you to choose what you share.



- Apple collects information about your Apple Music activity, such as the songs you play and how long you play them, to personalize the service when you are subscribed or enrolled in a preview of our services, send you notifications, and compensate our partners.
- Your cloud library sends information from your music library to Apple, such as song and artist names, to identify and unlock copies of any of your songs that are also available in Apple Music.
- We associate your cloud library information with you for as long as you remain subscribed and for a short time after. We retain records of the songs you play for the periods specified by applicable laws relating to financial reporting.
- To help identify and prevent fraud, information about how you use your device, including the approximate number of phone calls or emails you send and receive, will be used to compute a device trust score when you attempt a purchase. The submissions are designed so Apple cannot learn the real values on your device. The scores are stored for a fixed time on our servers.

Protecting the privacy and security of your information is a priority for everyone at Apple. We work hard to collect only the data we need to make your experience better, and when we do collect data we believe it's important for you to know what we're collecting and why we need it, so you can make informed choices. Apple Music, like every Apple product and service, is designed with these principles in mind.

We use your personal information to provide the services and features in Apple Music. This information includes your account and payment information, which you can access and change in Settings or System Preferences.

When you subscribe, Apple collects information about how you use Apple Music in order to tailor features to your musical tastes. These features include Listen Now, where you see albums and playlists picked for you, and Radio, which plays selections from your favorite artists and genres. We also use this information so that we can contact you by email and push notification about upcoming releases, new artists, and other happenings on Apple Music that you may like.

When you participate in a preview of our services, Apple collects information about how you use Apple Music and may use this information in order to tailor your experience.

If you want to connect or share with other people using Apple Music, you can create a personal profile by providing a user handle (for example, @johnappleseed), display name, and, if desired, a profile photo and

other information. Apple stores this information with your account so that you can access it from any of your devices. Your user handle, display name, and profile photo can appear alongside any content you post and activity that you share on Apple Music. Sharing and posting content are not currently intended for or available to Apple IDs for children.

Other people may also be able to find your Apple Music profile using the information that you've provided.

You can make the contents of your profile, like listening activity and playlists, available only to those you choose. However, your profile information, such as handle, display name, photo, your followers, and who you are following, are always visible to everyone.

When you create a profile on Apple Music, we will recommend other Apple Music subscribers with whom you may want to connect as friends. Apple does not learn or store information from your contacts when checking for friends to recommend. Only shortened and encrypted hashes of the phone numbers and email addresses in your contacts are sent to Apple, and then matching Apple Music subscribers to be recommended are determined locally on your device. Apple Music can periodically check your contacts to recommend new friends in the future; you can control this in Account Settings by disabling Contacts on Apple Music. If you do not want to be found by others based on the Apple ID contact information they may have about you in their contacts, you can change this in Account Settings by disabling Allow Finding by Apple ID.

Information that you provide in your profile may be updated or removed by you at any time. Whenever you share online, you should think carefully about what you are making public. When you share from Apple Music to other websites or social networks, anything you share is governed by the privacy policies of those other services.

If your mobile network provider offers Apple Music memberships and free trials, Apple may check your phone number to determine if you are eligible through a mobile network provider partner. If you signed up through your mobile network provider, your phone number is used to identify your account and to let the mobile network provider know that you have activated your membership. We will use the phone number associated with your membership to verify your account at sign in and to connect your Apple Music activity with your account. We also use your phone number to request cancellation of your membership with your mobile network provider at your request.

Your cloud library, which is a benefit of your Apple Music membership, allows you to have access to the songs and playlists in your library from any of your devices. This feature sends information from your music library to Apple, such as song and artist names, in order to identify and unlock copies of any of your songs that are also available in Apple Music. Any songs that can't be found in Apple Music are uploaded to your personal cloud library, so that you can have access to your complete collection from any of your devices. To stop syncing your cloud library on iOS and iPadOS, go to Settings > Music and tap to turn off Sync Library. On Mac, open Apple Music and go to Preferences > General, then deselect Sync Library.

When you use your Apple Music membership, we collect information about the songs and videos you play or add to your music library or playlists, and the content you love, comment or share. Information such as the account, IP address, and device, app, or car interface you used to play, where in Apple Music you were when you played it, the time you played it, and for how long is noted and sent to Apple. We use this information to customize your Apple Music experience, to send you emails and notifications, and to help us understand how Apple Music is being used so we may improve it. For example, this information can help us pick the music, videos, and artist content that we show you in Listen Now and Radio. It also allows us to make other recommendations to you that reflect your tastes, create city charts to show you trending music by city, pay royalties and prevent or take action against activities that are, or may be, in breach of the Apple Media Services Terms and Conditions or applicable law.

We retain this information for the duration of your Apple Music membership and thereafter where it is necessary for financial reporting for the periods specified by applicable laws relating to such reporting,

which vary by region. For most customers, that requires at least a 10-year retention period, but in regions such as China that period can be 30 years.

If you use SharePlay to listen to content with other users, the Apple Music app will collect that you listened to that content during a SharePlay session and the approximate number of participants in the SharePlay session, but does not collect any information to identify the participants of a SharePlay session.

Apple may use information about your account, such as the Apple products you own and your subscriptions to Apple services, to send you communications about Apple Music and other Apple products, services, and offers that may be of interest to you, including Apple One. Your device serial number and other hardware identifiers may be used to check eligibility for service offers. If you are in a Family Sharing group, Apple may send you communications about products, services, and offers available to you through Family Sharing. If you purchase an Apple One subscription, we may send you emails and push notifications about the features of each of the services for which you have subscribed. Apple may also use information about your activity within Apple Music to send you emails and push notifications about new features, content, and offers available in Apple Music. You can change your email preferences and opt out of receiving these emails by going to appleid.apple.com. To update your notification preferences on iOS and iPadOS, go to Settings > Notifications > Music. On Mac, open Apple Music and go to Preferences > General > Notifications. Apple uses information about your interactions with our communications, including notifications, to improve our services.

Some Apple Music features, such as certain broadcast radio stations, may not be available in your region. Apple may use the IP address of your Internet connection to approximate your location and determine availability. We also compute a device trust score on your device when you attempt a purchase using information about how you use your device, including the approximate number of phone calls or emails you send and receive. The submission is designed so Apple cannot learn the underlying values on your device. The score is stored for a fixed time on our servers.

We may collect, use, transfer, and disclose non-personal information for any purpose. For example, we may aggregate your non-personal information with that of other Apple Music users in order to improve the service. We may also collect certain performance metrics from your device when you use Apple Music, including radio frequency strength, country code, network code, and cellular radio access technology.

At all times, information collected by Apple will be treated in accordance with Apple's Privacy Policy, which can be found at www.apple.com/privacy

Disclosure to Third Parties

When you use Apple Music to listen to broadcast radio, your device connects directly to the broadcast radio station to provide you the requested content. When it connects, your device's IP address will be visible to the broadcast radio station. The handling of your IP address by the broadcast radio station is governed by the privacy policies of the broadcast radio station or its provider.

We are obligated to provide some aggregated non-personal information about the use of Apple Music, as well as aggregated user demographics such as age group and gender (which may be inferred from information such as your name and salutation in your Apple ID account), to record labels, publishers, and artists so that they can measure the performance of their creative work and meet royalty and accounting requirements. In addition, we share aggregated listening activity with chart compilers for music charts around the world and with music marketing platforms that help labels and artists reach listeners. In order to determine your subscription eligibility if you subscribe through a third-party partner like a mobile network provider, or to complete your purchase, we share limited personally identifiable information with that partner.

iOS and iPadOS apps may request access to Apple Music and your cloud library. If you give such permission to an app, it can access information like your cloud library on device, whether you are an Apple Music subscriber, your music and video play activity, and your Listen Now recommendations. A permitted app can also modify data associated with your account, such as which songs are in your library and

playlists. You can disable an app's access on your iOS or iPadOS device by going to **Settings > Privacy > Media & Apple Music**. On Mac, go to **System Preferences > Security & Privacy > Privacy > Media & Apple Music**. If you have removed the app or granted an app access using a version of iOS prior to iOS 11 or iPadOS, you can disable its access in your Apple Music account settings.

Retention

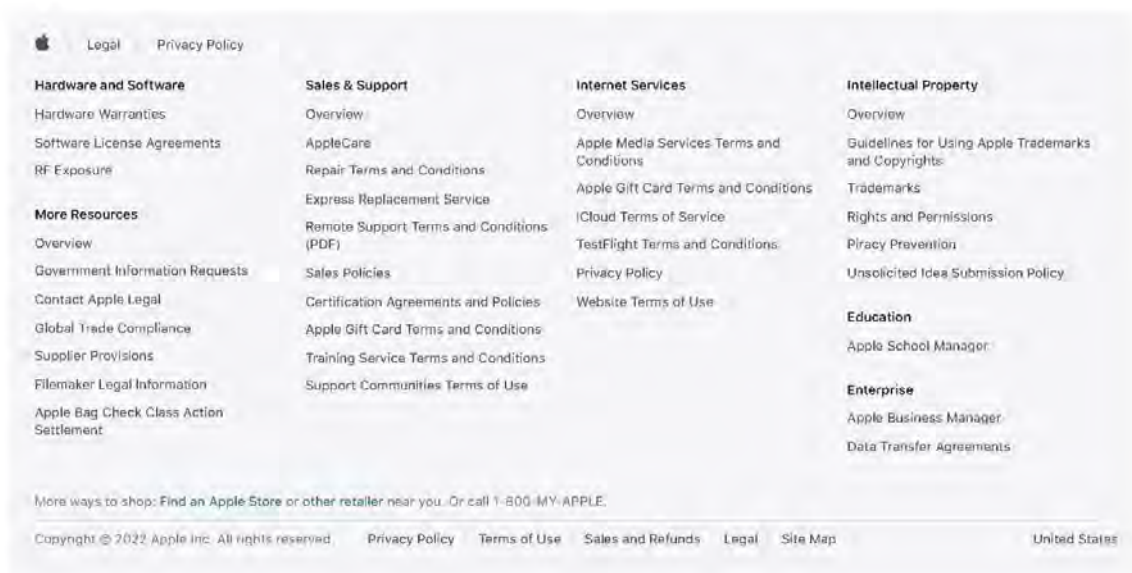
When you use a payment card, Apple may retain and automatically update your card number and billing information for future purchases, recurring transactions, or other uses you authorize. Apple may obtain this information from your financial institution or payment network, and also use it for fraud prevention and verification.

[Learn More About Apple Music](#)

For more detailed information, including features and pricing, visit www.apple.com/apple-music.

For information about Apple Music Web Player & Privacy, visit www.apple.com/legal/privacy/data/en/apple-music-web.

Published Date: May 13, 2022



Source: Apple Music & Privacy, available at:
<https://www.apple.com/legal/privacy/data/en/apple-music/>.

Exhibit D

We understand that the stories you read and listen to are personal, so we designed the News and Stocks apps so your reading and listening activity is not linked to other Apple services. The data we collect is associated with an identifier specific to the News and Stocks apps.

Recommendations in Apple News are made based on the information stored on your device. To clear your reading and listening history, tap or click Clear in the History section of News in iOS or iPadOS. On your Mac, go to News > Clear History and click Clear History. This will also reset the identifier used for News and Stocks. You can also reset the identifier without clearing your reading and listening history on your iOS or iPadOS device by going to Settings > News, then tapping to turn on Reset Identifier. On your Mac, open News, then go to News > Clear History and click Reset Identifier.

Source: Apple News & Privacy, available at: <https://www.apple.com/legal/privacy/data/en/apple-news/>

From: **Angelena Bradfield** [REDACTED]
To: **Regulations** <Regulations@cpga.ca.gov>
CC: **Matthew Rosenthal** [REDACTED]
Subject: CPGA Public Comment
Date: 23.08.2022 21:26:38 (+02:00)
Attachments: BPI Letter to CPGA re CCPA Regulatory Changes Under CPRA vF.pdf (33 pages)

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

To Whom It May Concern: Please find attached the comments from the Bank Policy Institute on the CPGA's proposed changes to CCPA regulations in light of the CPRA. Please let us know if you have any questions, we would be happy to discuss our comments further.

Sincerely, Angelena

Angelena Bradfield

Senior Vice President, AML/BSA, Sanctions & Privacy
[REDACTED]

Phone: [REDACTED]



August 23, 2022

Via electronic mail

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

Re: **Proposed Regulations Under the California Consumer Privacy Act**

To Whom It May Concern:

The Bank Policy Institute¹ appreciates the opportunity to submit comments to the California Privacy Protection Agency on proposed regulations implementing the California Consumer Privacy Act, as amended by the California Privacy Rights Act.²

I. Executive Summary

BPI members are committed to promoting robust privacy protections for California consumers within the parameters set out by the CCPA. BPI's members are financial institutions that have invested significant time and resources into building data protection and information security compliance systems that align with federal and state financial privacy laws.

Drawing on the experience of its members operationalizing privacy and security safeguards for their customers, BPI has carefully considered the Proposed Regulations, which reflect nearly 70-pages of detailed requirements that build on, and in some cases impose new requirements that go beyond, statutory protections.

While we support aspects of the Proposed Regulations, we recommend through this letter certain amendments, including to ensure consistency with the statutory text and other federal and state privacy and consumer protection frameworks. We also have identified several areas of the Proposed Regulations where prescriptive requirements limit flexibility for businesses that are

¹ The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost two million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

² Cal. Civ. Code § 1798.100 *et seq.*

subject to multiple privacy frameworks, which may lead to consumer confusion rather than provide consumers greater clarity, as we presume was intended. The Proposed Regulations should focus on incentivizing businesses to better protect consumers, without detailed technical requirements with no tangible consumer benefit that could serve to distract businesses from focusing on core protections. In addition, we identify proposed requirements that potentially undermine the privacy aims of the statutory framework by requiring businesses to obtain and maintain more information about consumers than they otherwise would or by making it more challenging for businesses to safeguard consumers against identity theft and other data security risks.

For ease, **Appendix A**, which is referenced throughout, contains a set of proposed amendments that BPI urges the Agency to adopt.

II. Key Principles

Our comments on the Proposed Regulations focus on three key principles that we urge the Agency to consider as it undergoes the important process of evaluating and refining the Proposed Regulations.

First, the Proposed Regulations should enhance the consumer experience by protecting consumers' choices about their personal information, promoting practices grounded in data minimization and streamlining disclosures and choices presented to consumers.

The Proposed Regulations are strongest when they set forth clear but flexible standards that embody these principles, such as requirements that disclosures and communications be "easy to read and understandable by consumers."³ Consumers are not necessarily served by lengthy and technical disclosures or overly prescriptive presentation requirements. Indeed, federal banking regulators spent years developing model notices for financial institutions that embody "succinct" and "streamlined" disclosures intended to promote comprehension and readability.⁴ Likewise, the Proposed Regulations best preserve consumer autonomy and choice by avoiding defaults or requirements that constrain or presuppose consumer intent.⁵

Further, the Proposed Regulations should align with principles of data minimization. As discussed in the ISOR, data minimization is an internationally recognized fair information practice principle.⁶ It should be a touchstone of the Proposed Regulations, which should avoid requirements that could result in businesses collecting or retaining more personal information than they otherwise would.

Second, the Proposed Regulations must operate within the parameters established by the legislature and California voters, reflecting the judgment captured in relevant statutory language

³ See § 7003(a); *see also* Initial Statement of Reasons ("ISOR"), § 7003.

⁴ See 74 Fed. Reg. 62890 (Dec. 1, 2009).

⁵ See Cal. Civ. Code § 1798.185(19).

⁶ See ISOR, § 7026.

as to the appropriate balance between privacy principles and other considerations. Longstanding principles of administrative law make clear that the Agency does not have the authority to amend the statute.⁷ The Agency plays a critical role in ensuring that any new requirements are consistent with both the plain language and statutory design of the CCPA.

Third, the Proposed Regulations should recognize the critical role of other federal and state privacy and consumer protection frameworks in augmenting the protections created under the CCPA. Banks and non-banks alike are subject to a broad suite of other state, federal and international privacy laws. The overall CCPA framework should complement these broader protections and avoid new requirements that do not align with other laws that apply to businesses. Indeed, the Agency’s interest in preserving a state framework in addition to any federal privacy standard that emerges would be best served by requirements that afford the flexibility required to achieve consistency and interoperability with other federal and state privacy laws.

This is particularly important for banks, which are subject to extensive regulatory requirements that provide a comprehensive framework to manage privacy and security risks. Even with respect to data that is not governed by the federal Gramm-Leach-Bliley Act (“GLBA”) or the Fair Credit Reporting Act (“FCRA”), BPI’s members are subject to a constellation of federal banking agency rules and guidance relating to data protection and information security, including with respect to risk management for service providers and other third parties and the management of risks relating to the integrity of data and use of models.⁸

III. Proposed Amendments

a. **Highly prescriptive contract requirements do not safeguard consumers and aspects may be inconsistent with statutory text.**

The Proposed Regulations call for businesses to implement specific contract terms in agreements with service providers and third parties to whom personal information is sold or shared beyond those terms contemplated by the statute. However, the statute already adopts detailed requirements for written contracts with service providers. Therefore, there should be a high bar before the Agency adopts new requirements, particularly where the new language further deviates from emerging U.S. and global privacy standards. In this case, the bar is not

⁷ See Cal. Gov’t Code § 11342.2 (2022) (“[A] state agency has authority to adopt regulations to implement, interpret, make specific or otherwise carry out the provisions of the statute, [but] no regulation adopted is valid or effective unless consistent and not in conflict with the statute and reasonably necessary to effectuate the purpose of the statute.”); see also *San Bernardino City Sch. Dist.*, 294 Cal. Rptr. 3d 348, 352 (Cal. Ct. App. 2022) (noting that a regulation is unenforceable if it “conflicts with the Legislature’s intent as manifested in the statute”).

⁸ See, e.g., Office of the Comptroller of the Currency (“OCC”) Bulletin 2021-55, Computer-Security Incident Notification (Nov. 23, 2021); OCC Bulletin 2013-29, Third-Party Relationships: Risk Management Guidance (Oct. 30, 2013); OCC Bulletin 2020-10, Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-19 (Mar. 4, 2020); OCC Bulletin 2011-12, Supervisory Guidance on Model Risk Management (Apr. 4, 2011); Federal Reserve Board, SR 11-7, Supervisory Guidance on Model Risk Management (Apr. 4, 2011).

satisfied, as the additional requirements will confer minimal incremental benefit to consumers while imposing a substantial burden on both businesses and their service providers.

For example, Subsection 7051(a)(2) of the Proposed Regulations states that service provider and contractor contracts must:

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 (emphasis added).

As an additional example, the Proposed Regulations require contract language specifying a five-day time period for a service provider or contractor to notify a business that it can no longer meet its obligations under the CCPA. These new terms do not have a clear consumer benefit where businesses have imposed contract terms that are consistent with the contract terms contemplated by the statute.⁹

Businesses often retain service providers to support activities that involve the processing of personal information that is subject to multiple privacy frameworks. However, the prohibition on using generic language deviates from, and therefore makes the CCPA framework less interoperable with, other federal, state, and international privacy laws. For example, the prohibition on using “generic terms” to define business purposes or services is not found in other similar privacy laws or even Article 28 of GDPR.¹⁰ Such a prohibition creates particular complexity for banks retaining service providers to support a bank’s activities that do not just involve the processing of personal information subject to the CCPA—but also involve the processing of nonpublic personal information subject to GLBA’s separate requirements for contractual agreements with service providers.¹¹ Banks are also subject to broader third-party risk management guidance issued by banking regulators.

Further, many businesses have already updated their contracts multiple times to adhere to the evolving requirements set out in the CCPA and its implementing regulations. Indeed, businesses have already been working to update contracts for the CPRA based on the statutory language, but the Proposed Regulations further move the goal posts by adding additional,

⁹ See, e.g., Cal Civ. Code § 1798.140(ag)(B), (C). Standard contract provisions requiring compliance with law and indemnification sufficiently incentivize parties to comply with the CCPA.

¹⁰ The Agency should seek to make its rules interoperable with and complementary to other U.S. state and federal privacy laws. As such, the GDPR framework is not necessarily the best reference point. Here, however, this absolute prohibition on generic language doesn’t even have a basis in GDPR. Even non-binding guidance from the European Data Protection Board (“EDPB”) affords businesses flexibility in the description of processing purposes and recognizes that the comprehensiveness of the description may vary based on the processing activity. See EDPB, Guidelines 08/2020 on the concepts of controller and processor in the GDPR, version 2.0 (July 7, 2021).

¹¹ See, e.g., 12 C.F.R. § 1016.13(a).

idiosyncratic contract language without a clear benefit to consumers or basis in the statute. Incorporating another series of more specific contract requirements could require yet another update and unreasonably limit contracting flexibility. It also distracts businesses from focusing on substantive CPRA requirements in favor of detailed technical requirements with no tangible consumer benefit.

In addition, the new contract terms contemplated in the Proposed Regulations may not serve consumers. With respect to the five-day notification, businesses are best situated to define the appropriate notification timeline on a case-by-case basis that takes account of the risks to the business. For example, a business may want immediate notification of an existing, material compliance issue but may want notification of an expected future compliance issue within a certain proximity to the issue. The prohibition on “generic” language seems potentially inconsistent with language elsewhere in the Proposed Regulations and in the underlying statute, which defines “business purposes” for which service providers may use personal information to include, *inter alia*, “[p]erforming services on behalf of the business[.]”¹² For these reasons, and as proposed in **Appendix A**, we recommend that these provisions be deleted altogether.

Further, the requirements for third parties should not be tantamount to those that the CCPA contemplates for service provider and contractor relationships. The Proposed Regulations should reflect the differences between third parties, on the one hand, and service providers and contractors, on the other hand, that are manifest in the statute. Indeed, the statutory design is clear that businesses operate independently from any third party to which personal information is sold or shared. Under the CCPA, consumers have rights to opt out of the sale and sharing of their personal information with third parties, and those third parties, in turn, are subject to their own obligations under the CCPA to provide consumers with transparency and consumer rights.

As a result, it does not make sense to impose the kind of downstream third-party contract protections—such as restrictions on use of data to “specific” purposes—in agreements with third parties that are appropriate for a service provider relationship. Here too, the Proposed Regulations should defer to the relevant statutory language without adding new requirements that are not consistent with the statutory design.

b. Prescriptive privacy notice requirements should be clarified to avoid creating consumer confusion and to ensure consistency with the statute.

In the interest of crafting more consumer-friendly experiences, the Proposed Regulations should permit businesses to tailor their approach to privacy notices within the parameters of the statute, rather than creating requirements that make developing succinct and streamlined notices more difficult. We support Proposed Regulation Subsection 7003(a), which sets forth a general principle that disclosures should be easy to read and understandable to consumers. However, certain other elements of the proposed requirements relating to privacy notices are overly prescriptive, inconsistent with the statute, or unclear. We discuss examples of each point and propose specific revisions in this section and **Appendix A**.

¹² See, e.g., Cal. Civ. Code § 1798.140(e)(5); Proposed Regulations § 7050(b)(1) (“to process or maintain personal information on behalf of the business”).

The goal of providing privacy notices that are both meaningful and transparent to consumers would be undermined if businesses were subject to overly detailed content and format obligations for such notices. Requirements imposed by the Proposed Regulations, however, go beyond the information required under current rules or other U.S. privacy frameworks. For example, Subsection 7011(e)(1)(J) requires “[i]dentification of the specific business or commercial purpose for disclosing the consumer’s personal information[.]” while Subsection 7012(e)(6) maintains that a business must include “the names of all the third parties . . . [or] information about the third parties’ business practices” in its privacy notice “[i]f a business allows third parties to control the collection of personal information[.]”¹³ Other provisions of the Proposed Regulations seem to contemplate cross-references to particular provisions of the Proposed Regulations.¹⁴

The Proposed Regulations similarly contemplate highly prescriptive expectations for linking to a privacy policy when a business relies on a privacy policy to provide notice at collection.¹⁵ Such a requirement potentially limits the flexibility that businesses have to link to a privacy policy that contains information in different sections, even where that is the clearest presentation for consumers. It also creates significant confusion for non-California consumers. We recommend generalizing the requirements to permit businesses greater latitude to communicate effectively with consumers, both Californians and non-Californians alike.

The level of specificity dictated in the Proposed Regulations risks confusing and overloading consumers, rather than promoting transparency. This is particularly true for customers of financial institutions, as financial institutions must already provide multiple privacy notices to different categories of customers under federal privacy rules. The Proposed Regulations would prevent financial institutions from structuring notices to optimize transparency and clarity for these consumers.

c. Opt-out preference signal requirements do not include needed technical specifications and are inconsistent with the statute.

The requirements relating to opt-out preference signals should be consistent with the statutory design, which affords businesses flexibility as to whether to honor such signals or post a link on their home page.¹⁶ In any event, to the extent some businesses honor opt-out preference signals, the Proposed Regulations should be clear and consistent in terms of the relevant requirements. For example, the Proposed Regulations should be clear that the obligations to

¹³ Compare with Cal. Civ. Code § 1798.130(a)(5)(B)(iii), (iv) (requiring disclosure of “the business or commercial purpose for collecting or selling or sharing consumers’ personal information” and “the categories of third parties to whom the business discloses consumers’ personal information”).

¹⁴ See Subsection 7011(e)(1).

¹⁵ Proposed Regulations § 7012(f) (providing that it is not adequate to direct a consumer to “another section of the privacy policy . . . so that the consumer is required to scroll through other information”).

¹⁶ Cal. Civ. Code § 1798.135(a)–(b).

provide two or more designated methods for submitting requests to opt-out of sale/sharing¹⁷ do not apply where a business processes an opt-out preference signal in a frictionless manner. This would ensure consistency with the provisions explaining that processing an opt-out preference signal in a frictionless manner obviates the requirement to post a link.¹⁸ It also would better incentivize businesses to adopt opt-out preference signals.

Furthermore, the Proposed Regulations should include adequate technical specifications to afford businesses the guidance necessary to implement the opt-out preference signal. Implementing this solution will be a complex, and in some instances, multi-year effort. Promptly issuing technical specifications would make this development process more efficient and reduce the need for costly re-architectures in the future.

For this purpose, the CPRA charged the CPPA with “[i]ssuing regulations to define the requirements and technical specifications for an opt-out preference signal sent by a platform, technology, or mechanism[.]”¹⁹ The Proposed Regulations, however, do not include adequate detail, which is critical to the successful implementation of the signal—particularly at a platform level. At a minimum, the Proposed Regulations should fully address all the categories of technical specifications that are specifically contemplated under Cal. Civ. Code § 1798.185(a)(19), including specifications to ensure that signals clearly represent a consumer’s intent and be free of defaults constraining or presupposing such intent,²⁰ and to enable consumers to selectively consent to one business’s processing of their personal information without affecting their preferences for other business.²¹ This important language in Cal. Civ. Code Subsection 1798.185(a)(19) serves consumer autonomy.

The technical requirements for opt-out preference signals should be consistent with principles of consumer autonomy and recognize limitations in current technology. For example, notwithstanding language in Cal. Civ. Code § 1798.185(a)(19), Subsection 7025(c)(5) prohibits a business from interpreting the absence of an opt-out preference signal as consent to opt-in to the sale or sharing of personal information. If current technologies do not provide a separate opt-in option, then businesses *should* be able to interpret the absence of an opt-out preference signal as consent to opt-in.

In addition, the technical specifications also should address that universal opt-out preference signals must have sufficient scale to effectively communicate a consumer’s opt-out preference signals across a large universe of websites, online platforms, and mobile applications. At this time, there is no universal opt-out preference signal capable of effectively communicating a consumer’s opt-out preferences across websites, online platforms, and mobile applications.

¹⁷ Proposed Regulations § 7026(a).

¹⁸ *Id.* § 7025(e).

¹⁹ Cal. Civ. Code § 1798.185(a)(19)(A).

²⁰ *Id.* § 1798.185(a)(19)(A)(iii).

²¹ *Id.* § 1798.185(a)(19)(A)(v).

Finally, we note that Subsections 7026(f)(2) and (f)(3) require a business to notify certain third parties to whom the business has sold, shared, or made available a consumer's personal information of a consumer's request to opt-out of sale/sharing and to forward the consumer's opt-out request to "any other person with whom the person has disclosed or shared the personal information[.]" Both requirements go beyond the requirements of the statute and would be technically challenging, if not impossible, at the device level. The requirement to forward a consumer's request to any person with whom the person has disclosed or shared the information does not account for lawful disclosures to service providers, contractors, law enforcement, government agencies, or disclosures to other businesses or individuals pursuant to an explicit request or direction from the consumers to make the disclosure. We have included specific suggestions on language in **Appendix A**.

d. The Proposed Regulations should not impose new requirements to obtain "explicit consent" in ways that are inconsistent with the statutory design.

Language in the Proposed Regulations Subsection 7002(a) contemplates that a business should obtain "explicit consent" before processing personal information "for any purpose that is unrelated or incompatible with the purpose(s) for which the personal information [was] collected or processed." Such a provision would be inconsistent with the statutory design of the CCPA framework, which creates a number of *opt-out* rights for consumers. It also would be inconsistent with the plain language of Cal. Civ. Code Subsection 1798.100(a)(1), under which businesses must provide a consumer with *additional notice*—not obtain explicit consent—to use personal information in ways that are incompatible with the disclosed purposes for which personal information was collected initially.

To the extent that the Proposed Regulations provide examples of implementing Cal. Civ. Code Subsection 1798.100(c), they should focus on the data minimization principle—that is, to provide guidance about what it means to process personal information in a manner that is "necessary and proportionate" to disclosed processing purposes.

e. The Proposed Regulations should not disrupt the balance struck by the CCPA and CPRA between various privacy principles.

The CCPA and CPRA created clear exemptions reflecting a carefully negotiated balance between the statutory objectives and other important privacy principles, such as data minimization, understandability for consumers, and consumer choice. Key exceptions include, for example, prohibiting the re-identification or linking of consumers' personal information and clarifying that data regulated by sector-specific laws is not within the scope of the statute.²² These exceptions are critical to helping consumers understand their rights and protections under the CCPA and CPRA.

Certain provisions in the Proposed Regulations, however, muddy these principles by failing to reflect the clear and plain language of the statute. For example, Subsection 7025(c)(1) requires a business, upon receipt of an opt-out preference signal, to "treat the [signal] as a valid

²² See, e.g., Cal Civ. Code §§ 1798.145(e), (j).

request to opt-out of sale/sharing . . . for that browser or device, and, if known, for the consumer.” However, businesses typically do not maintain pseudonymous browser data with a customer’s account or other identifiable data. As another example, the definition of “disproportionate effort” suggests that businesses might otherwise have obligations to respond to a consumer request with respect to personal information that is “not [maintained] in a searchable or readily-accessible format[.]”²³

Consistent with the plain language of the statute and principles of data minimization, the rules should be clarified to avoid implying that businesses must (i) re-identify or link information that, in the ordinary course of business, is not maintained in a manner that would be considered personal information; (ii) maintain information in identifiable, linkable, or associable form; or (iii) collect, obtain, retain, or access any data or technology in order to be capable of linking or associating a verifiable consumer request with personal information. We have proposed specific language for such a clarification in **Appendix A**. Not only does such a clarification conform to the plain language of the statute, but it helps preserve the goals of data minimization that were preserved with nuanced statutory language.

These clarifications are more important in these Proposed Regulations than in past iterations of the statute and regulations, in light of new requirements established under Subsection 7025(a). The revisions would also enhance consumer privacy by encouraging businesses to maintain information in non-identifiable or non-linkable form in the ordinary course of business. For financial institutions, in particular, any requirement to link pseudonymous browsing data with a known customer or applicant could have the unintended effect of making more information subject to the GLBA and therefore exempt from the CCPA.

f. Obligations to address requests to know or for deletion and correction should permit businesses more flexibility to address data security risks.

Responding to consumer requests creates security challenges for all businesses, who must balance consumer rights with anti-fraud and security concerns—which, inherently, are in the interest of all consumers. Certain elements of the approach outlined in the Proposed Regulations exacerbate security risks, which is a particular problem for banks, who are frequent targets for fraud and other malicious activities due to the nature of their business. The consequences of such actions against banks, when successful, can be more severe than for other industries. We therefore propose amendments to these provisions to re-establish the balance between consumer rights and security, detailed in **Appendix A**.

For example, requirements relating to the right to know do not incorporate sufficient safeguards for consumer data. Specifically, businesses need latitude to withhold disclosure of “specific pieces of information” to consumers in consideration of security concerns. The Proposed Regulations should reinstate language clarifying that businesses should not provide consumers with specific pieces of personal information if the disclosure creates a substantial,

²³ See Proposed Regulations § 7001(h).

articulable and unreasonable risk to the customer or business's security.²⁴ If such information were to be compromised, malicious actors could use it to facilitate future fraudulent activity (e.g., spear phishing campaigns). Financial institutions are experienced actors in detecting and preventing such activities.

Also, with regard to data security, Subsections 7001(c) and 7063(b) of the Proposed Regulations would loosen safeguards pertaining to requests from authorized agents, providing more opportunities for malicious actors to engage in fraudulent activity. We recommend reinstating the requirements that authorized agents be registered California business entities and permitting businesses to require a power of attorney to use an authorized agent, as this may be necessary for consumer or business security in certain instances. We also recommend striking language that suggests that authorized agents may submit an opt-out preference signal without written permission from the consumer. It would not be consistent with the goals of consumer autonomy and control to require businesses to respond to requests from potentially rogue agents—whether they are malicious actors or just interested in interfering with businesses trying to comply with the requirements.

g. The Proposed Regulations do not permit needed flexibility for businesses to respond to consumer rights requests.

Aspects of the Proposed Regulations implement overly prescriptive requirements for handling data subject requests, risk confusing customers, and are not necessary to protect consumer interests. For example, Subsection 7022(f) states that where a business denies a customer's request to delete, it must "[p]rovide to the consumer a detailed explanation of the basis for the denial[.]" Even for personal information that is not subject to GLBA, heavily regulated entities, such as banks, have sophisticated mechanisms in place to support the integrity of their data—e.g., requirements to maintain information on historical account opening, historical transactions, and up-to-date credential and notification information. As a consequence of these existing requirements, the basis for denying a request to correct or delete information could result from a combination of factors, including regulatory and legal requirements, business needs, and fraud prevention purposes. Providing a detailed explanation for the basis of the denial in these circumstances would result in minimal corresponding benefit to consumers, while potentially confusing consumers about their rights under different legal frameworks.

Relatedly, Subsection 7023(f) requires a business denying a consumer's request to correct to, upon the consumer's request, "note both internally and to any person with whom it discloses, shares, or sells the personal information that the accuracy of the personal information is contested by the consumer." It is unclear what benefit would result from informing external parties that certain information is contested where the business has already arbitrated and denied the claim, and thus, where external parties would not take any further action.

²⁴ "A business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks." §999.313(c)(3).

We recognize that it would be challenging for the CPPA to promulgate separate rules tailored to each regulated industry. Instead, we urge the Agency to exempt entities already subject to quality and integrity requirements from these and related provisions. We have included specific suggestions on language in **Appendix A**.

h. Consumer rights are enforced most effectively directly by consumers.

The Proposed Regulations make businesses responsible for notifying third parties of consumer rights requests, even where the business is not the source of the relevant information. This allocation of responsibility is inefficient, and customers would be better served if they were directed to submit the relevant request at the information source.

For example, Subsection 7023(c) pertaining to correction rights requires that, “[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*.” At the same time, Subsection 7023(i) provides that “[w]here the business is not the source of the information that the consumer contends is inaccurate, in addition to processing the consumer’s request, the business shall provide the consumer with the name of the source from which the business received the alleged inaccurate information.”

We recommend revising these provisions to clarify that the source of the inaccurate information is primarily responsible for ensuring that personal information is corrected at the source and remains corrected when transmitted to other parties. This could include, for example, amending Subsection 7023(i) to create optionality for businesses in responding to requests to correct.

We also recommend deleting Subsection 7022(b)(3), which requires businesses in receipt of a deletion request to 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” The statute affords consumers granular rights to exercise deletion requests of Business A, but not Business B, and vice versa. The Proposed Regulations should not presuppose consumer intent, but rather continue to allow consumers to exercise these choices more granularly with regard to individual businesses.

We have included specific suggestions on language in **Appendix A**. In the alternative, we recommend that entities regulated by broad compliance frameworks, including banks, be permitted greater flexibility in responding to customer rights requests to account for security concerns.

i. Employee and business customer data is distinct from general consumer data, making the application of new restrictions unclear and complex to implement.

Employee and commercial data (the latter referred to herein as “B2B” data) is fundamentally different from consumer data that is processed outside the context of an employment or commercial relationship, particularly as the CCPA is at its core a consumer

protection statute. While there may be limitations on the Agency’s authority to effectively amend the statute, it is well within the Agency’s discretion to issue rules that further the purposes of the statute, which specifically observes that protections for employees and independent contractors should “tak[e] into account the differences in the relationship between employees or independent contractors and businesses, as compared to the relationship between consumers and businesses.”²⁵

Consistent with this statutory language, general consumer data protection rules should not be applied to employee and B2B contexts without careful consideration of their impact and analysis with other commercial legal frameworks and employment laws. The Agency has not yet done that affirmatively. Indeed, the examples and detail provided throughout the Proposed Regulations exclusively focus on consumer data rather than the employment and commercial contexts. For example, Subsection 7027(l) lists “[t]he purposes for which a business may use or disclose sensitive personal information without being required to offer consumers a right to limit[.]” However, none of the seven examples seem to contemplate processing activities that would be relevant for employee or B2B data.

Accordingly, we recommend that the CPPA clarify that the Proposed Regulations do not apply in employment or B2B contexts until there is a separate rulemaking. The compressed timeline for implementing the Proposed Regulations will be particularly infeasible for B2B and employment data.

j. The dates the Proposed Regulations become effective and enforceable should be extended to correspond to the statutory design.

BPI is committed to supporting the Agency’s efforts to expeditiously adopt implementing rules for the protection of consumer data that are pragmatic and consistent with the statute. However, that process takes time and the Agency has already announced that the rules will be finalized well after the July 1, 2022 date required by the statutory schedule. Indeed, the initial comment period was not open by that date.

In light of this delay, we encourage the Agency to extend the effective date of any implementing rules. Extending the date by twelve (12) months—at the earliest, January 1, 2024—would be consistent with the statutory design, which clearly contemplated that businesses should have a year to implement requirements of the law and regulations before enforcement of such rules would begin—and that is particularly important where the final rules create new substantive obligations (e.g., in the employment and B2B contexts).²⁶

In the alternative, we recommend extending the effective date of any implementing rules to at least July 1, 2023, which would align with the statutory date for administrative enforcement. The Agency cannot enforce the new requirements in advance of July 1, 2023 in any event, and this would afford businesses that take seriously their legal compliance obligations with at least some lead time before the rules are finalized to adopt appropriate controls. The Proposed

²⁵ CPRA, § 3.

²⁶ Cal. Civ. Code § 1798.185(d).

Regulations go well beyond implementing the statute. If the Agency is going to create ambitious new privacy protections, then it should ensure that the rulemaking process is transparent, open-minded, and methodical,²⁷ and the Agency must also provide businesses with fair and reasonable notice to come into compliance with the new obligations.

As noted above, **Appendix A** includes proposed amendments to address the above concerns. In addition, **Appendix A** sets out some initial clarifying edits that are important for the Agency to consider.

The Bank Policy Institute appreciates the opportunity to submit comments on the CPPA's proposed regulations implementing the CPRA. If you have any questions, please contact the undersigned by phone at [REDACTED] or by email at [REDACTED]

Respectfully submitted,

[REDACTED]

Angelena Bradfield
Senior Vice President
AML/BSA, Sanctions & Privacy
Bank Policy Institute

²⁷ Likewise, the economic analysis that the Agency performs as part of its rulemaking process should reflect the magnitude of investment that businesses are and will continue to make to comply with the CPRA, including analysis of the level of investment that multinational companies undertook to comply with GDPR and, in 2020, the CCPA. Further, to the extent the Agency retains the most prescriptive elements of the Proposed Regulations, it should consider the economic impact that will result if businesses operate separate online services and customer interfaces with California residents to avoid confusing non-Californians.

IV. Appendix A

Gray rows provide detail on points made in Part III. White rows include additional examples and/or points not addressed in Part III.

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
Section III.a – Contract Requirements		
Proposed Regulations §§ 7051, 7053 Cal. Civ. Code §§ 1798.100(d), 1798.140(e)(5), (j), (ag)	Service provider and third party contract requirements have been sufficiently defined in the statutory text and previous regulations. The proposed requirements do not serve to align the CCPA's contract requirements more closely with other statutory frameworks, such as the GDPR, but instead impose stricter requirements on third party contracting. Accordingly, additional prescriptive requirements should be deleted.	<i>Delete contract requirements in Proposed Regulations Subsections 7051 and 7053.</i>
Proposed Regulations §§ 7050(b)(2), 7051(a), 7053(a) Cal. Civ. Code § 1798.140(e)(5)	The prohibition against describing business purposes “in generic terms” is inconsistent with the statute and other sections of the Proposed Regulations.	<i>In the alternative to deleting § 7051 altogether, amend § 7051: “The contract required by the CCPA for service providers and contractors shall . . . 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.”</i> <i>Apply corresponding edits to similar language in Subsection 7053(a).</i>

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
<p>Proposed Regulations § 7051(a)(8)</p> <p>Cal. Civ. Code § 1798.100(d)(4)</p>	<p>The requirement that service providers and contractors notify the business within five days after determining that it cannot fulfill its CCPA obligations deviates from the statute and is overly prescriptive. Businesses are best situated to define the appropriate notification timeline on a case-by-case basis, based on the nature of the information and parties' relationship. Furthermore, standard contract provisions (e.g., those requiring compliance with applicable law) sufficiently incentivize parties to comply with the CCPA / CPRA.</p>	<p><i>In the alternative to deleting § 7051 altogether, amend § 7051(a)(8):</i></p> <p>“Require the service provider or contractor to notify the business no later than five business days <u>within a reasonable time frame specified by the business</u> after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.”</p>
Section III.b – Privacy Notices		
<p>Proposed Regulations § 7011(b)</p> <p>Cal. Civ. Code § 1798.130(5)(B)(iii)</p>	<p>Prescriptive requirements pertaining to the form and content of privacy notices exceed the statutory text and risk confusing consumers. The Proposed Regulations should include an alternative provision clarifying that businesses may forego the prescriptive requirements where they demonstrate a more consumer-friendly and privacy-protective approach.</p>	<p><i>Amend § 7011(b):</i> “The privacy policy shall comply with section 7003, subsections (a) and (b), <u>including as to the interpretation and implementation of the requirements of this section 7011.</u>”</p> <p><i>Conforming edits should be made to §§7012(b), 7013(b), 7014(b), & 7016(b).</i></p>
<p>Proposed Regulations § 7012(e)(6); <i>see also</i> § 7012(g)(2)</p> <p>Cal. Civ. Code § 1798.130(5)(B)(iv)</p>	<p>Prescriptive requirements pertaining to the form and content of privacy notices exceed the statutory text and risk confusing consumers.</p>	<p><i>Amend § 7012(e)(6):</i> “If a business allows third parties to control the collection of personal information, the names <u>categories</u> of all the third parties; or, in the alternative, <u>general</u> information about the third parties' business practices.”</p>
<p>Proposed Regulations § 7011(e)(3)(J)</p> <p>Cal. Civ. Code § 1798.130(a)(1)</p>	<p>Designating particular contact methods in privacy notices inhibits businesses from adopting the simplest and most efficient means for addressing consumers' questions and requests. Many</p>	<p><i>Amend § 7011(e)(3)(J):</i> “A contact for questions or concerns about the business's privacy policies and practices using a method reflecting the manner in which the <u>which</u> take account the manner in which</p>

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
	financial institutions use a combination of in-person, telephone, and online means to interact with customers, making the identification of a primary method of interaction difficult.	<u>the</u> business primarily interacts with the consumers.”
<p>Proposed Regulations § 7012(f)</p> <p>Cal. Civ. Code § 1798.100(a)(1)</p>	<p>The requirement that notice at collection must direct the consumer to a specific section of the privacy policy will complicate business’s efforts to provide transparent disclosures to consumers, particularly where a business is subject to additional privacy frameworks. This approach limits business’s ability to prioritize providing consumers easy-to-find information that is most relevant to them in light of the constellation of required privacy notices and disclosures.</p>	<p><i>Amend § 7012(f):</i> “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.”</p>
<p>Proposed Regulations §§ 7010(b); <i>see</i> 7012(a)</p> <p>Cal. Civ. Code § 1798.100</p>	<p>In explaining obligations to provide notice at collection, the Proposed Regulations remove the reference to collecting personal information “from a consumer,” suggesting that the online notice must cover personal information obtained from third parties as well as directly from consumers. The existing regulations’ language should be restored to ensure consistency with Subsection 7012(a) (“...to be collected from <i>them</i>” (emphasis added)).</p>	<p><i>Amend § 7010(b):</i> “A business that controls the collection of a consumer’s personal information <u>from a consumer</u> shall provide a notice at collection in accordance with the CCPA and section 7012.”</p>
<p><i>Section III.c – Opt-Out Preference Signal & Statutory Consistency</i></p>		

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
<p>Proposed Regulations §§ 7025, 7026</p> <p>Cal. Civ. Code §§ 1798.135(b), 1798.185(a)(19)–(20)</p>	<p>The statutory design plainly contemplates that it should be optional, not mandatory, for businesses to honor global opt-out preference signals.</p>	<p><i>Amend language in the Proposed Regulations implying that processing the opt-out preference signal is mandatory, including in §§ 7025(b), (c)(1),(3)–(4), 7026(a), etc.</i></p>
<p>Proposed Regulations §§ 7025(b), (c)(5)</p> <p>Cal. Civ. Code §§ 1798.135(b), 1798.185(a)(19)–(20)</p>	<p>According to requirements set out in the CPRA, the Agency should provide technical specifications for the opt-out preference signal, particularly at the platform level.</p> <p>For example, designing a useable opt-out preference signal that most accurately reflects consumers' preferences with regard to the use of their data requires symmetry and sufficient granularity of choice. The Proposed Regulations should attempt to capture consumers' choices as accurately as possible, rather than skewing their selections towards opt-out. Taking into account the requirements built into Subsection 7025(b), businesses should be able to rely on the absence of a signal to determine that a consumer has consented to the sharing of their personal information.</p>	<p><i>Include technical specifications for opt-out preference signals under §§ 7025 and 7026.</i></p> <p><i>For example, amend § 7025(b):</i></p> <p><i>“<u>To the extent that a business processes</u> A business shall process <u>any</u> opt-out preference signals, <u>those signals</u> that meets the following requirements <u>shall be considered valid as a valid</u> requests to opt-out of sale/sharing:</i></p> <ol style="list-style-type: none"> <i>(1) The signal shall be in a format commonly used and recognized by businesses <u>websites, online platforms, and mobile applications</u>. An example would be an HTTP header field.</i> <i>(2) <u>The signal shall be widely recognized by websites, online platforms, and mobile applications.</u></i> <i>(3) The platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer, whether in its configuration or in disclosures to the public, that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information. The configuration or disclosure</i>

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
		<p>does not need to be tailored only to California or to refer to California.</p> <p>(4) <u>The platform, technology, or mechanism that sends the opt-out preference signal shall provide symmetry of choice, clearly represent a consumer's intent, and be free of defaults constraining or presupposing that intent.</u></p> <p>(5) <u>The platform, technology, or mechanism that sends the opt-out preference signal shall provide a mechanism for the consumer to selectively consent to a business' sale of the consumer's personal information, or the use or disclosure of the consumer's without affecting the consumer's preferences with respect to other businesses or disabling the opt-out preference signal globally."</u></p> <p><i>Amend § 7025(c)(5): "When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b) . . . 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."</i></p>

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
<p>Proposed Regulations §§ 7025(e), 7026(a)</p> <p>Cal. Civ. Code §§ 1798.135(a)–(b), 1798.185(a)(19), (20)</p>	<p>The Agency should reconcile more stringent requirements for processing opt-out preferences under the Proposed Regulations with the alternative processes established under the CPRA. It should also clarify that posting links is not required where a business uses a frictionless opt-out preference signal applicable to the full scope of shared data.</p>	<p><i>Amend 7025(e):</i> “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 the alternative 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 the alternative opt-out link.</p> <p>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.”</p> <p><i>Amend § 7026(a):</i> “A business that sells or shares personal information shall provide two or more designated methods for submitting requests to opt-out of sale/sharing, <u>unless the business honors the opt-out-preference signal in a frictionless manner for all relevant shared data.</u> A business that</p>

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
		collects personal information from consumers online shall at a minimum , allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal <u>in a frictionless manner in accordance with subsections (f) and (g) of section 7025 of this regulation</u> and/or 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.”
Section III.d – Explicit Consent		
<p>Proposed Regulations § 7002(a)</p> <p>Cal. Civ. Code § 1798.100(a)(1)</p>	<p>Requirements under the Proposed Regulations suggesting that explicit consent is required in circumstances that are not compatible with an average consumer’s expectations are inconsistent with the statute. The statute requires the provision of notice prior to collecting new categories of personal information or using collected data for new purposes not initially disclosed. Further, the notion of explicit consent is at odds with the overall statutory design, which contemplates that consumers will be provided notice and choice with regard to a business’s processing activities.</p>	<p><i>Amend § 7002(a):</i> “A business’s collection, use, retention, and/or sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve the purpose(s) for which the personal information was collected or processed. To be reasonably necessary and proportionate, the business’s collection, use, retention, and/or sharing must be consistent with what an average consumer would expect when the personal information was collected. A business’s collection, use, retention, and/or sharing of a consumer’s personal information may also be for other disclosed purpose(s) if they are compatible with what is reasonably expected by the average consumer. A business shall obtain the consumer’s explicit consent in accordance with section 7004 <u>provide additional notice to the consumer</u> before collecting, using, retaining, and/or sharing the consumer’s personal information</p>

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
		for any purpose that is unrelated or incompatible with the purpose(s) for which the personal information collected or processed.”
<i>Section III.e – Balance of Privacy Principles</i>		
<p>Proposed Regulations § 7025(c)(1)</p> <p>Cal. Civ. Code § 1798.145(j)</p>	<p>Opt-out preference signal requirements in the Proposed Regulations should avoid the implication that a business must re-identify or link data not otherwise maintained in that state to comply with the signal.</p>	<p><i>Amend § 7025(c)(1):</i> “When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b): . . . The business shall treat the opt-out preference signal as a valid request to opt-out of sale/sharing submitted pursuant to Civil Code section 1798.120 for that browser or device, and, if known, for the consumer.”</p>
<p>Proposed Regulations §§ 7001(h), 7022(b)(3) (<i>and similar provisions</i>)</p> <p>Cal. Civ. Code § 1798.145(j)</p>	<p>The Proposed Regulations should clarify that its requirements never necessitate re-identifying or linking data with a customer where it is not already maintained in that format. We recommend clarifying this approach across the Proposed Regulations by adding a new § 7000(c).</p>	<p><i>Add a new § 7000(c):</i> “<u>(c) No provision of these regulations (1) shall require a business to maintain information in identifiable, linkable, or associable form, or collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating the consumer's request with personal information or (2) otherwise be construed to regulate any activity or data or impose any obligations in a manner that is inconsistent with the CCPA.</u>”</p>
<p>Proposed Regulations §§ 7026(f)(4) and 7027(g)(5)</p> <p>Cal. Civ. Code §§ 1798.120, 1798.121</p>	<p>The Proposed Regulations contemplate that businesses have obligations to provide consumers with the means to confirm that their request to opt-out of sale/sharing and/or a request to limit has been processed. Maintaining this information for noncustomers is contrary to principles of data minimization, and thus, it should be sufficient that the business responds</p>	<p><i>Delete § 7026(f)(4):</i> “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.”</p>

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
	affirmatively to the consumer's request.	<i>Delete § 7027(g)(5): “Providing a means by which the consumer can confirm that their request to limit has been processed by the business. For example, the business may display through a toggle or radio button that the consumer has limited the business’s use and sale of their sensitive personal information.”</i>
Sections III.f – Data Security		
<p>Proposed Regulations § 7024(c)</p> <p>Cal. Civ. Code §§ 1798.110, 1798.145</p>	<p>The Proposed Regulations should make clear that specific pieces of information need not be provided in response to a request to know where the disclosure would create a security risk for customers or the business, consistent with a previous draft of the AG regulations. §999.313(c)(3).</p>	<p><i>Amend § 7024(c): “<u>A business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer’s account with the business, or the security of the business’s systems or networks. Neither shall the business provide such information if the consumer’s request is intended to or has the effect of circumventing rules of discovery pertaining to an ongoing litigation.</u> In responding to a request to know, a business is not required to search for . . .”</i></p>
<p>Proposed Regulations § 7001(c), 7063(b)</p> <p>Cal. Civ. Code §§ 1798.130(a)(3), 1798.185(a)(7)</p>	<p>The Proposed Regulations should permit businesses to impose more stringent security safeguards on requests from authorized agents in the interest of consumer and business security.</p>	<p><i>Amend § 7001(c): “‘Authorized agent’ means a natural person or a business entity <u>registered with the Secretary of State to conduct business in California</u> that a consumer has authorized to act on their behalf subject to the requirements set forth in section 7063.”</i></p> <p><i>Amend 7063(b): “Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to</i></p>

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
		Probate Code sections 4121 to 4130. A business shall not require a power of attorney in order for a consumer to use an authorized agent to act on their behalf.”
Proposed Regulations § 7026(i)	The Proposed Regulations should strike language suggesting that authorized agents may submit an opt-out preference signal without written permission from the consumer. It would not be consistent with the goals of consumer autonomy and control to require businesses to respond to requests from potentially rogue agents—whether they are malicious actors or just interested in interfering with businesses trying to comply with the requirements.	<i>Amend § 7026(i):</i> “A consumer may use an authorized agent to submit a request to opt-out of sale/sharing on the consumer’s behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer’s signed permission demonstrating that they have been authorized by the consumer to act on the consumer’s behalf. The requirement to obtain and provide written permission from the consumer does not apply to requests made by an opt-out preference signal.”
<i>Section III.g – Rights to Correct and Delete</i>		
Proposed Regulation §§ 7022(f), 7023(f)	Entities regulated under other legal privacy frameworks should be exempt from certain prescriptive requirements relating to the rights to correction and deletion.	<i>Amend § 7022(f):</i> “In cases where a business denies a consumer’s request to delete in whole or in part, the business shall . . . 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[.] <u>This requirement shall not apply to businesses that are subject to federal laws or regulations governing the quality and integrity of personal information maintained by the business.”</u>

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
		<p><i>Amend § 7023(f):</i> “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 . . . Inform the consumer that, upon the consumer’s request, it will note both internally and to any person with whom it discloses, shares, or sells the personal information that the accuracy of the personal information is contested by the consumer. The business does not have to provide this option for requests that are fraudulent or abusive. <u>This requirement shall not apply to businesses that are subject to federal laws or regulations governing the quality and integrity of personal information maintained by the business.</u>”</p>
<p>Proposed Regulations § 7023(b)</p> <p>Cal. Civ. Code § 1798.106</p>	<p>The “totality of the circumstances” standard proposed for arbitrating requests to correct is ambiguous. In those same circumstances where businesses do not have obligations to delete data, it should be clear that businesses do not have obligations to correct data.</p>	<p><i>Amend § 7023(b):</i> “In determining the accuracy of the personal information that is the subject of a consumer’s request to correct, the business shall consider the totality of the circumstances relating to the contested personal information. A business may deny a consumer’s request to correct if <u>it is reasonably necessary to maintain the consumer’s personal information without correction for any of the activities set forth in Cal. Civ. Code § 1798.105(d) or the business</u> it determines that the contested personal information is more likely than not accurate based on the totality of the circumstances.</p>

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
		<p>(1) Considering the totality of the circumstances includes, but is not limited to, considering:</p> <p>(A) The nature of the personal information (e.g., whether it is objective, subjective, unstructured, sensitive, etc.).</p> <p>(B) How the business obtained the contested information.</p> <p>(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).</p> <p>(2) If the business is not the source of the personal information and has no documentation to support of the accuracy of the information, the consumer's assertion of inaccuracy may be sufficient to establish that the personal information is inaccurate.</p> <p><u>(3) In no event shall the business be held liable under this title for its decision as to the accuracy of the personal information under section 7023(b) unless the business is shown to have acted in bad faith in applying the totality of the circumstances standard or failed to apply the standard."</u></p>
<p>Proposed Regulations § 7023(d)</p> <p>Cal. Civ. Code § 1798.106</p>	<p>Documentation provisions associated with requests to correct hinder businesses from implementing more efficient and less resource-intensive processes for arbitrating consumer requests. Additionally, consumer interests would be better served by requiring more documentation for high impact issues, not less. These issues have the potential to carry the</p>	<p><i>Amend § 7023(d)(1):</i> "A business shall accept, review, and consider any documentation that the consumer provides in connection with their right to correct whether provided voluntarily or as required by the business, <u>unless the business has reason to believe that the documentation provided is irrelevant, excessive, or fraudulent.</u> <u>If the business does not review</u></p>

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
	heaviest consequences for consumers and should be subject to a more stringent assessment.	<p><u>documentation submitted by a customer, it must document its reasoning.</u></p> <p><i>Amend § 7023(d)(2)(D):</i> “A business may require the consumer to provide documentation if necessary to rebut its own documentation that the personal information is accurate. In determining the necessity of the documentation requested, the business shall consider the following: . . . The impact on the consumer. For example, if the personal information has a high impact on the consumer, the business may require less <u>more</u> documentation.”</p>
<p>Proposed Regulations § 7023(j)</p> <p>Cal. Civ. Code § 1798.130(b)</p>	<p>Consistent with the plain language of the statute, consumers should not be permitted more than two opportunities to make requests to know per year. Subsection 7023(j) effectively operates as a right to know, and thus arguably contradicts the statutory text, which limits a consumer to two disclosure requests per year.</p>	<p><i>Amend § 7023(j):</i> “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).”</p>
<p>Proposed Regulations § 7022(b)(1), (d)</p> <p>Cal. Civ. Code § 1798.105</p>	<p>With regard to requests to delete, business’s obligations for archived and back-up systems are ambiguous. The Proposed Regulations state that these systems are exempt from deletion requests, but also allow compliance with a deletion request affecting them to</p>	<p><i>§ 7022(b)(1) for reference:</i> “A business shall comply with a consumer’s request to delete their personal information by . . . [p]ermanently and completely erasing the personal information from its existing systems except archived or back-up systems,</p>

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
	be “delayed” in certain circumstances.	<p>deidentifying the personal information, or aggregating the consumer information[.]”</p> <p><i>Amend § 7022(d):</i> “If a business, service provider, or contractor stores any personal information on archived or backup systems, it may delay compliance with the consumer’s request to delete <u>is not required for those systems, with respect to data stored on the archived or backup system, unless</u> and until the archived or backup system relating to that data is restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose. <u>For the purposes of this provision, ‘access’ does not include de minimis or transient access for the purposes of maintenance, information security, fraud prevention, or system improvement.</u>”</p>
Section III.h – Allocation of Responsibility with Service Providers, Contractors, and Third Parties		
<p>Proposed Regulations §§ 7023(c), (c)(1), (i)</p> <p>Cal. Civ. Code § 1798.106</p>	<p>In response to requests to correct, the Proposed Regulations should clarify that the responsibility for correcting inaccurate information rests with the third party source of the information, rather than the business by default. This approach places responsibility for the correction with the entity most able to remedy the problem.</p>	<p><i>Amend § 7023(i):</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 <u>either</u> provide the consumer with the name of the source from which the business received the alleged inaccurate information <u>or communicate the consumer’s request to the source to make the necessary corrections in its systems.</u>”</p> <p><i>Amend § 7023(c):</i> “A business that complies with a consumer’s request</p>

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
		<p>to correct shall correct the personal information at issue on its existing systems and <u>where the business is not the source of the information that the consumer contends is inaccurate, then implement measures to help the consumer</u> ensure that the information remains corrected <u>by complying with subsection 7023(i).</u> 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.”</p> <p><i>Amend § 7023(c)(1):</i> “Business L maintains personal information about consumers that it receives from data brokers on a regular basis. Business L generally refreshes the personal information it maintains about consumers whenever it receives an update from a data broker. Business L receives a request to correct from a consumer and determines that the information is inaccurate. To comply with the consumer’s request, Business L corrects the inaccurate information in its system and ensures that the corrected personal information is not overridden by inaccurate personal information subsequently received from the data broker <u>informs the consumer of the data broker from which the business received the alleged inaccurate information or informs the data broker of the consumer’s request and instructs the data broker to make the</u></p>

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
		<u>necessary corrections in its respective systems.”</u>
Proposed Regulations § 7022(b)	The Proposed Regulations should provide greater flexibility for businesses to address deletion requests where information shared with or sold to third parties is implicated to improve efficiency for consumers and reduce the administrative burden on businesses.	<i>Delete Proposed Regulation § 7022(b)(3).</i>
Proposed Regulations §§ 7026(f)(2)–(3)	The Proposed Regulations should be conformed with the statute which provides businesses with 15 days to honor opt out requests. Further, the rules should not impose requirements that would be infeasible, if not technically impossible, at the device level without businesses collecting much more information about consumers and their devices.	<i>Strike Proposed Regulations § 7026(f)(2) and (f)(3).</i>
Section III.i – B2B and Employee Data		
Proposed Regulations § 7000 Cal. Civ. Code § 3(A)(8), § 1798.145(m), (n)	The Proposed Regulations insufficiently account for use cases particular to the employee and B2B data. The Agency should carve out these categories from the existing regulations to consider the implications of the rules to these categories of data in more detail.	<i>Add a new § 7000(d): “<u>(d) To provide the Agency with time to adopt appropriate requirements, these regulations and the California Consumer Privacy Act shall not, without amendment to these regulations, apply to personal information that is subject to Cal. Civ. Code § 1798.145(m) or § 1798.145(n), irrespective of whether those subdivisions are operative.</u>”</i>
Section III.j – Effective and Enforcement Dates		
Proposed Regulations § 7000 Cal. Civ. Code § 1798.185(d)	To adhere to the statutory timeline, dates the Proposed Regulations are effective and enforceable should be extended by twelve months.	<i>Add new § 7000(e): “<u>These regulations shall become operative not less than one year after the date on which these regulations are finalized.</u>”</i>

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
<i>Other Comments – Audit Rights and Complainant Notice</i>		
<p>Proposed Regulations § 7304(b)</p> <p>Cal. Civ. Code §§ 1798.185(a)(18), 1798.199.50–55, 1798.199.65</p>	<p>The audit authority conferred on the Agency is overbroad and lacking reasonable limits for the initiation of an audit.</p>	<p><i>Amend § 7304(b):</i> “Criteria for Selection. The Agency may conduct an audit to investigate possible violations of the CCPA <u>if it determines that it has Probable Cause with regard to a particular subject.</u> 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.”</p>
<p>Proposed Regulations § 7300(b)</p> <p>Cal. Civ. Code § 1798.199.45</p>	<p>Complainant notice requirements should be limited to avoid publicizing Agency investigatory actions prematurely, which has the potential to cause severe reputational impact on businesses before evidence of a violation has been uncovered.</p>	<p><i>Amend § 7300(b):</i> “<u>After Notice (as defined in Cal. Civ. Code § 1798.199.50) has been made,</u> the Enforcement Division will <u>may</u> notify the complainant in writing of the action, if any, the Agency has taken or plans to take on the complaint, together with the reasons for that action or nonaction. Duplicate complaints submitted by the same complainant may be rejected without notice.”</p>
<i>Other Comments – Ambiguous Standards and Statutory Inconsistencies</i>		
<p>Proposed Regulations § 7004(c)</p> <p>Cal. Civ. Code § 1798.140(l)</p>	<p>The proposed intent provision relating to dark patterns would effectively impose a strict liability standard for user interfaces. It is common for businesses of all sizes to experience problems with their websites and other features, caused by no negligence or malicious intent. The Proposed Regulations should not hold businesses responsible for issues that they could not have prevented.</p>	<p><i>Amend § 7004(c):</i> “A user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice, regardless of a business’s intent, <u>and if the business responsible for the user interface offered it to customers knowing that it was likely to have that effect.</u>”</p>

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
<p>Proposed Regulations § 7010(e), 7016</p> <p>Cal. Civ. Code § 1798.125(b)</p>	<p>The Proposed Regulations create disclosure and other obligations for the collection of personal information in exchange for a financial incentive or price / service difference. Consistent with the plain language of the statute, the Proposed Regulations should not regulate as financial incentives or price/service differences any incentives or differences that are not directly related to a consumer's exercise of her rights under the CCPA.</p>	<p><i>An additional example of what is not a financial incentive should be provided to make this more clear.</i></p>
<p>Proposed Regulations § 7004</p> <p>Cal. Civ. Code § 1798.185(a)(7)</p>	<p>Although BPI supports the principle of usability with regard to consumer request submission methods, specifying that broken links could indicate legal noncompliance is excessive. We recommend removing such specific examples in favor of emphasizing the overarching principle.</p>	<p><i>Amend § 7004(a)(5): "Easy to execute. The business shall not add 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. . . . 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."</i></p> <p><i>We recommend deleting similarly specific illustrative examples under this subsection.</i></p>
<p>Proposed Regulations § 7024(h)</p> <p>Cal. Civ. Code § 1798.130(a)(2)(B), 1798.185(a)(9)</p>	<p>The Proposed Regulations do not address the 12-month look-back period for consumer requests in a manner consistent with the statutory text. Consumers should be permitted to request older information from businesses, but the rules should not impose a mandatory requirement that</p>	<p><i>Amend § 7024(h): "In response to a request to know, a business shall provide all the personal information it has collected and maintains about the consumer <u>for the 12-month period preceding the business's receipt of the verifiable consumer request. A consumer may request that the business provide all the personal information it has</u></i></p>

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
	businesses <i>shall</i> affirmatively provide the information.	<p><u>collected and maintains about the consumer</u> on or after January 1, 2022, including beyond the 12-month period preceding the business's receipt of the request, unless doing so proves impossible or would involve disproportionate effort. That 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 an an 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 for its decision. The business shall not simply state that it is impossible or would require disproportionate effort."</p>
<p>Proposed Regulations § 7052(a)</p> <p>Cal. Civ. Code § 1798.105(c)(1), 1798.140(ah)</p>	<p>The Proposed Regulations imply that a third party that receives a request to delete or to opt-out of sale/sharing of a consumer's personal information from a business must comply with the request in the same way that the business must. To ensure consistency with the statutory text, the CPPA should clarify that this requirement is limited to third parties that received the personal information for the purposes of behavioral advertising or pursuant to a sale of the relevant information.</p>	<p><i>Amend § 7052(a):</i> "A third party <u>to whom a business has sold or shared a consumer's personal information</u> shall comply with a consumer's request to delete or request to opt-out of sale/sharing forwarded to them from a business that provided, made available, or authorized the collection of the consumer's personal information. The third party shall comply with the request in the same way a business is required to comply with the request under sections 7022, subsection (b), and 7026, subsection (f). The third party shall no longer retain, use, or disclose the personal information</p>

Citations	Comment	Proposed Redline to Cited Proposed Regulations Provision
		unless the third party becomes a service provider or contractor that complies with the CCPA and these regulations.”
<i>Other Comments – Sensitive Personal Information</i>		
<p>Proposed Regulations § 7027</p> <p>Cal. Civ. Code § 1798.121(d)</p>	<p>The Proposed Regulations should be mindful that the right to limit does not apply to “[s]ensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer.”</p>	<p><i>Amend § 7027(a):</i> “The unauthorized use or disclosure of sensitive personal information 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) <u>and Cal. Civ. Code § 1798.121(d).</u>”</p>
<p>Proposed Regulations § 7027(l)</p> <p>Cal. Civ. Code §§ 1798.121(a)–(b), 1798.140, 1798.185(19)(C)</p>	<p>The list of permissible uses for Sensitive Personal Information captured in § 7027(l) are too narrow and fail to capture important use cases for which Sensitive Personal Data is likely to be necessary.</p>	<p><i>Add § 7027(l)(8):</i> “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. . . . <u>For compliance and reporting purposes, such as completing regulatory reporting, creating Suspicious Activity Reports (SARs), responding to judicial, administrative, regulatory, or law enforcement inquiries, and executing investigations, orders, warrants, and subpoenas.</u>”</p>

From: **Matthew Schwartz** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment - App Association Responses
Date: 23.08.2022 21:43:07 (+02:00)
Attachments: App Association Comments on Rulemaking under the California Privacy Rights Act of 2020 FINAL.pdf (9 pages)

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

Good afternoon,

Attached please find comments from ACT | The App Association in response to CPPA's call for public comments on its draft regulations governing compliance with the California Consumer Privacy Act.

Best,

Matt Schwartz
Policy Associate
ACT | The App Association

P: [REDACTED]

E: [REDACTED]

August 23, 2022

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

RE: ACT | The App Association Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020

I. Introduction and Statement of Interest

ACT | The App Association (App Association) appreciates the opportunity to submit comments in response to the California Privacy Protection Agency's (CPPA or Agency) call for input regarding its draft proposed rules under the California Privacy Rights Act of 2020 (CPRA). In general, the App Association supports the Agency's rulemaking efforts to create a clear and fair set of rules for both small businesses, like our member companies, and consumers. At the same time, we believe the regulations, as currently drafted, should be further refined through subsequent rulemaking activities.

The App Association represents thousands of small business software application development companies and technology firms, including many based in California and/or conducting business in California and falling within the scope of law. Our member companies create technologies that generate internet of things (IoT) use cases across consumer and enterprise contexts and are primary drivers of the global digital economy. Today the ecosystem the App Association represents—which we call the app economy—is valued at approximately \$1.7 trillion and is responsible for tens of millions of jobs around the world, including 702,010 in California alone.¹ The growth of this vital ecosystem is expected to continue; worldwide consumer spending in mobile apps is projected to reach \$171 billion by 2024, more than double the \$85 billion from 2019.²

Consumers who rely on our members' products and services expect that our members will keep their valuable data safe and secure. The small business developer community the App Association represents practices responsible and efficient data usage to solve

¹ See *State of the U.S. App Economy: 2020*, ACT | THE APP ASSOCIATION, (2020) available at: <https://actonline.org/wp-content/uploads/2020-App-economy-Report.pdf> (noting that California has an estimated 702,010 app economy workers as of 2020).

² Sarah Perez, Mobile app spending to double by 2024, despite economic impacts of COVID-19, TechCrunch (Apr. 1, 2020), <https://techcrunch.com/2020/04/01/mobile-app-spending-to-double-by-2024-despite-economic-impacts-of-covid-19/>



problems identified across consumer and enterprise use cases. Their customers have strong data security and privacy expectations, and as such, ensuring that the company's business practices reflect those expectations by utilizing the most advanced technical protection mechanisms (e.g., end-to-end encryption) is a market-driven necessity.

The App Association serves as a leading resource in the privacy space for thought leadership and education for the global small business technology developer community.³ We regularly work to keep our members up to speed on the latest policy and legal developments and to translate those into practical and useable guidance, including on California privacy law, to ease the burden of compliance.⁴

II. General Comments

The App Association recognizes the complexity of the task set out for CPPA as it seeks to build organizational capacity as the nation's first state-specific privacy regulator, while at the same time working to draft and finalize the wide breadth of regulations authorized through CPRA. Given the fact that California boasts the 5th largest economy in the world and the largest app economy workforce of any state, any decisions CPPA makes will have an immense impact on the entire digital ecosystem.

As the Agency is aware, states around the country continue to introduce and pass comprehensive privacy legislation, meaning that the risk for excessively complex, or even conflicting, regulatory frameworks grows month after month. With this rulemaking process, the CPPA has the opportunity to introduce more standardization into our growing national privacy patchwork and reduce the complexity of existing regulations issued by the Office of the California Attorney General, which already run more than 11,000 words with 59 pages of explanatory notes.

As a general point, we appreciate the substantial amount of work that clearly went into reorganizing and improving the clarity and readability of this iteration of the regulations. With this set of draft regulations, CPPA organized information in a much more streamlined manner compared to previous versions, which should improve business' understanding of their expectations under the law. In particular, we appreciate the checklist format of Section 7011 which details *all* the requirements for company privacy

³ See e.g., ACT | The App Association, *Innovators Network Foundation Announces Inaugural Privacy Fellows* (September 2019), available at: <https://actonline.org/2019/09/23/innovators-network-foundation-announces-inaugural-privacy-fellows/>.

⁴ See e.g., ACT | The App Association, *General Data Protection Regulation Guide* (May 2018), available at: https://actonline.org/wp-content/uploads/ACT_GDPR-Guide_interactive.pdf; *What is the California Consumer Privacy Act* (January 2020), available at: <https://actonline.org/wp-content/uploads/What-is-CCPA.pdf>.



policies. Centralizing all requirements all in a single location rather than scattering them throughout the regulations cuts down on time needed to cross-reference and eases compliance overall.

At the same time, we are concerned that the timeline for finalization of these regulations remains unclear with less than four months before the law becomes enforceable, and more than a month after the formal statutory deadline for finalization already passed. Ultimately, the delay in proposing and finalizing these rules means that businesses will have little to no time to read, understand, and integrate the rules into a complete compliance program before they are legally liable.

This is now the fourth iteration of regulations implementing California privacy law (not counting the CPRA ballot initiative itself) and a stable legal landscape has yet to emerge to fully guide businesses or to have a meaningful impact on the ecosystem. This round of rulemaking adds new timelines for businesses to respond to consumer requests (which themselves depend on dynamic relationships with third parties that are subject to fluctuation), new definitions and concepts, and entirely new interpretations of the statute. It will not be trivial for businesses to digest and translate these new requirements into their business practices. As such, we urge that the Agency to push back the enforcement date for the law for a further 12 months, or at minimum enact a moratorium on enforcement until it can finalize the regulations and grant businesses a reasonable grace period to come into compliance.

In the alternative, we reiterate our call for the Agency to formally prioritize enforcement activities toward those with already documented privacy harms and/or particularly high-risk business practices, similar to the criteria for agency audits detailed in Section 7034(b). In the view of the App Association, the Agency should adopt a risk-based approach to its enforcement powers by prioritizing rules and enforcement actions that mitigate the most harmful activities that exist *today* and that erode consumer trust digital marketplace on a widespread basis. For example, the Agency should first rectify existing instances of non-compliance among the largest, data-hungry digital companies, such as through the evasion of the definition of sale under the law for the purpose of continuing a surveillance-based targeted advertising business model.

Finally, we note that CPPA has yet to take on the full breadth of its rulemaking powers, leaving some areas untouched at present, such as processing that presents a significant risk to consumers' privacy or security, cybersecurity audits and risk assessments performed by businesses, and automated decision making. We welcome formal notice regarding whether we can expect further guidance on these topics in this round of rulemaking or if these topics are being reserved for future rounds.



III. Comments on Specific Topics Addressed in the Draft Regulations

Definitions

Section 7001(h) establishes what “disproportionate effort” means within the context of responding to a consumer request, addressing an ambiguity created by CPRA whereby businesses must respond to consumer requests to know, correct, or delete unless that response “proves impossible or involves *disproportionate effort*,” a term left undefined in the statute itself.⁵ The draft regulations helpfully provide a few specific examples of what would constitute disproportionate effort, including responding to requests for personal information that is not in “a searchable or readily-accessible format, is maintained only for legal or compliance purposes, is not sold or used for any commercial purpose, and would not impact the consumer in any material manner.”⁶ One additional example we suggest CPPA add to the list is any requested data that is no longer accessible without creating a significant cybersecurity risk. For example, some businesses may only store certain personal information on archived backup drives maintained for emergency purposes that may introduce network security risks if accessed regularly.

We also suggest that the regulations consider a more granularized framework for the treatment of individual requests in light of the inclusion of household-level data in the definition of “personal information.” Previous Subsection K, defining “household” has been removed from the regulations, as the term is now defined through the text of CPRA.⁷ However, since the law states that personal information includes information that can be reasonably linked to a household, individuals are at risk for having their opt out preferences or consumer requests dictated by other members of their household. For example, many apps currently allow multiple users on the same device or account to create individualized preferences through user profiles. If one user of that device decides to opt out or requests that the business delete their data, it is unclear how the business can honor the requests of a different user of that same device that select a different set of preferences.

Restrictions on the Collection and Use of Personal Information

The concepts of “explicit consent” and “average consumer” are unnecessarily ambiguous. Section 7002 states that “[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” and that the businesses processing activities must be

⁵ California Civil Code § 1798.105 (c)(1)

⁶ CPPA Proposed Regulations, §7001 (h)

⁷ California Civil Code § 1798.140 (q)



consistent with what an "average consumer" would expect.⁸ In order to process personal information that is inconsistent with what an average consumer would expect or to collect additional categories of information, the business must receive "explicit consent." It is unclear whether the Agency intends for the term "explicit consent" to signal an elevated version of consent (similar to the implied vs. explicit consent construct in Europe's General Data Protection Regulation [GDPR]). Similarly, GDPR's data minimization construct includes a reasonableness standard but avoids the use of the ambiguous "average consumer" concept. The text of CPRA already clarifies the meaning of consent, and based on a plain reading, it seems consent requires an affirmative and informed decision by the consumer, which ostensibly meets the definition of explicit. Additional guidance on the relationship between explicit consent and consent as defined in CPRA would ease business understanding of the new regulations.

Section 7002 also provides several examples intended to clarify what compatible and incompatible processing purposes may be. In Example B, the Agency details a cloud storage service, saying that the business' use of personal information to improve the service is a compatible purpose, while the business' use of that information to create unrelated or *unexpected* services is not. In the experience of many App Association member companies, consumers may not always *expect* specific improvements to products and services, even if they ultimately benefit from them. While we agree that using personal information to create high-risk products and services without consumer consent, such as a facial recognition algorithm, is unacceptable, not all unexpected improvements are objectionable. A risk-based approach to incompatible processing purposes may be preferable in order to preserve businesses' ability to create innovative products that consumers may not anticipate but are unlikely to bring them harm.

Privacy Policies

Businesses now need to include in their privacy policies information related to how they will process user opt out preference signals, including information about "whether the signal applies to the device, browser, consumer, account, and/or offline sales, and in what circumstances."⁹ While understandable in light of CPRA's language referencing the ability for businesses to honor user opt out preference signals, many small businesses may not even know about the existence of user opt out preference signals, let alone that they must post detailed information about the way they intend to process them. Given the likely quick turnaround between final regulations and enforcement, we suggest that this requirement be delayed until the concept is further socialized with all businesses and that it be optional for businesses that do not sell or share personal information but nonetheless meet the coverage threshold for the law.

⁸ CPPA Proposed Regulations, §7002 (a)

⁹ CPPA Proposed Regulations, §7011 (3)(F-G)

Notice at Collection

Section 7012 (g)(3) should be clarified to read that a third party that controls the collection of personal information on the first party's *physical premises* shall provide a notice at collection at the physical premises. Without the clarification that the collection of personal information is taking place in the physical realm, such as in a vehicle or at a brick and mortar location, this subsection could be read to require third parties to provide notice at collection at the physical location of any first party for which it controls collection, even if that collection occurs online, which does not seem to be the intent of the statute or implementing regulations.

Obtaining Consumer Consent

Section 7004 states that “businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent” that are easy to understand, among other requirements. We urge the Agency to consider a more objective standard than “easy to understand” considering the ranges of age and sophistication of consumers submitting requests. Given the relative complexity of the underlying information businesses communicate with such notices, a high school graduate reading level might be the appropriate standard to index against. If the Agency remains intent on relying on a subjective standard, we urge it to include examples of what would be easy to understand versus overly complicated language, similar to other example sets provided in the Section.

Alternative Opt Out Link

We appreciate the flexibility enabled by Section 7015, which provides businesses with a new option of providing consumers with a single link that allows them to exercise both their right to opt out of sale/sharing and right to limit use of sensitive data. Given CPRA’s new right to limit use of sensitive data and the accompanying requirement that businesses post a conspicuous link for consumers to exercise this right, the new alternative opt out link helps businesses avoid posting two separate “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links. This both eases demands on UX/UI departments and helps avoid any consumer confusion that two separate opt out links could create.

Universal Opt Out

The App Association does not believe that the statute supports the Agency’s interpretation that businesses *must* abide by universal opt out signals. The text of CPRA simply states that a business shall not be required to provide the “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links, or the alternative opt out link, *if* it “allows consumers to opt out of the sale or



sharing of their personal information and to limit the use of their sensitive personal information through an opt out preference signal.”¹⁰ The text of Section 1798.1185 of the statute, which grants the Agency rulemaking authority, also does not support the Agency’s decision to require the honoring of opt out signals. Instead, it merely says the Agency may “issu[e] regulations to define the requirements and technical specifications for [emphasis added] an opt out preference signal sent by a platform, technology, or mechanism,” referring to the specifications of the opt out signal itself and not the business’s response to it.¹¹

Additionally, businesses that do not sell or share personal information should not have to confirm the receipt to opt out preference signals, as is currently required by Section 7026(f)(4). Similar to the requirement that all businesses disclose their approach to honoring opt out signals in their privacy policy, even if they do not sell or share data, such a confirmation requirement may come as a surprise to businesses that do not engage in the selling or sharing of personal information and serves minimal benefit to consumers. The subsection could simply be rewritten to read, “[a] business that *sells or shares personal information* shall comply with a request to opt out of sale/sharing.”

Agency Audits

CPRA grants the CPPA the ability to “issu[e] regulations to define the scope and process for the exercise of the agency’s audit authority” over covered businesses’ compliance with the law.¹² Unsurprisingly, the Agency grants itself broad authority to audit any “business, service provider, contractor, or person to ensure compliance” with any section of the law, so long as the audit involves an investigation of possible violations of CCPA, the business’s processing presents significant risk to consumers in the Agency’s determination, or if the business has a history of noncompliance with privacy laws.¹³ As stated in our general comments, we believe the Agency should focus its oversight authority, at least at the outset of its new regime enforcing a plethora of novel requirements coming into effect likely after the statutory enforcement date, on the companies in the latter two categories. Those are the businesses with the most power to harm consumers on a widespread basis and to undermine trust in digital products and services.

Consumers’ Right to Correct

CPRA expanded CCPA’s slate of consumer rights (the right to delete data, the right to know what data is collected, the right to access data, and the right to know what data is

¹⁰ California Civil Code § 1798.135 (b)(1)

¹¹ California Civil Code § 1798.185 (19)(A)

¹² California Civil Code § 1798.185 (18)

¹³ CPPA Proposed Regulations, §7034 (a-b)



shared or sold) by adding a new right to correct inaccurate personal data.¹⁴ Businesses are instructed to use "commercially reasonable" efforts to correct inaccurate personal information, though the term was left undefined in CPRA. With the draft regulations, CPPA left that term undefined even as it added prescriptive new requirements regarding businesses' addressing of these requests in Section 7020. Though the Initial Statement of Reasons accompanying the draft regulations state that the intention of Section 7020 (a) is to make operational the "commercially reasonable" standard, it remains unclear following the requirements set out in the remainder Section 7020 regulation satisfies the "commercially reasonable" standard.¹⁵ Adding an affirmation that businesses that follow the requirements in Section 7020 to correct personal information are using commercially reasonable practices could resolve ambiguity on this point, especially considering that a similar standard is not attached to requests to delete or know, which are also addressed Section 7020.

Information to Be Provided in Response to a Consumer Request to Know (Specific Pieces of Information)

CPRA expands the 12-month disclosure period for a consumer's right to know. Consumers may request to know about any new personal information collected or processed on or after January 1, 2022, even if that information is more than 12-months old at the time of the request, subject to certain exceptions detailed in the regulation. The App Association urges the CPPA to adopt a common-sense exception inclusive of instances where the business (1) migrated its data prior to the 12-month lookback to new storage facilities or service providers, (2) otherwise does not maintain access to the requested data, or (3) cannot make the requested data accessible without creating a significant cybersecurity risk.

Requests to Limit Use and Disclosure of Sensitive Personal Information

Section 7060 currently prohibits businesses from requiring that a consumer verify their identity to make a request to opt out of sale or sharing or to make a request to limit the use of sensitive information.¹⁶ The Initial Statement of Reasons justifies this decision by saying that "the potential harm to consumers from non-verified requests is minimal."¹⁷ We disagree, as in the case of limiting the use of sensitive information, the damage of an fraudulent opt out can be significant. For example, a connected healthcare application may use sensitive information about a person as an input to an algorithm that determines part of that person's individualized treatment plan. If a fraudster opts that person out of the use of that information and the algorithm is stripped of critical inputs, that person's treatment plan could be seriously altered without them even

¹⁴ California Civil Code § 1798.106

¹⁵ CPPA Initial Statement of Reasons § 7023 (a)

¹⁶ CPPA Proposed Regulations, §7060 (b)

¹⁷ CPPA Initial Statement of Reasons § 7060 (b)

realizing a change has been made. We urge the Agency to allow for verification of requests to limit sensitive information and, in general, caution the Agency against taking the stance that a person's decision to share sensitive information was made trivially and should be able to be easily undone.

IV. Conclusion

The App Association is a strong supporter of privacy regulation that upholds the mission of consumer protection and sets a clear baseline set of expectations for the businesses that are required to comply. From the small business perspective, it is also vital that privacy regulation create a predictable and consistent legal landscape and is scalable such that smaller entities can continue to comply and compete with larger entities. We are hopeful that the CPPA can strike the appropriate balance in future rulemaking activities.

We thank the CPPA in advance for its consideration of our views, and we look forward to engaging further in the future.


Sincerely,



Brian Scarpelli
Senior Global Policy Counsel

Matt Schwartz
Policy Associate

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005

e: 

From: **Edwin A. Lombard III** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
Subject: Written "CPPA Public Comment"
Date: 23.08.2022 14:44:18 (+02:00)
Attachments: CCPA Comments 2022 8.23.20.pdf (7 pages)

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

Good afternoon CCPA board members. I look forward to seeing you all tomorrow in Oakland. I have attached a comment letter from the primary ethnic chambers of commerce regarding the Privacy Protection Act Regulation. Please let me know if you received it.

Thank you,



Edwin A. Lombard III
President/CEO
ELM Strategies
1079 Sunrise Avenue, Suite B315
Roseville, CA 95661
[REDACTED]



August 23, 2022

California Privacy Protection Agency

Attn: Brian Soublet

2101 Arena Boulevard

Sacramento, CA 95834

Submitted via email: regulations@coppa.ca.gov.

Re: California Privacy Protection Agency (CPPA) Public Comments

Dear Mr. Soublet:

On behalf of our respective organizations and the California businesses we represent, we are submitting our collective comments on the CPPA's proposed California Consumer Privacy Act Regulations ("Regulations") published on July 8, 2022. We appreciate the opportunity to provide comments on a significant body of law that will have consequential impacts on the many small, diverse businesses we represent.

Our organizations remain committed to upholding Proposition 24 to provide strong privacy protections for consumers. We also recognize there are numerous challenges, including staffing amid the ongoing pandemic, for a new agency like CPPA to develop the complex set of regulations called for in Proposition 24. Thus, we supported the CPPA's budget proposal for 34 positions in fiscal year 2022-23, which would allow the CPPA to fulfill its immediate statutory responsibilities assigned by voters.

We also supported and called for extending the July 1, 2022 deadline for the CPPA to adopt the regulations when we testified at the Assembly Budget Subcommittee

on State Administration and the Senate Budget Subcommittee on State Administration and Local Government. We shared the following statement with the committees:

“There is too much at stake with the privacy protection mandates under Proposition 24 to “build a plane while flying it [as described by the CPPA].” Instead, we recommend the approach of building the plane the right way so that it can land safely for all Californians, eliminating the risk and uncertainty associated with innovating, groundbreaking, and first-in-the-nation regulatory actions on the fly. In this case, we want to help the [CPPA] get it right which means giving it more time to develop privacy regulations that are reasonable and practicable.”

At this point, however, after participating in a number of CPPA hearings, witnessing many critical CPPA actions – and inaction – and reviewing the agency’s draft regulations, it is unfortunate and disappointing that the CPPA and its proposed regulations fall short of what is required under Proposition 24.

The CPPA must work with the Legislature to extend the July 1, 2022, deadline, and July 1, 2023, enforcement date before the legislative session ends on August 31, 2022 to remedy issues in the draft regulations and rulemaking process.

Lack of Accountability

As mandated by Proposition 24, the CPPA is required to adopt privacy regulations by July 1, 2022 and enforce them by July 1, 2023.¹ The CPPA publicly admitted that it would not meet the July 1, 2022 deadline and discussed options to address it, but ultimately the agency took no action to meet its obligations under Proposition 24.

¹ Section 21: Civil Code 1798.895: (d) Notwithstanding subdivision (a), the timeline for adopting final regulations required by the act adding this subdivision shall be July 1, 2022. Beginning the later of July 1, 2021, or six months after the agency provides notice to the Attorney General that it is prepared to begin rulemaking under this title, the authority assigned to the Attorney General to adopt regulations under this section shall be exercised by the California Privacy Protection Agency. Notwithstanding any other law, civil and administrative enforcement of the provisions of law added or amended by this act shall not commence until July 1, 2023, and shall only apply to violations occurring on or after that date. Enforcement of provisions of law contained in the California Consumer Privacy Act of 2018 amended by this act shall remain in effect and shall be enforceable until the same provisions of this act become enforceable.

Consider the following CPPA record:

CPPA Meeting September 7, 2021

- “If we do the math, we can’t meet the May [submission] deadline to submit [to the Office of Administrative Law].”
- “Once we hire the Executive Director, we need to find a legislative champion to push back the deadline.” (Emphasis Added)
- “Hate to rush them.” “Rather get good set of rules.” “Lots of countries and states [are watching this] ..., get it right”

CPPA Meeting October 18, 2021

- The CPPA discussed “informally missing” the July 1, 2022 deadline.

CPPA Meeting February 17, 2022

- When asked about the July 1, 2022 deadline, the agency executive director acknowledged that the rulemaking process is likely to pass the July 1, 2022 deadline.

Assembly and Senate Budget Subcommittee 2022 Spring Hearings

- Our organizations raised the issue of legislatively extending the July 1, 2022 deadline when the CPPA’s budget was heard at the Legislature, but the CPPA declined to comment on the issue.

The CPPA’s inaction in working with the Legislature to extend the July 1, 2022 deadline means the small, diverse businesses we represent may have less time to comply with the regulations and are likely to be forced to spend even more money to make up for the CPPA’s lack of transparency and accountability. The agency must act to extend the truncated compliance period to be consistent with the one-year window specified by Proposition 24.

We reiterate that Proposition 24 is an extremely complicated body of law with significant impact for small, diverse businesses that serve many consumers. The

small businesses we represent are the backbone of our local communities and a major part of California's economic engine. Further, our state's small, diverse businesses cannot be expected to survive yet another layer of economic burden on top of rising inflation, supply chain challenges, workforce challenges and the ongoing pandemic they have already been forced to grapple with.

Lack of Authority

In our review of the regulations, the CPPA lacks the authority to adopt the regulations beyond July 1, 2022. Government Code Section 11349 (a) states:

- "Authority" means the provision of law which permits or obligates the agency to adopt, amend, or repeal a regulation.

Here, Proposition 24 had one provision about CPPA's obligations to adopt the regulation by July 1, 2022 and there are no other provisions stating that CPPA can adopt regulations beyond that date (see footnote 1).

It is also important to note that the CPPA has publicly declared that, more irresponsibly, it will miss the July 1, 2022 deadline as it will not promulgate regulations on cybersecurity audits (Section 1798.185 (a)(15)(A)), risk assessments (Section 1798.185 (a)(15)(B)), or automated decision-making technology (Section 1798.185 (a)(16) (See page 6 of Notice of Proposed Rulemaking.)

As it stands, the proposed regulations are in violation of Proposition 24, and therefore, CPPA must withdraw them. To remedy this issue, we suggest that the CPPA work with the Legislature to extend the July 1, 2022 deadline before the legislative session ends on August 31, 2022. Proposition 24, Section 25, allows the Legislature to amend the initiative by a majority vote "provided that those amendments are consistent with and further the purpose of and intent of [the] act as set forth in Section 3...."

Among other issues where the CPPA lacks authority is the proposed regulatory text on the global opt-out preference signal. The text of Proposition 24 makes it clear that abiding by the signal is a voluntary choice. The proposed regulation, however, exceeds this framework and would make observance of the signal mandatory.

Lack of Consistency

The regulations are inconsistent with Proposition 24. Government Code Section 11349 (d) states:

- “Consistency” means being in harmony with, and not in conflict with or contradictory to, existing statutes, court decisions, or other provisions of law.

As discussed above, the adoption of the regulations going beyond July 1, 2022 not only lack authority, but they are also inconsistent with the balance sought in Proposition 24, Section 3 (C)(1):

- The rights of consumers and the responsibilities of businesses should be implemented with the goal of strengthening consumer privacy while giving attention to the impact on business and innovation. (Emphasis added)

Both larger businesses and small, diverse businesses were given a one-year window to comply with the regulations; however, the adoption of these regulations beyond July 1, 2022 significantly reduces that time period for them.

Also, the Economic and Fiscal Impact Statement (EFIS, STD. 399) supporting the regulations that the CPPA prepared via the Berkely Economic Advising and Research (“Bearecon”) organization provided inadequate attention to the impact of businesses and innovation. For example, Bearecon states “[t]here is no readily available database that tracks the number of California businesses subject to the CCPA, thus we estimate the number of impacted businesses based on the three criteria included in the CPPA.” (See page 3 Bearecon Notes)

Presuming such data is unavailable is wrong, as information is readily available on small, diverse businesses (including at the various chambers of commerce listed on this letter). Yet, to our knowledge, neither Bearecon nor the CPPA reached out to such organizations to address the economic impact of the regulations on them.

Furthermore, the CPPA’s EFIS (number 5, page 3) has a conclusory statement about innovation: “Detailed specification of user interface may reduce product

variety, but this impact is expected to be minimal and confers important consumer benefits.” We are not aware of additional discussion regarding innovation in Bearecon notes related to CPPA’s EFIS to support CPPA’s assertions.

Another gap of information is CPPA’s claim that “[t]he proposed regulation has a small cost per business (\$127.50) and thus is unlikely to impact entry /exit decisions.” It is unclear how CPPA concluded that amount given that they (including Bearecon) admittedly had limited information.

Our organizations would like further explanation on other inconsistencies when comparing CPPA’s EFIS with California Department of Justice’s (DOJ) EFIS, STD 399 from 2019 (CCPA regulations):

Data	DOJ CCPA EFIS STD. 399 (2019)	CPPA CCPAR EFIS STD. 399 (2022)	Questions
Total number of businesses impacted	15,000-400,000	66,076	How did the number of businesses impacted decrease given the lack of data relied upon by the CPPA?
Number of jobs created and eliminated	261/ 9,776	47.7/ 0	How did the CPPA arrive at a different number?
Total statewide dollar costs that businesses and individuals may incur to comply with this regulation over its lifetime	\$467 to \$16,454 million	\$8,424,690	How did the CPPA arrive at a different amount given the lack of data relied upon by the CPPA?

In our view, the CPPA and the draft regulations have failed to adhere to the balance sought under Proposition 24; thus, such inconsistencies must be addressed. We recommend redoing the CPPA EFIS STD. 399 with meaningful data utilized and input from small, diverse businesses as opposed to broad estimates based on incomplete data.

Another recommendation to remedy the inconsistency discussed above with Proposition 24's balance of "giving attention to the impact on business and innovation" is for CPPA to work with the Legislature (before it adjourns on August 31, 2022) to extend the enforcement date of July 1, 2023 by six months, thereby giving all businesses the legally required one-year window to comply with the regulations as specified in Proposition 24.

Sincerely,



JULIAN CAÑETE

President & CEO
California Hispanic Chambers
of Commerce
1510 J Street, Suite 110
Sacramento, CA 95814



EDWIN A. LOMBARD III

President/CEO
ELM Strategies
1079 Sunrise Avenue, Suite B315
Roseville, CA 95661



PAT FONG KUSHIDA

President/CEO
California Asian Pacific
Chamber of Commerce
1610 R Street, Suite 322
Sacramento, CA 95811

cc:

Members of the Legislature

Ana Matosantos, Cabinet Secretary; Office of Governor Gavin Newsom

Christy Bouma, Legislative Affairs Secretary; Office of Governor Gavin Newsom

Dee Dee Myers, Senior Advisor & Director; Governor's Office of Business & Economic
Development

Tara Gray, Director; California Office of Small Business Advocate

From: **Andrea Amico** [REDACTED]
 To: **Regulations** <Regulations@cpha.ca.gov>
 CC: **Liz (Elizabeth) Magana** [REDACTED]
 Subject: CPPA Public Comment - Privacy4Cars
 Date: 23.08.2022 17:47:29 (+02:00)
 Attachments: Privacy4Cars - Statement for CPPA - 08232022.pdf (6 pages)

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

Thank you for the opportunity to file the attached comment for the hearing taking place on August 24-25 on the proposed rulemaking.

I'm available for further discussion or additional information as needed.

Kind regards

Andrea Amico

Founder & CEO, Privacy4Cars

<https://privacy4cars.com>

Download our whitepaper on the new Safeguards Rule or schedule a demo

NEW--> POLITICO: What your car knows about you

<https://www.politico.com/newsletters/digital-future-daily>

NEW--> Who Is Collecting Data from Your Car?

<https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car>

NEW--> New FTC directives driving change at car dealerships

<https://www.pymnts.com/internet-of-things/2022/new-ftc-data-directives-driving-change-at-car-dealerships/>

NEW--> How Fleets can Keep Information Safe

<https://www.automotive-fleet.com/10174166/reduce-your-risk-of-vehicle-data-breaches-tips-to-keep-your-information-safe>

NEW--> Automotive Compliance Professionals: Sell Cars, not PI

<https://view.flipdocs.com/spring-2022-acp>

Buying a used car? The previous owner may still be able to access app, control it remotely

<https://fox23maine.com/news/i-team/buying-a-used-car-the-previous-owner-may-still-be-able-to-access-app-control-it-remotely>

Google Play App: <https://play.google.com/store/apps/details?id=com.privacy4cars>

iTunes App Store: <https://itunes.apple.com/us/app/privacy4cars/id1370969499?mt=8&ign-mpt=uo%3D2>

Twitter: <https://twitter.com/privacy4car>



<https://Privacy4Cars.com>

CCPA Public Comment on “Proposed Rulemaking Under the California Privacy Rights Act of 2020”

Submitted to California Privacy Protection Agency via email at regulations@cppa.ca.gov

August 23rd, 2022

Privacy4Cars Inc. (“Privacy4Cars”) is pleased to present this statement to the California Privacy Protection Agency with respect to your invitation for comment on “Proposed Rulemaking Under the California Privacy Rights Act of 2020” in advance of the public hearings taking place on August 24th and 25th. I am writing to you to share our firsthand experience with how businesses respond to consumers’ data requests, specifically within a broad slice of the automotive industry (car rentals, vehicle manufacturers, service providers, and data brokers).

There are three devices that cause the collection of the massive amount of personal data: computers, smartphones, and vehicles. The first two are often discussed (and I am sure will be mentioned multiple times during this hearing). Vehicles however collect terabytes of sensitive personal information... but too often remain in the shadows of data privacy and security discussions. It is important for this Agency to realize that modern vehicles are like web browsers.... but in the physical world, and not only your “browsing history” is being collected, sold, and shared at accelerating and concerning pace, but also vehicle drivers and occupants (including minors) seem to have a harder time getting their privacy rights respected.

I founded Privacy4Cars to give businesses in the automotive industry a simple, reliable, and auditable solution to delete the personal data vehicles routinely collect from drivers and passengers in order to prevent harms to consumers’ privacy, security, and safety. This is an issue that affects over 100 million Americans every year and something the Federal Trade Commission warned about multiple times. We have also, from the very beginning of our company, offered free tools to consumers to help them reduce their vehicle data footprint. As part of that effort, Privacy4Cars’ wholly owned subsidiary, Privacy4Cars California LLC, was incorporated in California and registered with the Office of the Attorney General with the specific purpose to aid California consumers, free of charge, to file Data Subject Requests (“DSRs”) and assert their CCPA rights.

Just like with laptops and smartphones, focusing on the manufacturers of those devices alone is vastly insufficient to protect the privacy and security of consumers, because the data generated by those devices fuels an entire ecosystem. Privacy4Cars keeps track of hundreds of companies that engage in the collection, sharing, and brokerage of vehicle data.

Privacy4Cars' study

Between late May and late July 2022 Privacy4Cars submitted close to 4,000 California Consumer Privacy Act ("CCPA") Data Subject Requests on behalf of California residents. Those DSRs required respondents to provide a copy of the personal information companies possessed about the individuals: either collected directly from the individuals (through forms or the sensors of the vehicles they rented), or indirectly through data sharing agreements with affiliates or business partners. The recipients of the DSRs included hundreds of companies belonging to 4 broad categories: car rental companies, original equipment manufacturers ("OEMs", i.e. vehicle brands), data brokers, and service providers.

This comment is meant to spotlight several practical issues concerning such DSRs by considering the text of the CCPA and the proposed regulations published by the California Attorney General on February 10, 2022 ("Proposed Regulations"). Section 1798.100 requires businesses to disclose and deliver the personal information and outlines which Substantive Response Timing and Methods should be followed. Our study shows that, in the broader automotive domain, there are major gaps between what should be happening based on CCPA's requirement and what consumers and agents like ourselves face when attempting to assert the privacy rights granted under the law.

66% of DSRs failed to receive any response at all

Only 1,325 requests out of 3,908 requests, or less than 34% received any response at all. This is despite sending reminders to several of the companies that had not provided a response. Some companies claimed they had not received a request alleging "email issues", but several of those companies did not provide a response even after we forwarded a copy of the original request. Among the many companies that did not respond to all the DSRs we filed on behalf of California consumers, we were surprised to see that this list included:

- 3 Rental car companies
- 5 Automotive manufacturers
- 7 Automotive data brokers
- 16 Large high-tech companies that power in-vehicle services

We hope the Agency will keep watchful eye whenever companies ignore DSRs, whether they are filed directly by California consumers or their appointed Agents.

More than 80% of filed DSRs failed to be delivered within 45 days of receiving the verifiable request

As of today, Privacy4Cars has received only 1,154 responses out of the 3,908 requests placed on behalf of California consumers, or less than 30% of all requests filed. Of those, only 773 out of 1,154 requests that received a response, or less than 20% of the total number of requests, was received within 45 days.

In other words, despite companies having an option to extend the 45 days deadline, more than 80% of the requests were delinquent and did not meet the timeline requirements of CCPA.

Not responding or delayed responses are highly demotivating to consumers and to agents and cause significant friction and a degradation of consumer rights. We are interested in hearing the Agency's thoughts as to what escalation mechanisms California residents and their Appointed agents should be using to get timely responses.

Some consumers are facing costs when filing DSRs

The law requires that businesses offer responses free of charge. However, some businesses required notarized affidavits, despite the fact we provided an authorization form with every submitted request. In addition to demanding a notarized affidavit (while the law clearly states it is not necessary), those businesses did not have systems in place to reimburse consumers - even though providing a reimbursement for notarization is a requirement under CCPA. When, upon our pushback, companies pointed us to reimbursement forms, it was apparent that those forms did not contemplate CCPA notarization cost reimbursement as an acceptable category (see for example AAA's "[Automotive and Home Reimbursement Consideration Form](#)"). We doubt that most California residents would have known that the request for a notarized document was not necessary, nor that they should have been reimbursed for the associated legal costs. We hope the Agency will agree that these untrue "requirements" are harmful to consumers, recognize they hamper significantly consumers' and agents' ability to assert their rights, and should be restricted going forward.

Businesses, and especially data brokers, claim alleged exemption for de-identified data in order to avoid sending a copy of the Personal Information they collect about consumers and deleting it

Recently, the [Federal Trade Commission highlighted that](#): "**Claims that data is "anonymous" or "has been anonymized" are often deceptive.** Companies may try to placate consumers' privacy concerns by claiming they anonymize or aggregate data. Firms making claims about anonymization should be on guard that these claims can be a deceptive trade practice and violate the FTC Act when untrue. Significant research has shown that "anonymized" data can often be re-identified, especially in the context of location data. One set of researchers demonstrated that, in some instances, it was possible to uniquely identify 95% of a dataset of 1.5 million individuals using four location points with timestamps. Companies that make false claims about anonymization can expect to hear from the FTC."

Our experience after filing 3,908 DSRs on behalf of California consumers who rented a car is that data brokers who advertise on their website that they collect precise geolocation data from vehicles routinely claim they do not have to respond to requests because, they allege, the data in their possession has been anonymized or de-identified. For the Agency's benefit, here are three examples of responses provided by large-scale automotive data brokers:

1. **Wejo's response:** We acknowledge receipt of your subject access request. We have reviewed our records. We do not have any records containing *[consumer information and vehicle information redacted]*. For your general awareness, Wejo does not retain connected vehicle data associated with the name of any person, any license plate number, or any rental car unit

number. Wejo does not retain data identified with any person or household (including any person's name, license plate number, rental car unit number, or reservation number). Wejo is a global leader in connected vehicle data, revolutionizing the way we live, work and travel by transforming and interpreting historic and real-time vehicle data. With the most comprehensive and trusted data, information, and intelligence, Wejo is creating a smarter, safer, more sustainable world for all. Please be rest assured that Wejo takes privacy seriously, with this in mind we advocate for Data for Good™. Thank you for your correspondence, we value the interest of like-minded people wanting to advance transportation safety and the transportation experience.

2. **Arity's response:** Arity values your privacy and takes the privacy and security of your data seriously. We believe in your right to make informed decisions about your personal information. Arity works with app providers and other companies to collect certain geolocation and related driving behavior information using Arity's technology that is contained in a mobile app or a device installed in your vehicle. To enhance user privacy, Arity maintains driving behavior information in a de-identified format, which means it is not stored or associated with your name, phone number, address, or any other data that would allow Arity to reasonably match your identity to your driving behavior information. Arity also collects mobile advertising identifiers (referred to as Ad IDs) to serve relevant advertising based on your driving behavior. Arity does not associate the Ad IDs with any information that would allow us to identify you personally, but Ad IDs may be considered personal information under the California Consumer Privacy Act. Because we keep driving behavior data and Ad IDs in a de-identified manner, we are unable to verify your identity based on our data and return the specific pieces of this information to you. However, you may be able to obtain driving behavior data or other information directly from a company that you deal with directly that Arity services (Arity's business clients which include app providers).
3. **Otonomo's response:** We acknowledge receipt of your request to exercise your rights under the California Consumer Privacy Act. Following Otonomo request, you, *[consumer name redacted]* managed to provide Otonomo Privacy Team with authorization for Privacy4Cars to submit and manage your Data Subject Requests on July 28th, 2022. Having searched through our systems and according to the details provided in your request below, we could not locate any information related to you, *[consumer name redacted]*, and the VIN mentioned in your request below. Otonomo Privacy Team will emphasize that Otonomo does not hold drivers licenses' personal details, including without limitation the names of individuals in its services' information systems. Otonomo holds names and contact details only in relation to employees, prospects and customers' representatives. Otonomo designed and operates a portal through which data subjects can exercise any of their privacy rights. To do so, we will ask you in any of your future requests to complete the form at the Otonomo Driver Privacy Rights Portal available here: <https://otonomo.io/driver-privacy-portal/> which will route your request to the Otonomo process and enable you to exercise your privacy rights. As mentioned above for your request below, the Otonomo Privacy team has searched and could not locate any information related to the details you provided in your request. Please contact us at privacy@otonomo.io if any additional support is required.

We ask that the Agency develops a process to look into companies, especially data brokers, who allege consumer data has been anonymized or deidentified and routinely use that rationale to not fulfill DSRs.

We recommend that process includes audits done by the Agency or an expert third party. Those audits should test if consumers can or cannot be reasonably reidentified from companies' "anonymized data". At Privacy4Cars we have asked several companies who denied DSRs to publicly disclose a dataset so we could test the accuracy of their statements and confirm that reidentification of consumers was not reasonable. To date, not a single company has elected to share a dataset for independent verification.

Significant friction afflicts consumers who grant authorization to Registered Agents to submit DSRs on their behalf

As stated before, Privacy4Cars California LLC is a registered agent in compliance with the requirements of CCPA. However, we have often faced pushback and sometimes insurmountable obstacles and rejection from businesses when filing DSRs. Three mechanisms we want the Commission to be particularly aware of are:

1. **Requests of a signed Power Of Attorney ("POA") by the consumer.** The authorization forms we submitted with each of the 3,908 DSRs fully comply with the requirements outlined in CCPA. We find these requests for a POA to be a "dark pattern" because not necessary, overly burdensome, costly, and result in significant friction that severely reduces the ability of California residents to assert their rights.
2. **Requirement of logging into a consumer account.** Several companies (most notably Google and Apple) require consumers to sign into their account before submitting the DSR form or to access their data. While these mechanisms may have been put in place for security purposes, they are problematic for three reasons: (1) these tech giants' policies require consumers without an account to create one for the sole purpose of exercising their CCPA rights; (2) this process effectively impedes consumers' right to authorize a third party/registered agent to submit requests on their behalf; and (3) the law clearly states that copies of consumers' fulfilled DSR results should be "delivered through the consumer's account, by mail, or electronically at the consumer's option" - hence forcing consumers to have accounts goes beyond the requirements and intent of the law. For the Agency's benefit, here are examples of responses provided by Google and Apple when inquiring about the data they collect from California consumers who drive vehicles with Android Auto and Apple CarPlay respectively enabled:
 - **Google's response:** Thank you for contacting us. Upon further review of this case, please note: We take seriously our obligation to provide information to and otherwise communicate only with the users about whom the relevant information and accounts pertain. In order to protect our users' privacy and to be sure we only share data directly with the user concerned, we can only process requests for data which are sent from the user's Google Account. Therefore, please ask the individual concerned to submit their request from the email associated with their Google Account to data-access-requests@google.com or to the local entity's email alias if the requested data is held by them.
 - **Apple's response:** The California Consumer Privacy Act provides California consumers with the right to obtain from Apple information about the personal information about you that we collect, use, and disclose. You or your authorized agent can exercise your rights by signing in to privacy.apple.com [with consumer's Apple ID]. If you cannot access Apple's online tools, you or your agent can receive assistance with your request by replying to this

email or contacting via www.apple.com/legal/privacy/contact or by calling 1-800-275-2273.

Apple's Privacy Policy can be found at: <http://www.apple.com/privacy/privacy-policy/>.

3. **Authentication Emails.** Several businesses require consumers to authenticate and receive a second factor of authentication for EVERY back-and-forth communication with the agents. As required under CCPA, we, as agents, already verified the identity and California residency of consumers before filing DSRs. Consequently it should be frowned upon that companies would ask consumers to be directly involved for email verification purposes. This process typically means (a) the company will send a second factor of authentication to the personal email of the consumer named in the DSR (b) the consumer needs to communicate the second factor to the agent, and (c) the agent has to communicate to the company the second factor – and all of this needs to be done in a very tight timeline or the second factor code expires and the process needs to re-start. It is utterly unacceptable that this second factor of authentication verification is required every time a business posts a response, considering that oftentimes it takes many rounds of communication between the agent and the company to get the DSR fulfilled. To make matter worse, it is not uncommon for these verification emails to land in the spam folder of the consumer, further aggravating the situation. This practice of requiring an email verification for every exchange should be deemed by this Agency a dark pattern that needs to be banned. Once the business has verified the identity of the consumer and validity of the DSR, keep asking to authenticate on a portal has only one effect: to introduce friction, to discourage, and to harass consumers and agents, which often results in the consumer giving up. It is our understanding that a major privacy technology provider, OneTrust, is behind many of the portals where we faced this issue.

Our hope is that the Agency will recognize these three practices listed above undermine the liberties and rights of California consumers, and speak out about the need to end them.

This Agency has the power and ability to end the opaque and large scale breach of trust and deflection of consumer rights Privacy4Cars uncovered in its automotive DSR project. My hope is the Agency will recognize that vehicles are “the third screen”, and that consumers are deserving of the same privacy when they are behind the wheel as when they are using a computer or a smartphone.

Thank you for considering these concerns. I’m available for further discussion or additional information as needed.

Sincerely,

Andrea Amico
 Founder and CEO
 Privacy4Cars
<https://privacy4cars.com>

[REDACTED]

From: **Julie Jensen** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment - Proofpoint and Rapid7 Public Comments on California Consumer Privacy Act Regulations
Date: 23.08.2022 21:49:43 (+02:00)
Attachments: Proofpoint + Rapid7 - Public Comments on California Consumer Privacy Act Regulations.docx.pdf (5 pages)

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

Dear California Privacy Protection Agency,

Please receive the attached public comments on the California Consumer Privacy Act Regulations submitted by Proofpoint and Rapid7.

Thank you.

Julie Jensen

Senior Corporate Counsel, Product

Mobile: [REDACTED]

proofpoint.

This email is confidential and was prepared by a member of Proofpoint's legal department. It contains advice of counsel and may constitute privileged communication and/or attorney work product. If you are not the intended recipient, please delete immediately and contact the sender.

COMMENTS TO CALIFORNIA PRIVACY PROTECTION AGENCY

August 23, 2022

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

Re: Comments on Title 11(6)(1): California Consumer Privacy Act Regulations

Dear Mr. Soublet,

Proofpoint is a cybersecurity company specializing in helping organizations protect against advanced cybersecurity threats and compliance risks such as identity theft, phishing, ransomware and business email compromise. As part of its cybersecurity and compliance services, Proofpoint provides and uses a global intelligence platform that gives businesses the critical visibility they need to maintain the security of their email, Cloud applications, and other IT systems, and to respond to threats against the business and its employees.

For example, with respect to email borne cybersecurity threats, the Proofpoint service detects and filters harmful content included in email messages from reaching our customers' employees (including California consumers) by helping to detect fraudulent activity and potential threats to the business systems used by those employees. Another example of Proofpoint's services are the Proofpoint security training programs that empower our customers with highly effective cybersecurity training tools in order to train their employees (including California consumers) so they know how to protect themselves (and their systems) from malicious attacks such as identity theft and impersonation. As a leading enterprise security service provider of anti-fraud and threat detection products and services, we are on the cutting edge of helping organizations protect against advanced cybersecurity threats and compliance risks, and thereby protecting the privacy of California residents and the security of their personal information.

Rapid7 provides cybersecurity solutions that help organizations strengthen their security posture with visibility, analytics, and automation. Our solutions simplify the complex, allowing security teams to work more effectively with IT and developers to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Over 10,000 customers rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. Rapid7 solutions help protect consumers and enterprises worldwide, including in California.

Strong cybersecurity is essential for consumer privacy protection, and it is critical to ensure cybersecurity activities are permitted to make proportionate use of personal information to manage security risks and incidents. To that end, Proofpoint and Rapid7 offer comments on three sections of the draft CCPA regulations (draft regulations):

- First, we address Section 7014, which provides guidance on notice obligations regarding a consumer's right to limit the use of their sensitive personal information, and we propose clarifying modifications to ensure the regulations remain consistent with Section 7027(l)(2) and (l)(3) and do not inadvertently negatively impact security services that offer the type of data protection encouraged and required by the CCPA.
- Second, we address Section 7050, where we propose the addition of anti-fraud prevention language so that service providers in the security space can adequately assist businesses with taking reasonable precautions to protect consumer personal information from security breaches.
- Third, we address Section 7051 and propose the addition of anti-fraud exemption language to allow businesses to adequately protect their systems and the customer and consumer information maintained in those systems.

I. Section 7014: Notice of Right to Limit and the "Limit the Use of my Sensitive Personal Information" Link

Proofpoint and Rapid7 appreciate the Agency's commitment to drafting proposed regulations that account for the needs of businesses to help prevent and detect security incidents and protect against malicious, deceptive, fraudulent or illegal activity. To that end, Proofpoint and Rapid7 strongly support retention of Section 7027(l)(2) and (l)(3). Section 7027(l)(2) exempts businesses from the requirements to offer consumers a right to limit the business's use and disclosure of their sensitive personal information and post a notice of right to limit in cases where the business only uses sensitive personal information to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information, provided that the use of the consumer's personal information is reasonably necessary and proportionate for this purpose. Similarly, Section 7027(l)(3) exempts businesses from these requirements when they use sensitive personal information 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. Proofpoint and Rapid7 further supports the retention of Section 7014(g), which, consistent with Section 7027(l), states that a business does not need to provide a notice of right to limit or the "Limit the Use of My Sensitive Personal Information" link if it (1) only uses and discloses sensitive personal information that it collected about the consumer for the purposes specified in Section 7027(l); and (2) states in its privacy policy that it does not use or disclose sensitive personal information for any purpose other than what is specified in Section 7027(l).

To ensure consistency with Section 7027(l)(2) and (l)(3), the Agency should consider modifying Section 7014 to expressly provide that a business is not required to honor a consumer's request to limit the use of their sensitive personal information if such sensitive personal information is only used for purposes of preventing and detecting security incidents and/or protecting against malicious, deceptive, fraudulent or illegal activity, and if such use of the sensitive personal information is necessary and proportionate to the purpose for which it was collected.

Permitting consumers to limit the use of their sensitive personal information, when such information is used for the limited purposes of maintaining the security of their information (*i.e.*, preventing and detecting security incidents and/or protecting against malicious, deceptive, fraudulent or illegal activity) is counterproductive to the purpose of the CCPA. Preventing businesses from using sensitive personal information to evolve their security systems and controls to detect and prevent against security incidents that could compromise the availability, authenticity, integrity, and confidentiality of such personal

information would create a greater risk of consumer personal information being subject to unauthorized access, acquisition or exfiltration, which would thereby limit the consumer's ability to achieve control over their personal information in the manner intended by the CCPA. If businesses are required to comply with all consumer requests to limit the use of sensitive personal information, a security service provider's ability to provide its services in a meaningful way will be dramatically limited.

II. Section 7050: Service Providers and Contractors

Section 7050(b)(4) of the draft regulations provides:

[a] service provider or contractor shall not retain, use, or disclose personal information obtained in the course of providing services except 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 perform services on behalf of another person.

Proofpoint and Rapid7 recognize the commitment the Agency has shown to further clarify security and anti-fraud protections in the current draft regulations. To that end, we encourage the inclusion of additional language that provides for a clear security use and anti-fraud exemption for service providers and contractors. We request clarifying language to capture the legislative intent behind the exemptions already codified in connection with collection and use of personal information for fraud prevention purposes. Specifically, we propose that 7050(b)(4) above be amended to include the following additional sentence after the last sentence:

Nothing in this section shall prevent a service provider or contractor from using personal information to perform services on behalf of another person where such services are provided for the purposes of preventing, detecting, or responding to data security incidents and protecting against fraudulent or illegal activity.

The use of personal information across current and future customers is a critical component for service providers in the security space. Creating an express exception that allows service providers and contractors to use personal information to prevent, detect, and respond to data security incidents and protect against fraudulent or illegal activity will ultimately allow service providers and contractors to provide enhanced security measures, services, and threat intelligence to businesses over the course of time. This would further the intent behind the CCPA by allowing security service providers to help businesses take reasonable precautions to protect consumer personal information from security breaches as required, and to notify consumers when their personal information has been compromised.

Proposition 24, also known as the "California Privacy Rights Act of 2020," which amended or reenacted the CCPA, provided that "[c]onsumers should be able to control the use of their personal information, including limiting the use of their sensitive personal information, the unauthorized use or disclosure of which creates a heightened risk of harm to consumers...." The very goal of service providers like Proofpoint is to minimize the heightened risks that consumers face when it comes to the use and disclosure of their personal information. Proposition 24 further stated that "[t]he law should be amended, if necessary, to improve its operation, provided that the amendments do not compromise or weaken consumer privacy, while giving attention to the impact on business and innovation." Amending Section 7050(b)(4) in accordance with the

language proposed above would not only help to enhance consumer privacy, but also permit business' cybersecurity programs to keep pace with cyber criminals who are constantly finding new vulnerabilities to exploit.

III. Section 7051: Contract Requirements for Service Providers and Contractors

Section 7051(a)(5) of the draft regulations provides:

[t]he contract required by the CCPA for service providers and contractors shall prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider or contractor shall be prohibited from combining or updating personal information received from, or on behalf of, the business with personal information that it received from another source unless expressly permitted by the CCPA or these regulations.

While the CCPA expressly contemplates that a "service provider *may* combine personal information to perform any business purpose as defined in the regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185..." a "business purpose" includes "[h]elping to ensure security and integrity [only] *to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes.*"¹

Although Proofpoint and Rapid7 understand the intent behind this language, we encourage the Agency to add language to Section 7051(a)(5) clarifying that a service provider or contractor is not prohibited from combining or updating personal information received from, or on behalf of, a business with personal information that it received from another source where such actions are taken for purposes of helping to ensure security and integrity and where use of the consumer's personal information is reasonably necessary and proportionate for these purposes. Such clarification would be consistent with the legislative intent behind the CCPA of helping businesses take reasonable precautions to protect consumer personal information from security breaches. It would also be consistent with the business purposes already codified within the CCPA, as amended, and would therefore serve to harmonize the draft regulations with the amended statutory provisions.

As a service provider to businesses, Proofpoint and Rapid7 process consumer personal information on behalf of businesses for the business purpose of helping to ensure security and integrity of their systems. Like other security service providers, Proofpoint aims to continuously build upon and improve its services to better protect its customers and consumers alike. Proofpoint's system requires the combination of personal information from various sources in order to develop and enhance the sophistication of its threat intelligence services. We strongly support a regulation that allows service providers to pool consumer data for security and anti-fraud purposes.

Under the CCPA, businesses are to "implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from

¹ Cal. Civ. Code § 1798.140(ag)(1)(D) (emphasis added); 1798.140(e)(2) (emphasis added).

unauthorized or illegal access, destruction, use, modification, or disclosure,"² but in order to do so, they must be able to utilize security service providers that can develop and improve their services in a meaningful and effective way, taking into consideration advances in technology and increases in cybercrimes committed by threat actors. Many businesses outsource some degree of their security operations to service providers who specialize in detecting and preventing cyberattacks. Allowing security service providers to combine and share information across customers and industries is critical to advancing the important purpose and intent behind the CCPA to protect against the unauthorized use and/or disclosure of consumer personal information. Prohibiting security service providers from combining personal information to create threat intelligence insights for businesses creates unnecessary risk for businesses and consumers alike.

The proposed language of section 7051(a)(5) limits the ability of service providers in the security space to provide effective services that will ultimately detect, prevent, and reduce cyber risks to consumer personal information. Further, such limitations on security service providers creates a conflict under the CCPA, as in order for a business to satisfy its security-related obligations under the CCPA, it must engage a security service provider that has the ability to continuously develop its services in a meaningful way to keep up with cybercriminals and advancing technology. If security service providers are incapable of providing such services due to the limitations imposed upon them, covered businesses will struggle to meet their regulatory obligations under the CCPA.

IV. Conclusion

Proofpoint and Rapid7 believe that by incorporating additional language in targeted sections of the draft regulations, the Agency has an opportunity to ensure businesses can continue to adequately protect themselves, their customers, and consumers from cyber threats.

Proofpoint and Rapid7 thank you for your time and consideration. We welcome further discussion regarding the issues raised above.



Michael Yang
Senior Vice President
and General Counsel
Proofpoint, Inc.



Raisa Litmanovich
Senior Vice President
and General Counsel
Rapid7, Inc.

² Cal. Civ. Code § 1798.100(e).

From: **David Grossman** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
CC: **Michael Petricone** [REDACTED]
Subject: CPPA Public Comment – Consumer Technology Association
Date: 23.08.2022 21:54:49 (+02:00)
Attachments: CTA CPPA Public Comments FINAL.pdf (10 pages)

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

Good Afternoon,

Attached please find the Consumer Technology Association's public comment on the California Privacy Protection Agency's July 8, 2022, Notice of Proposed Rulemaking seeking comment on proposed regulations for the California Consumer Privacy Act, as amended by the California Privacy Rights Act. These comments are timely filed ahead of the 5 PM PST deadline on August 23, 2022.

Thank you for your consideration,

J. David Grossman

Vice President, Regulatory Affairs

Consumer Technology Association, producer of CES®

d: [REDACTED]

c: [REDACTED]

[CTA.tech](https://cta.tech) | [CES.tech](https://ces.tech)

Consumer
Technology
Association



Disclaimer

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by **Mimecast Ltd**, an innovator in Software as a Service (SaaS) for business. Providing a **safer** and **more useful** place for your human generated data. Specializing in; Security, archiving and compliance. To find out more [Click Here](#).

Before the
CALIFORNIA PRIVACY PROTECTION AGENCY
 Sacramento, CA 95814

In the Matter of)
)
 Proposed California Consumer Privacy Act)
 Regulations)
)

**COMMENTS OF
 CONSUMER TECHNOLOGY ASSOCIATION**

I. INTRODUCTION

Consumer Technology Association (CTA)[®] respectfully submits these comments in response to the Notice of Proposed Rulemaking (*NPRM*) by the California Privacy Protection Agency (“CPPA” or “Agency”) on proposed regulations to implement the Consumer Privacy Rights Act of 2020 (CPRA).¹ As North America’s largest technology trade association, CTA[®] is the tech sector. Our members are the world’s leading innovators – from startups to global brands – helping support more than 18 million American jobs. CTA owns and produces CES[®] – the most influential tech event in the world. CTA and its members thus have a substantial interest in the CPPA’s work to draft and ultimately implement consumer privacy regulations.

CTA’s President and CEO Gary Shapiro observed that, in our modern economy, “consumers should know what types of data companies have about them and how that data is shared. But we also must preserve the unique ecosystem that has allowed U.S. tech companies to flourish.”² In that vein, industry is proactively taking steps to help bring more cohesion to the

¹ California Privacy Protection Agency, *Notice of Proposed Rulemaking* (July 8, 2022), https://cppa.ca.gov/regulations/pdf/20220708_npr.pdf (*NPRM*).

² Gary Shapiro, *We Need a Federal Privacy Law – Not a Patchwork of State Laws*, Morning Consult (May 6, 2019), <https://morningconsult.com/opinions/we-need-a-federal-privacy-law-not-a-patchwork-of-state-laws>.

data privacy landscape by providing businesses and consumers with an understandable baseline for data privacy practices.³ The final CPPA regulations should support, not undermine, these efforts.

CTA commented on the CPPA’s Invitation for Preliminary Comments and continues to urge that “any regulations the CPPA ultimately adopts be necessary, timely, risk-based and implementable by business, including small businesses.”⁴ The regulations should ensure sufficient protections for consumers while also providing businesses with the necessary flexibility to remain innovative and competitive. Any final rules “should not create more barriers for consumers to access the services they want, whether in the form of onerous consents, more complicated notices, or more costly products.”⁵ As the Agency finalizes its regulations, it should ensure that the rules maintain consumers’ trust while also allowing innovation that relies on the use of data collected from consumers.

The CPPA should also be mindful of how any final rules will align with existing law as well as the burdens they impose on businesses. Importantly, the adopted regulations should comport with the text of the California Consumer Privacy Act, as amended by the CPRA, (collectively, the “Statute”) and align with existing federal privacy regimes. And to achieve the best policy outcomes for both consumers and innovators, any final rules should not impose unnecessary burdens on either businesses or consumers.

³ CTA, *Guiding Principles for the Privacy of Personal Health and Wellness Information* (Sept. 19, 2019), https://cdn.cta.tech/cta/media/media/membership/pdfs/final-cta-guiding-principles-for-the-privacy-of-personal-health-and-wellness-information.pdf?_ga=2.231361119.1523449757.1660524436-2118818048.1644440199.

⁴ See Comments of the Consumer Technology Association on the Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020, at 1 (Nov. 8, 2021) (CTA Comments).

⁵ *Id.*

II. ALIGNING REGULATIONS WITH EXISTING LAWS WILL PROVIDE INNOVATORS WITH A NARROWLY TAILORED, CONSISTENT REGULATORY REGIME AND AVOID UNNECESSARY BURDENS

Greater harmonization between existing laws and the final rules will best meet both consumer and industry expectations. CTA and its members recognize the importance of actively engaging with consumers to ensure they understand how their data is being collected and used. The emerging state-by-state regulatory approach creates a patchwork of rights and obligations that hampers innovation and confuses consumers. While the CPPA proposed some positive changes to the existing regulations, the Agency should ensure that any final rules align with the Statute while also accounting for other existing privacy regimes. In addition, any final rules should avoid adding unnecessary burdens to businesses and consumers.

CTA appreciates the work that the CPPA did to propose clearer and more implementable regulations – and CTA encourages the CPPA to continue to refine the current regulations and future final rules so that businesses can easily implement them. For instance, the proposed regulations would clarify language for how offline data collectors (i.e., brick-and-mortar stores) notify consumers on opting-out of selling/sharing their personal information.⁶ In addition, the draft regulations remove confusing language regarding augmenting data from how a service provider can use personal information internally to build or improve the quality of services.⁷ These positive changes demonstrate how aligning rules with the text of the Statute is the appropriate approach to balancing the need to protect consumers with allowing industry to remain flexible. CPPA should continue to evaluate and clarify other parts of its proposed rules,

⁶ Proposed Cal. Code Regs. tit. 11, § 7013(e)(3)(A).

⁷ Proposed Cal. Code Regs. tit. 11, § 7050(b)(4); CTA Letter on Revised CCPA Proposed Regulations (Feb. 24, 2020) (explaining that the term “augmenting” does not appear in the CCPA and does not have a common understanding in the industry) (CTA Letter).

such as clarifying the meaning of “employment-related information” and what data needs to be provided in response to a Request to Know from consumers.⁸ CTA urges the CPPA to ensure that any final regulations also prioritize aligning with other privacy laws so that consumers have a clear understanding of their data privacy rights and businesses can implement deconflicted rules to protect those rights.

A. The CPPA’s Authority Is Constrained by the Text of the Statute and Any Final Regulations Must Comport with Those Limitations

As the CPPA proceeds with its rulemaking, the Agency must ensure consistency with the text of the Statute, which limits the scope of any final regulations. To that end, the final regulations must not contradict the language of the Statute, which provides the outer bounds of the CPPA’s authority. Indeed, the *NPRM* acknowledges that the CPPA must “update existing [California Consumer Privacy Act (CCPA)] regulations to harmonize them with CPRA amendments to the CCPA” as well as “operationalize new rights and concepts introduced by the CPRA to provide clarity and specificity to implement the law.”⁹ Specifically, CTA notes two examples where the proposed regulations appear to conflict with the text of the Statute and urges the CPPA to review the entirety of the proposals to ensure consistency with the Statute:

- First, the draft regulations address the global opt-out preference signals and service provider restrictions. The Statute text takes a voluntary approach to how a business recognizes global opt-out preferences signals, but the draft regulations mandate recognizing global opt-out preferences signals. In addition, the draft regulations fail to implement the Statute’s technical and disclosure requirements for such signals.¹⁰
- Second, the draft regulations include an illustrative example that purports to prohibit a service provider or contractor from “us[ing] customer email addresses provided by [a

⁸ Cal. Civ. Code § 1798.145(m)(1) (effective Jan. 1, 2023); Proposed Cal. Code Regs. tit. 11, §§ 7001(w), 7021.

⁹ *NPRM* at 5.

¹⁰ Cal. Civ. Code § 1798.135 (effective Jan. 1, 2023); Proposed Cal. Code Regs. tit. 11, § 7025(b).

business]” to then advertise to those customers.¹¹ Yet, based on the text of the law, this practice is prohibited only for “cross-context behavioral advertising.”¹² This inconsistency creates significant uncertainty with how the Statute treats the relationships between businesses and service providers with respect to advertising as well as more broadly with respect to future contracts between businesses and service providers.

These examples highlight some of the tensions that remain between the proposed regulations and the text of the Statute. To avoid imposing requirements that directly conflict with the Statute’s explicit text, the Agency should identify similar cases and resolve those contradictions as well as ensure that any final rules are consistent with its authority under the Statute.

B. The CCPA Should Harmonize Its Adopted Rules with Other U.S. Privacy Regimes

Consistent protections across technologies, companies, agencies and state borders are a bedrock prerequisite to ensure consumer trust, continue data-driven innovation and realize the benefits of such innovation. Already in the U.S., several federal and state laws seek to protect consumer privacy and ensure consumer data security. Where possible, harmonizing regulations and leveraging existing, successful practices will better ensure consumer trust and continue data-driven innovation than establishing new and different rules for California.

The *NPRM* declares that “there are no existing federal regulations or Statutes comparable to these proposed regulations.”¹³ However, this is a narrow reading of the word “comparable” because, although Congress has yet to adopt a comprehensive federal privacy law, Congress has enacted sectorial and targeted legislation.¹⁴ These regimes have set clear expectations for

¹¹ Proposed Cal. Code Regs. tit. 11, § 7050(c)(1).

¹² Cal. Civ. Code § 1798.140(e)(6); *see also* Cal. Civ. Code § 1798.140(k) (defining “cross-context behavioral advertising”).

¹³ *NPRM* at 7.

¹⁴ *See e.g.*, Children’s Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 et seq.; Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq., § 6821 et seq.; Health Insurance Portability and Accountability Act of 1996 § 1320d et seq.; Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g.

consumers on how businesses handle certain categories of information. In addition, the existing privacy regimes provided industry with well-defined and stable rules that allowed businesses to innovate while also ensuring that consumers have sufficient control over their data. For instance, the Children’s Online Privacy Protection Act (COPPA) governs how internet service providers and online platforms can collect and use personal information from children under the age of 13. Under the proposed regulations, parental consent is required for the sale or sharing of personal information for consumers under 13 in addition to COPPA requirements.¹⁵ COPPA provides a comparable federal scheme, but the proposed rules would unnecessarily impose duplicative obligations on businesses that are also addressed under COPPA. Businesses have been successfully implementing COPPA-compliant practices for many years and thus conforming the California regulations to this nationwide regime will best protect consumers.¹⁶

Since 2020, when Californians voted to amend the CCPA, Colorado, Connecticut, Utah and Virginia have enacted privacy laws that come into effect in 2023. As the first state to promulgate final rules, CPPA is uniquely positioned to ensure a foundation that avoids furthering a data privacy regulatory patchwork that is becoming increasingly burdensome and hampering innovation.

CTA urges the CPPA to account for both federal and state privacy regimes to ensure that any final rules align with those regimes as much as possible to avoid imposing duplicative and conflicting obligations on businesses.

¹⁵ Proposed Cal. Code Regs. tit. 11, § 7050.

¹⁶ See CTA Letter.

III. LIMITING REGULATIONS TO REQUIREMENTS THAT IMPOSE THE LEAST BURDEN NECESSARY ON BUSINESSES WILL MAXIMIZE RESULTS FOR CONSUMERS AND INNOVATORS

Consumers will benefit most from easy-to-understand and easy-to-implement regulations that establish a clear baseline for their data privacy rights. And businesses cannot effectively innovate if their legal obligations are not clearly set or tailored in a manner that allows businesses to comply with them efficiently. Accordingly, any final rules must avoid placing unnecessary burdens on both consumers and businesses.

As CTA previously explained, any final rules should be “necessary” and “implementable by business[es],”¹⁷ especially for innovators with smaller enterprises and start-ups. Regulatory compliance burdens not only impose costs on businesses, but consumers too.¹⁸ When inflation is at record highs,¹⁹ encouraging consumer technology is important because “historically, tech has been the biggest deflationary force in the American economy.”²⁰ Indeed, “we must pull the handbrake on government actions raising costs to consumers. We need to encourage investment in energy, reward people who work and be cautious issuing new rules imposing costs on businesses.”²¹

¹⁷ CTA Comments at 1.

¹⁸ Dustin Chambers & Courtney A. Collins, *How Do Federal Regulations Affect Consumer Prices? An Analysis of the Regressive Effects of Regulation*, Mercatus Center George Mason University (Feb. 23, 2016) (finding that an increase in regulations contributes to inflation across all income groups, but especially lower income households); *see also* Daniel Castro, Luke Dascoli, & Gillian Diebold, *The Looming Cost of a Patchwork of State Privacy Laws*, Information Technology and Innovation Foundation (Jan. 24, 2022) (estimating that California’s privacy law will annually cost the U.S. economy \$78 billion and small businesses approximately \$15 billion).

¹⁹ U.S. Bureau of Labor Statistics, *Consumer Price Index unchanged over the month, up 8.5 percent over the year, in July 2022* (Aug. 15, 2022), <https://www.bls.gov/opub/ted/2022/consumer-price-index-unchanged-over-the-month-up-8-5-percent-over-the-year-in-july-2022.htm>.

²⁰ Gary Shapiro, *The Consumer Tech Industry Can Help Combat Inflation*, LinkedIn (June 2, 2022), <https://www.linkedin.com/pulse/consumer-tech-industry-can-help-combat-inflation-gary-shapiro/>.

²¹ *Id.*

CTA encourages the CPPA to put these principles into practice. For instance, under the proposed rules, when a business denies a consumer’s deletion request, it must provide the consumer with a detailed, fact-intensive explanation as to why the business denied the request.²² Businesses must provide consumers or business partners similarly detailed explanations in other circumstances in which they are unable to effectuate a requested action in the most complete manner possible.²³ Such a requirement is unnecessarily burdensome on consumers and businesses. Requiring businesses to provide consumers with lengthy explanations when a consumer exercises their rights is unnecessarily complex and undermines the goal of providing consumers with clear explanations about how a business uses their personal data.²⁴ In addition, not only would the proposal be burdensome but, as discussed above, it is also problematic because mandating that a business explains in detail why it denied the deletion request, along with a lengthy factual basis for the denial, obligates the business to provide more information to the consumer than the Statute requires.²⁵

The draft proposals would also require businesses to maintain deletion request records for 24-months – double the general benchmark used in the Statute – when risks, necessity and other principles do not justify such a burden. The Statute, when setting forth lookback periods, consistently uses 12-month intervals²⁶ but the draft regulations would impose a 24-month recordkeeping timeframe on businesses to maintain deletion request records.²⁷ The proposal

²² Proposed Cal. Code Regs. tit. 11, § 7022 (f)(1).

²³ Id. §§ 7022(b)(3), (c)(4); 7023(f)(2); 7024(h).

²⁴ The California Privacy Rights Act of 2020, § 2(H).

²⁵ Cal. Civ. Code §1798.145 (h)(2) (requiring that a business need only provide a reason for deciding not to act on a consumer deletion request and provide the consumer with information on any rights to appeal the business’s decision).

²⁶ See, e.g., Cal. Civ. Code §1798.130(2)(B), (5)(B)-(C).

²⁷ Proposed Cal. Code Regs. tit. 11, § 7101(a).

creates risks to consumers by requiring businesses to retain records for longer than they might otherwise retain records (e.g., 12 months), contrary to the data minimization principle in the Statute.²⁸ Requiring businesses to maintain consumer deletion request records for at least 24 months obligates businesses to have a separate and unnecessary compliance timeframe for one particular rule that is not entertained by the Statute. Adopting a final rule with a 12-month record retention requirement would avoid creating risks to consumers, burdens to business and, as discussed in the previous section, disharmony with the Statute.

The proposed rules also include provisions that would impose onerous compliance burdens on businesses without providing a corresponding consumer benefit. The Statute outlines the contractual provisions that should govern relationships between businesses and service providers or third parties,²⁹ but the proposed regulations would impose new and granular requirements for these contracts, obligating businesses to redraft numerous contracts over the next few months.³⁰ These new provisions would include identifying specific business purposes for which personal information is processed, a requirement to notify a business within five days if a service provider cannot meet its obligations, a prohibition on the use of service providers for behavioral advertising and a de facto requirement to conduct due diligence of service providers, contractors and third parties.³¹ These provisions create significant expense for businesses and restrict their freedom to set contractual terms with their partners.

²⁸ See, e.g., Cal. Civ. Code § 1798.100 (requiring that a business cannot retain a consumer’s personal information or sensitive personal information for longer than is “reasonably necessary” by the business).

²⁹ Cal. Civ. Code §§ 1798.140(j), (ag).

³⁰ Cal. Code Regs. tit. 11, § 7050, 7051, 7053.

³¹ *Id.* at §§ 7051(a)(2), (a)(8), 7053(a)(1), (a)(6), 7050(c), 7051(e), 7053(e).

Finally, the proposed rules do not adequately “define the scope and process for the exercise of the agency’s audit authority,” as provided in Statute.³² An audit authority without a meaningful scope could consume significant time and resources of both the Agency and the business subject to the audit in a way that is not productive or protective of California consumers. The proposed regulations should ensure that the audit authority is more concrete and provide specific measures that businesses must take to comply with the Statute.

Any final rules should be tailored to allow businesses to provide consumers with easy-to-understand and appropriate information and options without stifling innovations or creating overwhelming compliance burdens. Necessary, timely, risk-based and implementable by business, including small businesses, rules can further the Statute’s consumer protections goals without undermining its core data privacy principles or confusing consumers.

IV. CONCLUSION

As the Agency proceeds with its rulemaking, CTA urges the CPPA to adopt rules that better align with existing laws and do not place unnecessary burdens on businesses. Doing so will provide businesses with a clear and consistent means to comply with any final regulations without hindering innovation, as well as protect consumer’s data privacy rights.

Sincerely,

/s/ J. David Grossman
J. David Grossman
Vice President, Regulatory Affairs

August 23, 2022

³² Cal. Civ. Code § 1798.185(a)(18); see also, § 1798.199.40(f).

From: **Daniella Doern** [REDACTED]
 To: **Regulations** <Regulations@coppa.ca.gov>
 CC: **Lisa LeVasseur** [REDACTED]
 Subject: CPPA Public Comment
 Date: 23.08.2022 21:58:07 (+02:00)
 Attachments: ISL Public Comment & Safety Scorecard for CPPA Rulemaking.pdf (8 pages)

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

Dear California Privacy Protection Agency,

Internet Safety Labs (formerly Me2B Alliance) is an independent software safety product testing and research organization. We create software safety standards and measure the safety of connected software. Since 2020, we've been evaluating the behavior of mobile apps and websites to measure safety and digital harms. Our non-profit organization is comprised of software engineers, policy analysts, UX experts, business, and philanthropic leaders with a vision of safe and respectful technology for all.

We applaud the Agency's tremendous efforts on the proposed California Consumer Privacy Act Regulations. We have been following the California Privacy Protection Agency's journey from its inception and have been participating throughout the rulemaking process.

We voice our support for many of the principles introduced in the proposed regulations and submit our safety scorecard to draw your attention to a few areas of concern. *Please see attached.*

Please do not hesitate to reach out to us with any questions you may have. We would be happy to assist the Agency in any way that we can.

Sincerely,

 <p>INTERNET SAFETY //LABS</p>	<p>Daniella Doern Policy Advocacy Manager</p> <p>Web: www.internetsafetylabs.org</p> <p>We've changed our name but not our mission! The Me2B Alliance is now Internet Safety Labs</p>
--	---






August 23, 2022


Introduction

The ISL Consumer Scorecard compares the text of the proposed California Consumer Privacy Act Regulations, released on July 8, 2022, against ISL regulation safety criteria listed below. Note that this scoring does not reflect the overall CPRA regulations.






Legend



ISL SAFETY SCORE	SCORE KEY
	Regulation aligns with/supports the ISL safety regulation principle.
	Regulation partially supports the ISL safety regulation principle.
	Regulation does not support the ISL safety criteria.
N/A	Not within current topics for rulemaking

Terminology Mapping


ISL Terminology	CCPA/CPRA	GDPR
<i>Data Subject</i>	"Consumer"	"Data Subject"
<i>Data Controller</i>	"Business"	"Data Controller"
<i>Data Processor</i>	"Service Providers" and "Contractors" *both added by CPRA	"Data Processor"
<i>Data Co-Controller</i>	 Not Included	"Joint Controller"
<i>Personal Information</i>	"Personal Information"	"Personal Data"
<i>Data Broker</i>	"Third Party"	"Third Party"
<i>B (business) includes Data Controller, Data Processor, Data Co-Controller, Data Broker</i>	"Business", "Service Provider", "Contractor, and "Third Party"	"Data Controller", "Data Processor", "Joint Controller", and "Third Party"

ISL CONSUMER SAFETY SCORECARD v1.0



#	ISL SAFETY CRITERIA	ISL SAFETY SCORE	CCPA REFERENCES & RATIONALE	RECOMMENDATIONS TO THE AGENCY
SAFE BY DEFAULT				
1	Regulation requires that all software be private by default.	N/A	N/A	
SAFE NOTICE PRINCIPLES				
2	Regulation requires all B-s to provide data subjects with complete & accurate notice.		§7010-7012	Consumers deserve to know the identity of the third parties that have their personal information. This knowledge would enable consumers to act on their behalf or empower trusted third parties to act on their behalf for their best interest. Without having this knowledge consumers are forced to rely on limited government resources.
a	All B-s must provide complete & accurate notices.		§7010-7011 B-s that control the collection of personal information must provide notice at collection including comprehensive description of online & offline practices.	
b	Including identification of all third-party entities that receive personal information.		§7012 Notice does not require B-s to disclose a list of all third parties. Instead, B-s are given the option to either identify third parties or provide information about the third parties' data practices within its notice.	Regulation should require B-s to list all third parties. We understand that there are situations where third parties aren't known to the B such as with the use of AdTech, which is discouraged in our ISL Safety Criteria #13 below.
3	Regulation ensures that notices are monitored & enforced.		§7300-7304 See also ISL Safety Criteria #17	
SAFE PERMISSION/CONSENT				
4	Since online "Notice & Consent" is inherently unsafe for people, regulation must ensure that "Notice & Consent" not be the sole legal basis for data processing.		§7002; §7004 B-s shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the principles listed in §7004. (Methods that do not comply may be considered a Dark Pattern). Symmetry in choice is a principle that is required for consent. Any agreement obtained with the use of dark patterns shall not constitute consumer consent.	Note that during the preliminary rulemaking activities many of us urged the Agency to rephrase the term "dark pattern." We continue to advocate for the use of "harmful pattern" instead.

			See also §7022; §7050-7051; §7052-7053	
5	Regulation requires that B-s receive uncoerced, informed permission from the data subject to use the data subject's personal information for any purpose that is inconsistent with the original purpose listed in the notice.		§7002; §7004 B-s must obtain the consumer's consent before collecting, using, retaining, and/or sharing PI for any purpose that is unrelated or incompatible with the purpose(s) for which the personal information collected or processed.	
6	Regulation requires that B-s provide data subjects with a definitive, recorded affirmation of permission(s).	N/A	N/A	
7	Regulation requires that the data subject's permissions be shared with all data processors and data co-controllers.		§7022 B-s must share consumer permissions and changes with all other service providers, contractors, and third parties. See also §7050-7051; §7052-7053	




SAFE IDENTIFICATION OF DATA SUBJECTS

8	Regulation minimizes identification of data subjects.	N/A	N/A	
9	Regulation minimizes the need for age validation by technology. If age verification must be done, it must be done in a way that is mandated to be both ephemeral and anonymous. ¹		§7070-§7072 No mention or reference of age verification.	

SAFE DATA COLLECTION

10	Regulation limits the information that a B receives from the data subject or other, observes, or derives about the data subject to what is reasonably necessary and:		§7002	
a	proportionate to the service/product provided,		§7002 The collection and use of personal information is restricted to what is reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed. To be reasonably necessary and proportionate,	




¹ Age must not be remembered, B-s must calculate age every time and forget it every session. Note that if safety principle #1 is in place, there is less of a need for age validation.

			the B-s collection, use, retention, and/or sharing must be consistent with what an average consumer would expect when the personal information was collected. <i>See also ISL Safety Criteria #5 and §7050-7051</i>	
b	proportionate to the commitment and current state of the Me2B Relationship. ² (see Fig. 1)		§7002 B-s collection, use, retention, and/or sharing of a consumer's PI may also be for other disclosed purpose(s) if they are compatible with what is reasonably expected by the average consumer.	We suggest adding another example to illustrate that the deeper the Me2B relationship, the more data collection and processing is expected. For example, the first time a user visits a retail website they have a reasonable expectation of anonymity, but later in the Me2B relationship, they create an account at that site, and expect that their behaviors may be tracked, and their experience will be personalized. (i.e., they expect to be "recognized, remembered, and personally responded to".)
11	Regulation regards any and all information that is or is likely to be correlated to a person as sensitive personal information, regardless of how it is collected.	N/A	N/A	
12	Regulation disallows B-s to maintain data about a data subject without a direct relationship ³ with that data subject.		§7050-7053 There is no requirement for a direct relationship, but the regulations do prohibit the use, disclosure, or retention of personal information obtained while providing services for any purpose, unless an exception applies. ⁴	
a	Unless the main data controller has strong and appropriate contractual management over all data processors and data co-controllers.		§7050-7053 Regulations require written contracts and establishes baseline requirements for Service Providers, Contractors, and Third Parties.	
b	Regulation includes an easy universal opt out for registered data brokers.	N/A	N/A	
SAFE DATA PROCESSING				

² Me2B Relationship refers to the relationship a user (Me) forms with a business (B) and with the products and services that the business provides. Just like human relationships, the Me2B Relationship changes over time, generally increasing in trust and intensity. The state of the Me2B Relationship is therefore crucial context for data sharing norms.

³ Direct Relationship means the data subject has an account and has entered into some kind of service agreement with the company and can thus correct/view personal information. Data Brokers typically have no direct relationship with the data subjects.

⁴ Exceptions listed in CCPA 1798.145(a)(1)-(a)(7).

13	Regulation disallows the use of data subject tracking for marketing or advertising purposes, including:		Not fully addressed in the regulation.	
a	Current RTB infrastructures.		§7052 Regulation only calls out cross contextual ads stating that cross contextual ads are not a Business Purpose for which a B & Service Provider can contract for.	The Agency's use of cross contextual behavioral ads is very narrow in scope, but it does limit the harms of current AdTech. Also, data brokers having to comply with the opt-out signal may change the behavior of AdTech for the better (especially if strictly enforced). We have concerns are about other profiling tactics, including emerging forms.
14	Regulation requires B-s that process large amounts of personal information for an ongoing period of time owe a duty of loyalty ⁵ to the data subject. Examples include social networks, email, and messaging services.		§7102 CCPA sets disclosure requirements for B-s collecting large amounts of personal information. Requirements apply only to B-s that know or reasonably should know that they sell the personal information of 10,000,000 or more consumers. The Agency's statement of reasons ties the 10,000,000 number to approximately 10% of CA's total population.	The Agency's assumption that "large" be based on large amounts of data held about a large amount of people is inadequate. It shouldn't only be about how many consumers' PI is collected. It's also about the depth of data collected in their records. Big data sets matter. We believe the Agency has authority to promulgate a duty of loyalty. ⁶ To the extent the Agency does not have the authority they should get the authority to do so. The CCPA is weaker than ADPPA here given that the ADPPA provides a duty of loyalty.





SAFE SCOPE OF REGULATION

15	Regulation must reassess what is considered "reasonable public information" in light of the internet age where data can be weaponized through scraping and aggregation at massive scale.	N/A	N/A	
16	Regulation does not exclude the following B-s from the duties of data controllers, data processors, and data brokers:	N/A	N/A	
a	non-profits,	N/A	N/A	
b	government, law enforcement, etc.	N/A	N/A	

SAFETY ENFORCEMENT

⁵ A duty of loyalty has well-established roots in the common law of fiduciaries and trusts. A hallmark of the obligation is to have no conflicts of interest between the client and third parties, and to always act in the client's best interest. Modern examples of entities with these same duties are doctors, lawyers, and certain financial advisors.

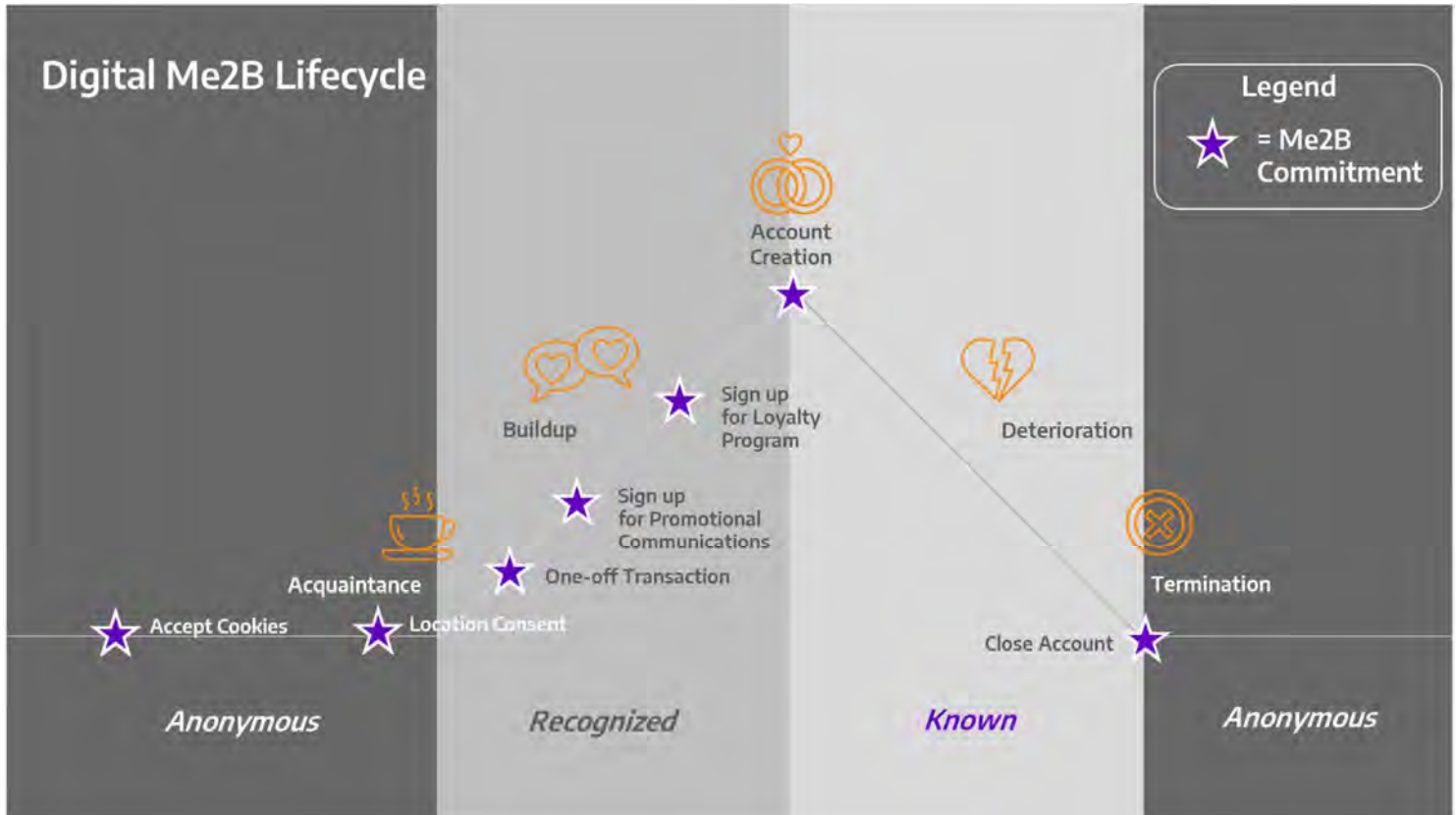
⁶ It remains unclear whether the Agency has the power to promulgate regulations on duty of loyalty during this rulemaking period.

17	Regulation provides for a practical and scalable means for ongoing enforcement of software safety regulation.		<p>§7300-7304 Agency is authorized to audit B-s, Service Providers, Contractors to ensure compliance with CCPA.</p> <p>Agency may conduct audits if the collection or processing of personal information presents significant risk to consumers privacy or security or if there is a history of noncompliance with privacy law(s). Audits may also be conducted to investigate possible violations of the CCPA.</p>	Auditing is too large a job for a single entity. It will need a network of authorized, independent, auditing entities. Authorized auditing entities must be independent organizations that are not owned, operated, or compensated by data controllers, co-controllers, data processors, or data brokers.
a	Enforcement of Business Behavior		<p>§7100-7101 ^Changes had no regulatory effect (aka nonsubstantive changes).</p> <p>See also §7102, addressed in ISL safety criteria #14.</p>	
b	Enforcement of Software/Technology Behavior		<p>§7300-7304 Auditing measures the actual behavior of the technology.</p>	
c	Regulation must provide for authorized auditing and reporting entities to support the volume of audits required to ensure compliance.		Not addressed in the regulation.	<i>See response in #17 above. We're advocating for inclusivity, transparency, and accountability in authorized auditing entities: Transparency in qualifying criteria, selection, and ongoing performance of authorized auditors.</i>

Additional Comments to The Agency

- **[§7011(e)(1)]**
 - (b) “Categories of sources” is a good start but would be much better to list the companies.
 - (e) “Categories of third parties” is inadequate; company names must be listed.
 - (g) “Actual knowledge” should be changed to “constructive knowledge” which enables efficient enforcement while minimizing age verification. The current knowledge requirement isn’t adequately robust and leaves children and minors vulnerable.
 - (i) “Categories of third parties” is inadequate; company names must be listed.
- **[§7051]** “B(6)(a)(6) Collect or sell a consumer’s personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer’s personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.”
 - Why isn’t CPPA applying the same logic as GDPR Article 3 “Territorial Scope” item 1 such that Californians would be protected regardless of whether the processing takes place in California <https://gdpr-info.eu/art-3-gdpr/>
 - In general, Californians will reasonably expect to be protected everywhere.
 - As written, these requirements could result in invasive location tracking of Californians.
 - This section is important and needs to be carefully revised.

Figure 1: Me2B Relationship & Lifecycle (referenced in ISL Safety Criteria #10b)



From: **Eric Goldman** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment from Prof. Eric Goldman
Date: 23.08.2022 14:58:18 (+02:00)
Attachments: Eric Goldman Comments to CPRA Regulations August 2022.pdf (10 pages)

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

Please see the attached PDF. Regards, Eric.

Eric Goldman (he/him)
Associate Dean for Research and Professor, Santa Clara University School of Law
Co-Director, High Tech Law Institute & Supervisor, Privacy Law Certificate
[REDACTED]



**Comments to the CPPA's Proposed Regulations
Pursuant to the Consumer Privacy Rights Act of 2020**

August 23, 2022

Brian Soublet
The California Privacy Protection Agency
2101 Arena Blvd.
Sacramento, CA 95834
By email: regulations@cppa.ca.gov

I am a tenured law professor at Santa Clara University School of Law, where I teach Internet Law and direct the school's Privacy Law Certificate. These comments represent only my views and not the views of my employer or any third party.

Section	Proposed Revisions	Explanation
7001(h)	1) Change "significantly outweighs" to "outweighs" 2) Change "the benefit provided to the consumer" to "the benefit to the consumer (as documented by credible evidence from the consumer)" 3) Add "A business need not consider any consumer benefit that is not documented by credible evidence or is obviously pretextual." 4) Delete everything after the first sentence. If not, make corresponding changes and define "adequate."	Asking businesses to evaluate consumers' benefits does not work. Businesses rarely know or can confidently guess what benefits consumers will idiosyncratically derive, and consumer self-reports of their purported "benefits" are unreliable and easily gamed. Instead of adopting my suggestions, a better approach would be to adopt a definition that doesn't depend on gauging consumer benefit at all.

Section	Proposed Revisions	Explanation
7002(a) 7002(b) 7027(a) 7027(l) 7053(a)	Replace “average” consumer with “reasonable” consumer	<p>The CADOJ proposed the “average consumer” phrase in its initial draft of the CCPA regulations, but then it backtracked when it recognized the error of its ways. It’s unfortunate that this phrase has been resurrected. As I wrote in response to the initial regulations:</p> <p>“The ‘average consumer’ standard does not represent the prevailing national approach in consumer protection law. The FTC expressly considered the appropriate standard for measuring consumer confusion in its 1983 Policy Statement on Deception. In that statement, the FTC adopted the standard of ‘a consumer acting reasonably in the circumstances.’ This standard has served consumers and the FTC well for over three decades. Among other advantages, it avoids the indeterminacy of defining what constitutes an ‘average’ consumer when a business caters to multiple heterogeneous consumer segments.”</p>
7003(c)	Replace “other” with “the smallest text-based”	Websites contain links in a variety of formats (such as text, images, and buttons) and sizes. The proposed regulation incorrectly assumes a single standard for how links are presented.
7004(a)(2)	1) Replace “symmetry” with “similarity” 2) Replace “shall not be longer” with “shall not require consumers to take more steps or actions” 3) In subpart (D), delete “more prominent (i.e.,” the end parenthesis, and “is not symmetrical”	<p>“Symmetry” implies “equality,” but it’s impossible to promote two items “equally” on a web page. By definition, one option must always be to the left of, or above, other options. Subpart (D) similarly assumes that options can have equal prominence.</p>

Section	Proposed Revisions	Explanation
7004(a)(4)	1) Define “choice architecture” 2) Delete the “guilt or shame” and “manipulative and shaming” standard 3) Define “bundles consent”	<p>The terms “choice architecture” and “bundled consent” are jargon.</p> <p>The proposed restrictions on “guilting” and “shaming” are improper. Businesses cannot control or always anticipate consumers’ subjective feelings. Furthermore, all persuasive material, including advertising, necessarily prompts consumers to think about and second-guess their choices. The regulation essentially equates standard marketing techniques with “guilting” or “shaming” techniques. Thus, the proposed standard is both indeterminate on the businesses’ side and overinclusive on the enforcement side. Standard false advertising principles of deception and unfairness can sufficiently police any abusive business practices in this situation.</p>
7004(a)(5)	1) Define “unnecessary burden or friction” 2) Define “aggressive filters” 3) Define “unnecessarily wait”	<p>These terms are jargon.</p>
7004(b)	Reconsider the definition of “dark pattern” and possibly define “user interfaces”	<p>The CPRA authorizes the CPPA to define “dark patterns” only with respect to “user interfaces.” The statute does not define “user interface,” but typically the term includes only actual “interfaces,” not every aspect of a business’ goods/service or operations. Parts of 7004(a) seem likely to reach beyond “user interfaces,” such as restrictions on a product’s “choice architecture” (whatever that jargon means). The CPPA should reevaluate if its definition of “dark patterns” stays within the scope of its authority. It may also be worth defining “user interface” to self-impose boundaries on the scope of dark patterns.</p>

Section	Proposed Revisions	Explanation
7012(f)	Delete the last sentence	Deep-linking is not always possible due to technological constraints. The requirement also assumes that a disclosure will fully address the applicable topic in a single place, but consumers often need to read the entire disclosure (including definitions, disclaimers, exceptions, and more) to properly understand any specific provision. In those cases, deeplinking will hinder consumer understanding. Also, businesses do not control the displays on consumers' devices, so scrolling may be required even if a business uses deeplinking.
7015(b)	Replace “any other” with “the smallest”	Businesses will use many different-sized icons on their website. It would not be proper to require businesses to make this opt-out icon as large as the largest icon on the page. That would clutter up pages, would not be scalable if other regulators took the same position, and would disrupt the businesses' abilities to maximize the page's helpfulness to consumers.

Section	Proposed Revisions	Explanation
7023	<p>1) In (b), replace “determines that the contested personal information is more likely than not accurate based on the totality of the circumstances” with “has a reason to believe that the requested correction may not be accurate”</p> <p>2) Delete (b)(2)</p> <p>3) Delete (d)(2)(D) or make changes similar to those mentioned in 7001(h)</p> <p>4) In part (f), add an immunity for the explanations</p> <p>5) In part (f), add a qualifier that businesses are required to append information to a record only when their database software is designed to accommodate that function.</p> <p>6) In part (f), add the following: “No explanations are required where disclosures would expose trade secrets, put the business at a competitive disadvantage, or increase the business’ risk of exposure to consumers’ attempts to undermine its policies or offerings.”</p> <p>7) Similar qualifications should be made to part (i).</p> <p>8) In part (g), delete “within the past six months of receiving the request.”</p>	<p>The proposed correction process does not follow good information governance practices. It requires businesses to “adjudicate” the truth of disputed information—but skews the businesses’ incentives towards accepting the consumer’s assertions even when the consumer may be wrong or lying. Thus, the proposed regulation facilitates the collection and propagation of inaccurate information.</p> <p>The proposed regulation stacks the decks in favor of inaccurate information. First, it says the business must accept the correction even if it has 49% doubt about the veracity. Second, it puts the burden on businesses to document and explain why they think a consumer’s correction request is fraudulent or abusive. Together, these burdens (and the associated legal risk) pushes businesses towards acquiescing to consumer correction requests, even when the business has substantial doubts about the correction’s veracity.</p> <p>When consumers manipulate these burdens to force improper corrections, it harms everyone. The corrected information will be relied upon by other businesses, and consumers can weaponize the undeserved trust in data quality to commit fraud or perpetrate public deceptions. This also puts the business at risk of legal liability if they are sharing false information that consumers forced into their databases.</p> <p>The explanations requirement further nudges businesses towards accepting improper corrections. By definition, this issue will arise only when the facts are contested, which means the businesses are already unsure of what’s the “truth.” Then, if businesses reject the correction, they will fear liability for whatever they disclose in the explanations (<i>see, e.g., Isaac v. Twitter, Inc.</i>, 557 F. Supp. 3d 1251 (S.D. Fla. 2021))—another liability risk they can avoid by acquiescing. To avoid the pro-inaccuracy implications of the explanations liability, the</p>

		<p>regulations should provide an immunity from liability for these disclosures.</p> <p>Explanations may also enable consumers to engage in adversarial behavior, such as gaming the business' policies/systems or exposing trade secrets. Explanations should not be required where those consequences are possible.</p> <p>Appending information to records should be required only when a business' database software facilitates it. Otherwise, this requirement may impose disproportionate costs on businesses because they will have to change databases to accommodate the requirement.</p> <p>Part (d)(2)(D) makes the same error as 7001(h). Businesses cannot assess the idiosyncratic impacts on consumers unless the impact has been credibly documented to them.</p> <p>Part (g) seems to authorize a consumer to reargue the exact same issue 2x/year in perpetuity, with all of the associated costs. That doesn't serve anyone's interests.</p>
--	--	---

Section	Proposed Revisions	Explanation
7025	Add a certification process before any technology is legally designated as an opt-out preference signal, and add a phase-in period for businesses to accommodate the designation	As ridiculous as it was for the California Attorney General to tweet that the CADOJ considered the Global Privacy Control to be a qualifying opt-out signal, the tweet at least provided guidance to the business community about the department's views. Without that tweet, businesses would otherwise have to guess what technologies qualify because the regulations do not provide any other official signals to businesses. The CPPA should develop a process for validating software that meets the regulatory standards, publicize its determination to the community, and give businesses an adequate period to make the technical adjustments on their side. Even tweets from the CPPA would be more helpful than the current proposed regulation.
7025(g)(2)	Delete part (C)	This provision has unintended consequences. Effectively, it requires a business to encourage consumers to adopt opt-out preference signals to communicate directly with it, but the consumer's adoption of an opt-out preference signal will affect the consumer's relationships with all businesses, not just the one business in question. In other words, a consumer's decision to adopt an opt-out preference signal just to interact with one business will have a much broader and potentially unwanted and unanticipatable effects. The proposed regulation implicitly encourages consumers to make this consequential choice with incomplete information.
7060(b)	Delete	The regulations proceed on the assumption that opt-outs or requests to limits will always be in the consumers' interests, but in fact they are weaponizable by adversaries like the other CPRA's consumer rights. Thus, these requests should be authenticated as well.
7062(d)	Delete "or correction of the spelling of a name"	Name corrections are a vector of attack for identity theft.

Section	Proposed Revisions	Explanation
7102	Delete	<p>If the CPPA wants to continue this non-statutory requirement, it should provide empirical justification that the transparency reports benefit anyone. I am unaware of any such empirical support. The initial statements of reasons makes an unsupported empirical claim that the disclosures are “necessary to inform the Agency, Attorney General, policymakers, academics, and members of the public about businesses’ compliance with the CCPA.” I trust the Agency would make that empirical claim only if it had substantial evidence demonstrating that necessity based on actual in-the-field data since the existing requirement has been in effect. Many people, including me, would like to see the Agency’s supporting evidence. Until then, the public evidence to date vitiates the purported “necessity” because the initial batch of transparency reports appeared to be useless. <i>See, e.g. Susannah Luthi, 'Functionally Useless': California Privacy Law's Big Reveal Falls Short</i>, POLITICO (Aug. 5, 2021). The likely failure of these disclosures aren’t surprising; there is an extensive literature on why mandatory disclosures fail. <i>E.g. ARCHON FUNG, MARY GRAHAM & DAVID WEIL, FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY</i> (2007); OMRI BEN-SHAHAR & CARL E. SCHNEIDER, <i>MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE</i> (2014). Failure is virtually guaranteed when a regulator doesn’t follow best practices in structuring mandatory disclosure requirements (which the CADOJ did not do). Until it can provide empirical proof of the purported “necessity,” the CPPA should abandon this section as a failed regulatory experiment.</p>

Section	Proposed Revisions	Explanation
7304	Add a requirement that any audit is authorized only when the Agency complies with applicable legal process	<p>The CPPA has a wide range of investigatory tools available to it, including information demands, administrative subpoenas, and court orders. The regulations should specify that any “audit” is permitted only after the CPPA has followed the appropriate legal process associated with the information the CPPA seeks to obtain. Any lesser standard exceeds the CPPA’s legal authority and raises major constitutional problems.</p> <p>With respect to ensuring recidivist noncompliance, the CPPA can include audit rights in any settlement or consent order. No regulation is required to implement that.</p>

Two other points beyond the proposed regulations:

First, the CPPA has already missed its statutory deadline for completing the rule-making process, and this delay ensures that businesses will not get an appropriate and fair turnaround time to implement the regulations. The CPPA should provide explicit guidance on an updated schedule for businesses’ expected compliance obligations and the CPPA’s enforcement efforts.

Second, the statement of financial impact raises several red flags about how the CPPA is justifying its regulations, including:

- The supporting economic report (which did not include the authoring firm’s name, a perhaps prudent decision given its problems) excluded businesses that are GDPR-“compliant” from its calculations.* Why? The CPPA’s Notice of Proposed Rulemaking expressly acknowledges “key differences between the GDPR and CCPA, especially in terms of how personal information is defined and the consumer’s right to opt-out of the sale or sharing of personal information (which is not required in the GDPR).” Given the CPPA’s position about the dissimilarities of the CCPA and GDPR, it is contradictory for the CPPA’s economic report to treat GDPR “compliance” as part of the regulatory baseline. Indeed, it raises questions about how the CPPA could accept the report with such a critical (and obvious) conflict with the CPPA’s own positions.
- Section B(3) of the statement of financial impact estimates that reporting businesses will incur \$2.8M in annual compliance costs. Yet, the statement of financial impact also estimates lifetime compliance with the regulations will cost \$8M total. The CPPA should explain these apparent discrepancies.
- The economic report’s estimate that it will take businesses 1.5 hours of compliance with the new regulations is not credible. It’s not possible to read and understand the 29,000+

* I do not know any privacy practitioner who would say that a company can be GDPR-“compliant” due to the ongoing and indeterminate nature of the GDPR’s requirements.

words in the proposed regulations in 1.5 hours, ** let alone actually interpret them, make judgments about which regulations require changes, and then implement those changes. As just one of dozens of possible unaccounted-for costs, businesses may need new software to accommodate the correction appending requirements, with associated (and potentially substantial) acquisition, migration, and training costs. I do not understand how the economic consultant failed to model that scenario. The failure to properly account for the true economic consequences of the proposed regulations raises obvious questions about whether this rule-making process complies with California law.

Thank you for considering my comments.

[REDACTED]
 Professor Eric Goldman
 Associate Dean for Research
 Co-Director, High Tech Law Institute
 Supervisor, Privacy Law Certificate
 Santa Clara University School of Law
 500 El Camino Real
 Santa Clara, CA 95053
 [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]

** If a reader could maintain an average reading speed of 250 words per minute, the regulations would take about 2 hours to read.

From: **Caitriona Fitzgerald** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 18:04:32 (+02:00)
Attachments: EPIC-coalition-CPPA-Comments-Round1-Aug2022.pdf (26 pages)

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

Attached please find comments from the Electronic Privacy Information Center (EPIC), the California Public Interest Research Group (CALPIRG) Education Fund, Center for Digital Democracy (CDD), Consumer Action, the Consumer Federation of America (CFA), Ranking Digital Rights, and the U.S. Public Interest Research Group (U.S. PIRG) in response to the Agency's July 8th notice of proposed rulemaking.

Please feel free to reach out with any questions.

Best,
Caitriona Fitzgerald
EPIC Deputy Director

--
Caitriona Fitzgerald (she/her)
Deputy Director
Electronic Privacy Information Center (EPIC)
202.483.1140 [REDACTED]
epic.org | [@epicprivacy](https://twitter.com/epicprivacy)

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER,
 CALPIRG EDUCATION FUND, CENTER FOR DIGITAL DEMOCRACY,
 CONSUMER ACTION, CONSUMER FEDERATION OF AMERICA,
 RANKING DIGITAL RIGHTS, AND U.S. PUBLIC INTEREST RESEARCH GROUP

to the

CALIFORNIA PRIVACY PROTECTION AGENCY
 On Proposed Rulemaking Under the California Privacy Rights Act of 2020
 (Proceeding No. 01-21)

August 23, 2022

The Electronic Privacy Information Center (EPIC), the California Public Interest Research Group (CALPIRG) Education Fund, Center for Digital Democracy (CDD), Consumer Action, the Consumer Federation of America (CFA), Ranking Digital Rights, and the U.S. Public Interest Research Group (U.S. PIRG) submit these comments in response to the California Privacy Protection Agency (CPPA)'s invitation for public input concerning the agency's development of regulations under the California Privacy Rights Act of 2020 (CPRA) and the California Consumer Protection Act of 2018 (CCPA). We commend the agency for its work to establish data privacy protections for Californians and urge the agency to include more use cases and more detail in the regulations to provide consumers and businesses clear guidance with respect to their rights and obligations.

Our Organizations

EPIC is a public interest research center based in Washington, D.C. that was established in 1994 to focus public attention on emerging privacy and related human rights issues and to

protect privacy, the First Amendment, and constitutional values.¹ EPIC has a long history of promoting transparency and accountability for information technology.²

The California Public Interest Research Group (CALPIRG) Education Fund is an advocate for the public interest. CALPIRG Education Fund speaks out for the public and stand up to special interests on problems that affect the public's health, safety and wellbeing in California.

The Center for Digital Democracy's mission is to ensure that digital technologies serve and strengthen democratic values, institutions and processes. CDD strives to safeguard privacy and civil and human rights, as well as to advance equity, fairness, and community.

Consumer Action has been a champion of underrepresented consumers since 1971. A national, nonprofit 501(c)(3) organization, Consumer Action focuses on financial education that empowers low to moderate income and limited-English-speaking consumers to financially prosper. It also advocates for consumers in the media and before lawmakers and regulators to advance consumer rights and promote industry-wide change particularly in the fields of consumer protection, credit, banking, housing, privacy, insurance and utilities.

¹ EPIC, *About EPIC* (2022), <https://epic.org/about/>.

² See Comments of EPIC et al. to Cal. Priv. Protection Agency (June 8, 2022), <https://epic.org/wp-content/uploads/2022/06/GlobalOptOut-Coalition-Letter.pdf>; Comments of EPIC and Coalition to Cal. Priv. Protection Agency (Nov. 8, 2021) <https://epic.org/documents/comments-of-epic-and-three-organizations-on-regulations-under-the-california-privacy-rights-act-of-2020/>; Comments of EPIC to Cal. Office Att'y Gen. (Feb. 25, 2020), <https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Feb2020.pdf>; Comments of EPIC to Cal. Office of the Att'y Gen. (Dec. 6, 2019), <https://epic.org/wp-content/uploads/apa/comments/EPIC-CCPA-Dec2019.pdf>; see also Comments of EPIC (Mar. 25, 2022), <https://epic.org/epic-recommends-cfpb-strengthen-buy-now-pay-later-bnpl-market-inquiry-on-customer-acquisition-and-data-practices/>; Comments of EPIC to White House Office of Sci. and Tech. Policy, Implementation Plan for a National Artificial Intelligence Research Resource (Oct. 1, 2021), <https://epic.org/documents/request-for-information-rfi-on-an-implementation-plan-for-a-national-artificial-intelligence-research-resource/>; EPIC, *AI & Human Rights* (2022), <https://www.epic.org/issues/ai/>; EPIC, *AI in the Criminal Justice System* (2022), <https://epic.org/issues/ai/ai-in-the-criminal-justice-system/>.

The Consumer Federation of America (CFA) is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education.

Ranking Digital Rights (RDR) is a non-profit research and advocacy program at New America that works to advance freedom of expression and privacy on the internet by establishing global standards and incentives for companies to respect and protect the human rights of internet users and their communities.

The U.S. Public Interest Research Group (U.S. PIRG) is a nationwide citizen advocacy group committed to serving the public interest. U.S. PIRG works for common sense solutions that make the future healthier, safer and more secure for everyone.

Below, please see our feedback on the proposed regulations. The Appendix contains specific line edits for certain provisions, particularly:

- § 7002 - Restrictions on the Collection and Use of Personal Information (A-1)
- § 7011 - Privacy Policy (A-2)
- § 7012 - Notice at Collection of Personal Information (A-3)
- § 7022 - Requests to Delete (A-3)
- § 7023 - Requests to Correct (A-4)
- § 7025 - Opt-Out Preference Signals (A-4)
- § 7026 - Requests to Opt-Out of Sale/Sharing (A-7)
- § 7027 - Prohibition Against the Use and Disclosure of Sensitive Personal Information (A-8)
- § 7050 - Service Providers and Contractors (A-12)
- § 7052 - Third Parties (A-13)

I. GENERAL PROVISIONS (Article 1)

a. Request to Opt-In to Sale/Sharing – § 7001(y)

We recommend that the definition of “request to opt-in to sale/sharing” in § 7001(y) include an illustrative example of what type of action sufficiently demonstrates “that the consumer has consented to the business’s sale or sharing of personal information about the

consumer by a parent or guardian of a consumer less than 13 years of age or by a consumer at least 13 years of age[.]” This action should require more than simply checking a box with little to no information.

b. Data Minimization – § 7002

The CPPA should not provide an exception in § 7002 to the consumer expectation standard that would degrade user privacy and experience. We urge the CPPA to amend the draft regulation implementing § 1798.100(c) of the CPRA to fully implement the law, which prohibits businesses from processing personal information in a way that is not compatible with the context in which that personal information was collected. Section 1798.100(c) reads in full:

(c) A business’ collection, use, retention, and sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.

The proposed CPPA regulations provide a useful mechanism to determine the scope of what is “reasonably necessary and proportionate” through the “reasonable consumer” standard.

However, the proposed regulations include an exception that would allow businesses to collect data for reasons beyond what a reasonable consumer expects and beyond the context in which the data was collected. Specifically, § 7002 of the draft regulations provides that:

A business shall obtain the consumer’s explicit consent in accordance with section 7004 before collecting, using, retaining, and/or sharing the consumer’s personal information for any purpose that is unrelated or incompatible with the purpose(s) for which the personal information collected or processed.

We recommend the CPPA delete this exception. This exception would incentivize data uses that are inconsistent with the data minimization restriction in § 100(c) and would likely lead to a constant barrage of consent requests, which will increase consumer consent fatigue and have the

unintended consequence of disempowering consumer rights created by the CCPA.³ Please see page A-1 for our recommended line edits to section § 7002.

II. REQUIRED DISCLOSURES TO CONSUMERS (Article 2)

a. Disclosures to Consumers – § 7010 - 7012

We support the proposal to have clear and understandable notice requirements and encourage the agency to adopt language which provides consumers more than a notice-and-choice privacy regime. Specifically, the disclosures required by the regulations provide sufficient notice to consumers of their rights, including the collection notice, opt out notice, right to limit notice, and financial incentive notice requirements. We support the requirements that the privacy policies and notices must be clearly labeled, easily understandable, and conspicuous. Please see pages A-2 to A-3 for our recommendations for edits to section § 7011 and § 7012.

III. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS (Article 3)

Please see pages A-3 to A-12 for our recommended line edits to §§ 7022, 7023, 7025, 7026, and 7027.

a. User Rights – §§ 7020 - 7024

The rules need to make clearer that both businesses and third parties have obligations to ensure that deletion and correction requests are delivered to and complied with by the third

³ Cameron Kormylo & Idris Adjerid, *Reconsidering Privacy Choices: The Impact of Defaults, Reversibility, and Repetition*, Pamplin College of Business (2021), https://www.ftc.gov/system/files/documents/public_events/1582978/reconsidering_privacy_choices_the_impact_of_defaults_reversibility_and_repetition.pdf (“Repetition of choices can introduce new decision biases; for example, (Schaub et al. 2015) find that habituation in repeated choice contexts prevents the retrieval of new information. Past literature has shown that individuals exhibit what has been termed “privacy fatigue,” where they disclose more information over time when faced with increasing complexity and less usability in privacy controls (Keith et al. 2014). Choi et al. (2018) show how privacy fatigue leads to a perceived loss of control and a sense of futility with protecting one’s privacy that results in less informed privacy decision making. This theory has also been applied to privacy and security notices (Schaub et al. 2015).”).

parties. The rules should also make clear whether written permission is something that must be given on paper or whether it may be electronic.

b. Opt-Out Preference Signals – § 7025

We urge the agency to revise § 7025(c)(7) of the proposed regulations to make it clear that a business which has received an opt-out preference signal may not prompt a consumer to confirm that preference or otherwise collect additional personal information in connection with such signal. An opt-out preference signal is by itself sufficient confirmation and authentication of the consumer's intent to opt out, which the business must honor. Absent this clarification, businesses may attempt to undermine the efficacy of opt-out preference signals by barraging consumers with confirmatory pop-ups and fomenting consent fatigue.

c. Limiting Use and Disclosure of Sensitive Information – § 7027

We recommend that the agency amend the proposed regulations in § 7027, which implement Cal. Civ. Code § 1798.121, to prohibit companies from using or disclosing sensitive data for any purpose with limited exceptions. The proposed regulations wrongly place the responsibility on the consumer to enforce data minimization and limit the use and disclosure of sensitive personal information. Companies, not consumers, should have the affirmative duty to limit the collection and use of sensitive personal information. The regulations implementing the CPRA and CPPA should impose an affirmative duty on companies to refrain from the collection or use of sensitive data with limited exceptions.

Section 7027 expressly acknowledges the heightened risk of consumer harm from the unauthorized use or disclosure of sensitive personal information, and the proposed regulations should adequately address this risk. Overbroad data collection and retention poses a significant

risk to consumer privacy.⁴ In a recent white paper, EPIC and Consumer Reports explained that excessive data collection “necessarily subjects consumers to the risk of data breaches, employee misuses, unwanted secondary uses, inappropriate government access, and can have a chilling effect on consumers’ willingness to adopt new technologies, and to engage in free expression.”⁵

Excessive data collection and retention provides companies with massive amounts of personal information that they can use, share, and disclose with few limitations. This practice is particularly harmful when it implicates sensitive personal information. A recent survey conducted by the Future of Technology Commission reflects the severity of this problem: 68% of respondents agreed “it should be illegal for private companies to sell or share information about people no matter what” and only forty-six percent agreed that it would be okay for companies to “sell consumers’ data as long as they are transparent about how the data is used and make it clear to consumers.”⁶ Personal information collected online can reveal sensitive consumer information, including sexual orientation, gender identity, sexual activities, political affiliation, and health conditions.⁷ Often this data is collected without the consumer’s knowledge and shared with data brokers or other third parties. Californians’ most urgent need is not for more notices

⁴ See, e.g., Letter from Access Now et al., to Chair Khan and Commissioners Chopra, Slaughter, Phillips, and Wilson (Aug. 4, 2021), <https://www.lawyerscommittee.org/wp-content/uploads/2021/08/FTC-civilrights-and-privacy-letter-Final-1.pdf>.

⁵ EPIC and Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (Jan. 2022) at 6, https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDDataMinimization_012522_VF_.pdf citing Justin Brookman and G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, <https://cdt.org/wp-content/uploads/2018/08/September-2013-Brookman-Hans-Why-Collection-Matters.pdf>

⁶ Benson Strategy Group, Future of Tech Commission: Tech Attitudes Survey (July 2021), https://d2e111jq13me73.cloudfront.net/sites/default/files/uploads/pdfs/bsg_future_of_technology_topline_c1-1.pdf.

⁷ EPIC & Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (Jan. 2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDDataMinimization_012522_VF_.pdf.

about their rights; it is for substantive, meaningful limitations on the use and disclosure of their sensitive personal information.

Worse yet, the proposed regulations are a further extension of the failed “notice-and-choice” regime. In the current “notice and choice” regime, consumers are expected to read vague and expansive data privacy policies, understand those policies, and make decisions to protect their own privacy. This onerous system prevents consumers from meaningfully participating in the market while protecting their privacy. Overcollection of data also poses data security risks, as security incidents and breaches are common.⁸ As written, the proposed regulations provide sensitive data the same treatment as non-sensitive data from the consumer’s perspective. The CCPA and proposed regulations recognize the heightened risk associated with the use and disclosure of sensitive personal information. Accordingly, the proposed regulation should provide heightened security for such data. The current proposal for § 7027 does not address this significant consumer harm.

Consumers should be protected from the harms associated with the collection, use, and disclosure of their sensitive personal information regardless of whether they have taken steps to prevent this harm. Instead, companies should be prohibited from engaging in this behavior. Placing the burden of action on to the consumer is not a workable solution to the problems that the CCPA and the proposed regulations seek to address. Even with constant and aggressive regulation of notice, defaults, and choice architecture, the proposed regulation for § 7027 places too much burden on consumers to vet and understand the nature of internet services and what

⁸ See Mahmood Sher-Jan, *Is it an incident or a breach? How to tell and why it matters*, IAPP (Feb. 28, 2017), <https://iapp.org/news/a/is-it-an-incident-or-a-breach-how-to-tell-and-why-it-matters> (“In today’s threat-filled world, sensitive customer information is constantly at risk for exposure. Cyberattacks, ransomware, spear phishing, malware, system & process failure, employee mistakes, lost or stolen devices — the list of dangers continues to expand. Indeed, it’s a near certainty that your organization’s customer data will be — or already has been — exposed.”).

data is being collected as they navigate their everyday lives. Our proposed additions and changes above reflect the goal of protecting consumers' sensitive personal information.

IV. SERVICE PROVIDERS, CONTRACTORS, AND THIRD PARTIES (Article 4)

a. Service Providers – §§ 7050 - 7052

We believe the regulations should clearly reflect that some companies are both service providers and third parties depending on the purposes for which they collect information in § 7050. The regulations should include additional protections to ensure that companies, including service providers and contractors, cannot retain personal information for the purposes of improving their services. To that end, we recommend that the agency specify in § 7050(b)(4) that service providers and contractors may not “retain the personal information longer than necessary.”

Further, § 7051 contains the language “unless expressly permitted by the CCPA or these regulations[,]” which is too broad. Consumers' rights under the CCPA apply even when a business contracts with service providers, secondary service providers, or tertiary service providers. The regulations therefore should enumerate the specific circumstances under which service providers and contractors may retain personal information.

We also recommend that § 7052 be updated to clarify that third parties must comply not only with deletion and opt out requests from consumers, but correction and access requests as well.

Please see pages A-12 to A-13 for our recommended line edits to section § 7050 and § 7052.

b. Contract Requirements for Third Parties – § 7053

We emphasize the importance of § 7053 and supports its adoption. This section is important to ensure that the rules and rights under the CCPA are adequately enforced and truly limit the flow of information to various entities beyond the business with which the user directly interacts. Consumers may understand the scope of their relationships with the businesses they directly interact with, but so much can happen with their personal information outside of those relationships through data transfers and sales. Section 7053 is crucial for reining in the unregulated data collection and use in the data ecosystem.

V. VERIFICATION REQUESTS (Article 5)

a. Verification Requests – § 7060

We request that the agency provide illustrative examples for § 7060(d) to demonstrate how and under what circumstances a business can request additional information to verify the identity of the requestor. With respect to § 7060(f), verification is important in certain contexts to ensure that a party who seeks to delete, request, or correct personal information is entitled and authorized to do so. We further agree with the rules in § 7060(b) that businesses may not require a consumers to verify their identity before processing opt-out requests, that businesses may only collect the limited information necessary to complete such requests, and that businesses must delete such information after it is no longer needed for that limited purpose. As noted above, we request that the agency clarify whether “signed permission” as mentioned in § 7063 must be written or electronic.

VI. NON-DISCRIMINATION (Article 7)

a. Discriminatory Practices and Calculating the Value of Consumer Data – §§ 7080 - 7081

We commend the CPPA for its inclusion of Article 7 protecting not only consumers' rights to privacy, but also their ability to exercise those rights. The non-discrimination provisions explicitly protect consumers who exercise their right to privacy from facing discriminatory price or differential service, leaving consumers free to choose privacy. The CCPA's guardrails to ensure that financial incentives practices may not be "unjust, unreasonable, coercive, or usurious in nature" are critical to ensuring that incentive programs do not provide a backdoor for businesses to coerce individuals into agreeing to waive their privacy rights. The examples in this section are particularly useful and clarify for both businesses and consumers which practices are allowed under law. Additionally, the examples make it clear that services such as loyalty programs, coupons, and discounts can still continue, even if consumers exercise their right to delete or to opt out of sale or sharing of their information. This clarification is useful because these are often popular programs that people may be concerned about losing, so explaining that these can coexist with privacy rights is important.

However, we do have some concerns about how the regulations instruct businesses to calculate the value of consumer data. We are particularly worried about the inclusion of a good-faith exception. Allowing businesses to create their own method of calculating the value of consumer data as long as it is done in good faith can result in undervaluing consumer data or valuing some consumers' data more than others. We would recommend deleting clause (8) from § 7081(a).

VII. TRAINING AND RECORDKEEPING (Article 8)

a. Training and Recordkeeping – §§ 7100 - 7101

We commend the agency for mandating training and record-keeping in the regulations. These measures are essential to ensure that employees who handle consumers' personal data are trained in how to keep data private and secure. Specifically, we support the regulations' requirement that businesses not only train employees about the provisions of the CCPA but also about how to direct consumers to exercise their rights under the law. The record-keeping requirements are particularly strong, and the agency should adopt them. Requiring businesses to record consumer requests and their responses is a vital step toward ensuring businesses comply with the requirements of the CCPA. Importantly, the record-keeping provision also requires that businesses not use this data for any purpose other than CCPA compliance and that the data not be shared with third parties. Regarding the requirements for businesses collecting large amounts of personal data, we recommend revising one of the metrics the businesses are required to disclose. Instead of allowing businesses to report either the mean or the median number of days it took to substantively respond to consumer requests, the regulations should choose one. Requiring the businesses to report this information using the same metric will make it easier to compare across businesses, identify trends in the responses to consumer requests, and ensure compliance with the regulations.

VIII. INVESTIGATIONS AND ENFORCEMENT (Article 9)

a. Investigations and Enforcement – §§ 7300 - 7304

We support the investigation and enforcement regulations and urge the agency to adopt Article 9. We commend the inclusion of multiple methods for investigation, including sworn complaints, anonymous complaints, referrals, and agency-initiated investigations. To ensure

these enforcement mechanisms operate as intended, however, we recommend adding a provision outlining who has standing to file a sworn complaint. Given California's public interest standing doctrine, standing can be fairly broad. Specifying who has standing would eliminate confusion and ensure that public interest organizations and watchdog groups can file complaints in addition to individuals. A useful way to indicate who has standing to file complaints would be to provide a few examples in the regulations, consistent with the examples given in other articles.

Conclusion

EPIC, CALPIRG Education Fund, CDD, Consumer Action, CFA, Ranking Digital Rights, and U.S. PIRG applaud the agency's open and robust rulemaking process to protect consumers in accordance with the California Consumer Protection Act. We will continue to be available for discussion about our recommendations and about how the Department can best protect Californians under the CCPA.

Respectfully submitted,

Electronic Privacy Information Center
CALPIRG Education Fund
Center for Digital Democracy
Consumer Action
Consumer Federation of America
Ranking Digital Rights
U.S. Public Interest Research Group

APPENDIX

§ 7002. Restrictions on the Collection and Use of Personal Information.

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

(b) Illustrative examples follow.

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

(2) Business B provides cloud storage services for consumers. An average consumer expects that the purpose for which the personal information is collected is to provide those cloud storage services. Business B may use the personal information uploaded by the consumer to improve the cloud storage services provided to and used by the consumer because it is reasonably necessary and proportionate to achieve the purpose for which the personal information was collected. However, Business B should not use the personal information to research and develop unrelated or unexpected new products or services, such as a facial recognition service, ~~without the consumer's explicit consent~~ because such a use is not reasonably necessary, proportionate, or compatible with the purpose of providing cloud storage services. In addition, if a consumer deletes their account with Business B, Business B should not retain files the consumer stored in Business B's cloud storage service because such retention is not reasonably necessary and proportionate to achieve the purpose of providing cloud storage services.

(3) Business C is an internet service provider that collects consumer personal information, including geolocation information, in order to provide its services. Business C may use the geolocation information for compatible uses, such as tracking service outages, determining aggregate bandwidth use by location, and related uses that are

reasonably necessary to maintain the health of the network. However, Business C ~~must~~ not sell to or share consumer geolocation information with data brokers ~~without the consumer's explicit consent~~ because such selling or sharing is not reasonably necessary and proportionate to provide internet services, nor is it compatible or related to the provision of internet services.

(4) Business D is an online retailer that collects personal information from consumers who buy its products in order to process and fulfill their orders. Business D's provision of the consumer's name, address, and phone number to Business E, a delivery company, is compatible and related to the reasonable expectations of the consumer when this personal information is used for the purpose of shipping the product to the consumer. However, Business E's use of the consumer's personal information for the marketing of other businesses' products would not be necessary and proportionate, nor compatible with the consumer's expectations. ~~Business E would have to obtain the consumer's explicit consent to do so.~~

(5) Business F is a news website that publishes articles, displays advertising in the context of such articles, and collects personal information concerning consumers' browsing habits on the website. Business G is an online ad exchange that collects information about users' browsing habits and uses that information to target cross-contextual behavioral advertising to users of Business F's website. Business F's use of data to suggest additional articles to consumers would be compatible with the consumer's expectations. However, Business F sharing browsing information with Business G for its marketing purposes would not be necessary and proportionate, nor compatible with the consumer's expectations.

(c) A business shall not collect categories of personal information other than those disclosed in its notice at collection in accordance with the CCPA and section 7012. If the business intends to collect additional categories of personal information or intends to use the personal information for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected, the business shall provide a new notice at collection. However, any additional collection or use of personal information shall comply with subsection (a)

§7011. Privacy Policy.

(e) The privacy policy shall include the following information:

- (1) A comprehensive description of the business's online and offline practices regarding the collection, use, sale, sharing, and retention of personal information, which includes the following:

(L) Identification of the specific business or commercial purpose for which the business uses or discloses sensitive personal information regardless of whether it falls within a § 7027(L) exception or not.

(M) A log of material changes retained as copies of previous versions of its privacy policy for at least 10 years beginning after the date of enactment of this Act and publish them on its website. The business shall make publicly available, in a clear, conspicuous, and readily accessible manner, a log describing the date and nature of each material change to its privacy policy over the past 10 years. The descriptions shall be sufficient for a reasonable individual to understand the material effect of each material change.

§ 7012. Notice at Collection of Personal Information.

(l) At or before the point of collection, the business shall provide a short-form notice of the categories of personal information to be collected from them, the purposes for which the personal information is collected or used, and whether the personal information is sold or shared. The business must provide a short-form notice of the business' covered data practices in a manner that is concise, clear, conspicuous, and not misleading. The short-form notice should be readily accessible to the individual, based on what is reasonably anticipated within the context of the relationship between the individual and the large data holder. The short-term notice shall be inclusive of an overview of individual rights and disclosures to reasonably draw attention to data practices that may reasonably be unexpected to a reasonable person or that involve sensitive covered data and no more than 500 words in length. The business should provide further notice by linking directly to the privacy policy. For example, a mobile app user is prompted with a short-form notice that informs them the categories of personal information to be collected from them, the purposes for which it is collected, and whether it is sold or shared the first time that the user uses the app.

§ 7022. Requests to Delete.

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

(d) If a business, service provider, ~~or~~ contractor, or third party stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose.

(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:

(4) Instruct all service providers, ~~and~~ contractors, and third parties 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.

§ 7023. Requests to Correct.

(c) A business that complies with a consumer's request to correct shall correct the personal information at issue on its existing systems and implement measures to ensure that the information remains corrected. The business shall also instruct all service providers and contractors that maintain the personal information at issue in the course of providing services to the business to make the necessary corrections in their respective systems. 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. The business shall also instruct all third parties to which it has sold or shared the personal information at issue to make the necessary corrections in their systems. Third parties shall comply with the business' instructions to correct the information and should take steps to ensure that the personal information at issue remains corrected. Illustrative examples follow.

(1) Business L maintains personal information about consumers that it receives from data brokers on a regular basis. Business L generally refreshes the personal information it maintains about consumers whenever it receives an update from a data broker. Business L receives a request to correct from a consumer and determines that the 31 information is inaccurate. To comply with the consumer's request, Business L corrects the inaccurate information in its system and ensures that the corrected personal information is not overridden by inaccurate personal information subsequently received from the data broker.

(2) Business M stores personal information about consumers on archived or backup systems. Business M receives a request to correct from a consumer, determines that the information is inaccurate, and makes the necessary corrections within its active system. Business M delays compliance with the consumer's request to correct with respect to data stored on the archived or backup system until the archived or backup system relating to the personal information at issue is restored to an active system or next accessed or used for a sale, disclosure, or commercial purpose.

(3) Business N has sold or shared personal information to a third party. Business N receives a request to correct from a consumer. Business N complies and correct the personal information in its system and notifies the third party of the correction.

§ 7025. Opt-Out Preference Signals.

(a) The purpose of an opt-out preference signal is to provide consumers with a simple and easy-to-use method by which consumers interacting with businesses online can automatically exercise their right to opt-out of sale/sharing. Through an opt-out preference signal, a consumer can opt out of sale and sharing of their personal information with all businesses they interact with online without having to make individualized requests with each business.

(b) A business shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing:

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

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

(c) When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b):

(1) The business shall treat the opt-out preference signal as a valid request to opt-out of sale/sharing submitted pursuant to Civil Code section 1798.120 for that browser or device, and, if known, for the consumer.

(2) The business shall not require a consumer to provide additional information beyond what is necessary to send the signal. However, a business may provide the consumer with an option to provide additional information if it will help facilitate the consumer's request to opt-out of sale/sharing. For example, a business may give the consumer the option to provide information that identifies the consumer so that the request to opt-out of sale/sharing can apply to offline sale or sharing of personal information. Any information provided by the consumer shall not be used, disclosed, or retained for any purpose other than processing the request to opt-out of sale/sharing.

(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 the opt-out preference signal, but may notify the consumer of the conflict and provide the consumer with an opportunity to consent to the sale or sharing of their personal information. The business shall comply with section 7004 in obtaining the

consumer's consent to the sale or sharing of their personal information. If the consumer consents to the sale or sharing of their personal information, the business may ignore the opt-out preference signal for as long as the consumer is known to the business, but the business must display in a conspicuous manner the status of the consumer's choice in accordance with section 7026, subsection (f)(4).

(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 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, 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 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. Upon receiving the opt-out preference signal, Business N shall stop selling and sharing Caleb's browser identifier for cross-contextual advertising, and shall not prompt him to confirm his choice to opt-out or otherwise collect additional personal information from Caleb. ~~But~~ ~~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) Caleb visits a browser with an opt-out browser signal enabled. Business N shall not require Caleb to provide any additional information. Business N should not prompt Caleb to confirm his choice to opt-out because it has already detected the signal expressing his preference to opt-out.

~~(B)~~ (C) Noelle has an account with Business O, an online retailer who manages consumer's privacy choices through a settings menu. 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.

~~(C)~~ (D) Noelle revisits Business O's website at a later time using a different browser that does not have the opt-out preference signal enabled. Business O knows that it is Noelle because she is logged into her account. Business O shall not interpret the absence of the opt-out preference signal as consent to opt-in to the sale of personal information.

~~(D)~~ (E) 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)~~ (F) Ramona clears her cookies and revisits Business P's website with the opt-out preference signal enabled. Business P no longer knows that it is Ramona visiting its website. Business P shall honor Ramona's opt-out preference signal as it pertains to her browser or device.

§ 7026. Requests to Opt-Out of Sale/Sharing.

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

- (1) Ceasing to sell to and/or share with third parties the consumer's personal information as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. Providing personal information to service providers or contractors does not constitute a sale or sharing of personal information.
- (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. The business shall also instruct all third parties to which it has sold or shared the personal information at issue to cease to sell and/or share the consumer's personal information. Third parties shall comply with the business' instructions to cease to sell and/or share the consumer's personal information. 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.

**§ 7027. ~~Requests to Limit Use and Disclosure of Sensitive Personal Information:~~
Prohibition Against the Use and Disclosure of Sensitive Personal Information.**

(a) The unauthorized use or disclosure of sensitive personal information creates a heightened risk of harm for the consumer. Therefore, businesses should limit the use and disclosure of sensitive personal information to what is necessary to perform the function for which it was collected with certain limited exceptions set forth in (1). ~~The purpose of the request to limit is to give consumers meaningful control over how their sensitive personal information is collected, used, and disclosed.~~ The purpose of the prohibition against the use and disclosure of sensitive personal information is to protect how consumers' 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 (1).~~ The consumer should also have the right 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, or is necessary to carry out one of the purposes set for in subsection (1). The right to limit 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).

(b) A business that uses or discloses sensitive personal information for purposes other than those set forth in subsection (l) shall provide two or more designated methods for submitting requests to limit. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the sensitive personal information that it uses for purposes other than those set forth in subsection (l), available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to limit. 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 sensitive personal information from consumers online shall, at a minimum, allow consumers to submit requests to limit through an interactive form accessible via the “Limit the Use of My Sensitive Personal Information” link, alternative opt-out link, or the business’s privacy policy.

(2) A business that interacts with consumers in person and online may provide an in person method for submitting requests to limit in addition to the online form.

(3) Other methods for submitting requests to limit include, but are not limited to, a tollfree phone number, a designated email address, a form submitted in person, and a form submitted through the mail.

(4) A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to limit because cookies concern the collection of personal information and not necessarily the use and disclosure of sensitive personal information. An acceptable method for submitting requests to limit must address the specific right to limit.

(c) A business’s methods for submitting requests to limit shall be easy for consumers to execute, shall require minimal steps, and shall comply with section 7004.

(d) A business shall not require a consumer submitting a request to limit to create an account or provide additional information beyond what is necessary to direct the business to limit the use or disclosure of the consumer’s sensitive personal information.

(e) A business shall not require a verifiable consumer request for a request to limit. A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer to whom the request should be applied. However, to the extent that the business can comply with a request to limit without additional information, it shall do so.

(f) If a business has a good-faith, reasonable, and documented belief that a request to limit is fraudulent, the business may deny the request. The business shall inform the requestor that it will

not comply with the request and shall provide to the requestor an explanation why it believes the request is fraudulent.

(g) A business shall comply with a request to limit by:

(1) Ceasing to use and disclose the consumer's sensitive personal information for purposes other than those set forth in subsection (l) as soon as feasibly possible, but no later than 15 business days from the date the business receives the request.

(2) Notifying all the business's service providers or contractors that use or disclose the consumer's sensitive personal information for purposes other than those set forth in subsection (l) that the consumer has made a request to limit and instructing them to comply with the consumer's request to limit within the same time frame.

(3) Notifying all third parties to whom the business has disclosed or made available the consumer's sensitive personal for purposes other than those set forth in subsection (l), after the consumer submitted their request and before the business complied with that request, that the consumer has made a request to limit and direct them 1) to comply with the consumer's request and 2) forward the request to any other person with whom the person has disclosed or shared the sensitive personal information during that time period.

(4) Notifying all third parties to whom the business makes sensitive personal information available for purposes other than those set forth in subsection (l), including businesses authorized to collect sensitive personal information or controlling the collection of sensitive personal information through the business's premises, that the consumer has made a request to limit and directing them 1) to comply with the consumer's request and 2) forward the request to any other person with whom the third party has disclosed or shared the sensitive personal information during that time period. In accordance with section 7052, subsection (b), those third parties and other persons shall no longer retain, use, or disclose the sensitive personal information for purposes other than those set forth in subsection (l).

(5) Providing a means by which the consumer can confirm that their request to limit has been processed by the business. For example, the business may display through a toggle or radio button that the consumer has limited the business's use and sale of their sensitive personal information.

(h) 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 presented than the other choices.

(i) A consumer may use an authorized agent to submit a request to limit on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf.

(j) A business that responds to a request to limit by informing the consumer of a charge for the use of any product or service shall comply with Article 7 and shall provide the consumer with a notice of financial incentive that complies with section 7016 in its response.

(k) Except as allowed by these regulations, a business shall wait at least 12 months from the date the consumer's request to limit is received before asking a consumer who has exercised their right to limit to consent to the use or disclosure of their sensitive personal information for purposes other than those set forth in subsection (l).

(l) The exceptions for which a business may use or disclose sensitive personal information are as follows. A business that only uses or discloses sensitive personal information for these purposes is not required to notify the consumer of the use or disclosure. The purposes for which a business may use or disclose sensitive personal information that is not necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, 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.

(1) To perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services to the customer who requests the goods or services whose sensitive personal information is being used or disclosed. For example, a consumer's precise geolocation may be used by a mobile application that is providing the consumer with directions on how to get to specific location. A consumer's precise geolocation may not, however, be used by a gaming application where the average consumer would not expect the application to need this piece of sensitive personal information.

(2) To detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information, provided that the use of the consumer's personal information is reasonably necessary and proportionate for this purpose. For example, a business may disclose a consumer's log-in information to a data security company that it has hired to investigate and remediate a data breach that involved that consumer's account.

(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.

(4) To ~~ensure the physical safety of natural persons~~ prevent an individual, or group of individuals, from suffering harm where the business believes in good faith that the individual, or group of individuals, is at risk of death, serious physical injury, or other serious health risk, provided that the use of the consumer's personal information is reasonably necessary and proportionate for this purpose. For example, a business may

disclose a consumer's geolocation information to law enforcement to ~~investigate an alleged~~ locate the victim of an alleged kidnapping to prevent death or serious physical injury.

(5) For short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business. For example, a business that sells religious books can use information about its customers' religious beliefs to serve contextual advertising for other kinds of religious merchandise within its store or on its website, so long as the business does not use the sensitive personal information to create a profile about an individual consumer or disclose consumers' religious beliefs to third parties.

(6) To perform services on behalf of the business, such as maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.

(7) To verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the business provided that the service or device being maintained, repaired, or enhanced was the purpose for which the sensitive data was being collected. For example, a car rental business may use a consumer's driver's license insofar as it is reasonably necessary to test ~~for the purpose of testing~~ that its internal text recognition software accurately captures license information used in car rental transactions. The car rental business may not use or disclose sensitive personal information beyond what is necessary to run the test and may not store the data for longer than necessary to run the test. The car rental business may not use or disclose sensitive personal information to test a separate facial recognition software that it controls.

§ 7050. Service Providers and Contractors.

(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 be deemed a service provider or contractor with regard to that person or organization for purposes of the CCPA and these regulations. 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.

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

- (1) To process or maintain personal information on behalf of the business that provided the personal information or authorized the service provider or contractor to collect the personal information.
- (2) For the specific business purpose(s) and service(s) set forth in the written contract required by the CCPA and these regulations.
- (3) To retain and employ another service provider or contractor as a subcontractor, where the subcontractor meets the requirements for a service provider or contractor under the CCPA and these regulations, provided that the service provider or contractor does not retain the personal information longer than necessary.
- (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 retain the personal information longer than necessary and does not use the personal information to 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 improve its services and offer those improved services to everyone. But the service provider cannot use the original email list to send marketing emails on behalf of another business.

(B) A shipping service provider that delivers businesses' products to their customers may use the addresses received from their business clients and their experience delivering to those addresses to identify faulty or incomplete addresses, and thus, improve their delivery services. However, the shipping service provider cannot compile the addresses received from one business to send advertisements on behalf of another business, or compile addresses received from businesses to sell to data brokers.

§ 7052. Third Parties.

(a) A third party shall comply with a consumer's request to delete, request to correct, request to know, or request to opt-out of sale/sharing forwarded to them from a business that provided, made available, or authorized the collection of the consumer's personal information. The third party shall comply with the request in the same way a business is required to comply with the request under sections 7022, subsection (b), and 7026, subsection (f). The third party shall no longer retain, use, or disclose the personal information unless the third party becomes a service provider or contractor that complies with the CCPA and these regulations.

From: **Melissa O'Toole** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
CC: **Allison Adey** [REDACTED]
Subject: CPPA Public Comment
Date: 23.08.2022 22:04:47 (+02:00)
Attachments: PIFC CPPA Regulation Comments 08232023.pdf (5 pages)

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

Good afternoon,

Attached, please find the Personal Insurance Federation of California (PIFC) comments to the CPPA's Notice of Proposed Rulemaking regarding the proposed California Privacy Rights Act (CPRA) regulations.

Can you please confirm that you have received our comments?

Thank you,

Melissa O'Toole

Legislative and Communications Manager
Personal Insurance Federation of CA

C: [REDACTED]
W: www.pifc.org
E: [REDACTED]
1201 K Street, Suite 950
Sacramento, CA 95814





Date: August 23, 2022

To: Members, California Privacy Protection Agency

SUBJECT: COMMENTS ON THE PROPOSED REGULATIONS UNDER THE CALIFORNIA PRIVACY RIGHTS ACT OF 2020

Dear Members of the Board,

The Personal Insurance Federation of California (PIFC) is a statewide trade association that represents seven of the nation's largest property and casualty insurance companies (State Farm, Farmers, Liberty Mutual Insurance, Progressive, Mercury, Nationwide and Allstate as well as associate members CHUBB, CONNECT by American Family Insurance, NAMIC and Kemper) who collectively write the majority of personal lines auto and home insurance in California.

We greatly appreciate the opportunity to provide comments regarding the proposed regulations that the California Privacy Protection Agency ("Agency") released on June 8th, 2022.

For purposes of background, we believe it is important to understand that insurance is a highly regulated industry nationally, but particularly in California. Insurers are subject to federal privacy laws under the Graham Leach Bliley Act (GLBA), and the Insurance Information and Privacy Protection Act in California specifically. Conformity with both of these privacy structures has been enforced and overseen by the California Department of Insurance up to and through this point in time.

The state's Insurance Commissioner heads the largest consumer protection agency in the United States with over 1300 staff and a \$300 million budget. Current law provides the commissioner with unrestricted access to the records, employees, officers, and contractors of any insurer. The commissioner is required to investigate the compliance of an insurer (commonly referred to as a "market conduct examination") periodically (generally every five years) but is permitted to examine an insurer at any time. Notably, insurers must reimburse the commissioner for the costs incurred conducting an examination. Few industries have the routine presence of a regulator with the power of the Insurance Commissioner.

Regarding the specific topics and questions the Agency has formulated to frame discussion, PIFC respectfully submits the following general comments to help inform future work. These are intended to be insurance industry specific comments that should be considered in addition to the comments the Agency will receive from the broader business community, which also reflect input from insurers.

Existing State and Federal Law Exemptions

Due to the extensive oversight that insurers are already subject to, a decision was made during the adoption of the California Consumer Privacy Act (CCPA) that those already subject to federal privacy law would not be subject to certain provisions of the CCPA (SB

1121 (Dodd) Chapter 735, Statutes of 2018). The importance of these exceptions was critical to ensure conformity and compliance across multiple industries. It is for those same reasons that similar exemptions exist in the American Data Privacy Protection Act (H.R. 8152), currently being considered before the House of Representatives.

Notably, the draft regulations do not have the exemption explicitly enumerated. Exemptions structured similarly to those under California Civil Code Section 1798.145 are essential to companies maintaining their compliance with other laws and reflect longstanding and complex consumer protections. The benefits of these exemptions have already been affirmed by unanimous votes on both the Assembly and Senate Floors and should not be disregarded. The CPPA draft regulation's silence on the issue of the exemptions is read by those in our organization to reflect an understanding and affirmation of the importance and necessity for those exemptions, and a continuation of those protections through the statutory codes.

Delay in Enforcement

The California Privacy Rights Act required rulemaking to be finalized by July 1, 2022 and enforcement of the rules to begin a year later *Cal. Civ. Code § 1798.185(d)*. It is understandable that there are significant demands upon the CPPA and the delay in initiating the current rulemaking. The CPPA needs to clarify its plans for enforcement and effective dates of the CPRA regulations. Only some of the anticipated regulations have been drafted, with some of the most complex and potentially complex proposed rules yet to be promulgated (*i.e.*, *Insurance Clarification section*). The Agency should clarify that enforcement, in line with the spirit of the CPRA text, make recommendations at least by July 2024, and the rules should take effect no sooner than January 2024. This will provide businesses enough time to implement the complex requirements.

On November 8, 2021, the California Department of Insurance ("Department") sent a letter to the Agency asking that "the Agency provide the Department with the opportunity to work with the Agency before the adoption of any regulation that would implement the insurance privacy subdivision of the Civil Code [Section 1798.185(a)(21)]." The Department explained that it:

Participates in the National Association of Insurance Commissioners ("NAIC"), which serves as a regulatory college and policy coordination body for the insurance commissioners of the states and territories of the United States. Among the NAIC functions is the development of Model Acts which membership may adopt. California's IIPPA is based on the NAIC Insurance Information and Privacy Protection Model Act; NAIC Model Act #670.

The NAIC is in the process of soliciting regulator and stakeholder comments on revisions to Model #670. For the last two years, CDI has participated in a working group of insurance regulators charged with determining the applicable scope of privacy protections for insurance consumers. The working group report is scheduled to be presented this December and will likely recommend amendments to Model #670. Because California's IIPPA is based on Model #670, the IIPPA will likely be amended in the next 2-4 years, after the adoption of revisions to the NAIC Model, or development of a new model. The PNPI regulations are based on the IIPPA, and are also likely to be revised. Due to the impending

amendment of applicable insurance privacy statutes, the Department respectfully requests that the Agency provide the Department with the opportunity to work with the Agency before the adoption of any regulation that would implement the insurance privacy subdivision of the Civil Code. Because the NAIC is actively working to amend Model #670, which will affect the IIPPA and related PNPI regulations overseen by [the Department], close coordination between the Department and the Agency is critical. This will avoid duplicative efforts on the part of the Agency and the Department, and promote certainty on the part of consumers and regulated entities.

The Agency and California Attorney General should declare a moratorium on enforcement of CCPA/CPRA regulations in the insurance sector until after the review and rulemaking done in connection with the above and required by 1798.185(a)(21) are completed. Because the regulations will be integral to determining how insurers must comply with the statute, the moratorium should include enforcement of the CCPA/CPRA statutory provisions.

Ideally, the moratorium should cover:

- Any enforcement activity until the insurance-specific regulations are effective; and
- Any retroactive enforcement relative to acts and omissions prior to the effective date of the regulations.

There is concern that insurers will invest significant time and resources on compliance decisions that will almost certainly need to be revisited when the insurance-specific regulations are issued. This will be confusing for Californians, who already enjoy significant privacy protections under Cal. Ins. Code § 791, *et seq.*, the related privacy regulations (10 CA ADC § 2689.1, *et seq.*), and the California Financial Information Privacy Act, Ca. Fin. Code § 4050 *et seq.* Together, these laws have, for decades, provided Californians with notice, choice, disclosure, and correction rights, not unlike those found in the CCPA/CPRA.

Notice at Collection

Proposed Section 7012(c)(5) is overly restrictive. There is no provision for the personal information that is collected over the phone or in person. When there is personal information collected in these manners a company should be able to (1) refer the consumer to the business's website for the notice at collection, or (2) offer to email or mail the notice to the consumer. The notice at collection required by CPRA, even without the proposed regulatory disclosures, is far too lengthy to be recited orally to a consumer.

Section 7012(g) creates an unreasonable burden. If a third party collects information on behalf of or with the permission of the first party, a notice at collection that is provided by the first party, together with a right to opt out, provides sufficient and meaningful protection to consumers, without overwhelming them with numerous and potentially redundant notices. Evidence has shown that the more numerous and lengthier the notices, the less likely a consumer is to read it at all. This redundant notice requirement is unnecessary and problematic.

Finally, The Proposed Regulations mandate the notice given at the time of collection to detail "the length of time the business intends to retain each category of personal

information...or if that is not possible, the criteria used to determine the period of time it will be retained.” *Proposed Regulation § 7012(e)(4)*. Such prescriptive requirements are difficult to comply with because businesses deal with various factors such as the consumer relationship, transaction duration, and other legal requirements. A specified data element could have various retention periods under the law.

Business Practices for Handling Consumer Requests

There are several issues under these sections that raise concerns for implementation to insurers.

The first being that insurers already have mechanisms and procedures in place to ensure that the information on their consumers is as up to date as possible. The procedural burdens that the regulations outline would delay and complicate the existing practice, which would harm consumers. Insurance is an industry that relies on accuracy of information at its core. Industries which already have existing structures to allow consumers to update their names, addresses, marital status, and other personal information should not be compelled to adopt a system which creates unnecessary and damaging distance and delay.

To the point above, “inaccurate information” is vague as to what information the consumer has the right to correct. Within the insurance context, while personal information such as name, date of birth, and marital status are easily updated. However, there is critical information, such as an individual’s driving record, which cannot and should not be corrected without a showing of inaccuracy by the consumer. The burden should not be placed exclusively on the insurer due to insufficient documentation. Information regarding driving records is collected and reported by the DMV, and a request to correct such information should place the burden on the consumer to show that the information is, in fact, incorrect.

Finally, throughout Article 3 of the proposed regulations there are references to business exemptions under “subsection 1” including in sections of the Article which contain no subsection 1. For clarity those sections must include clearly defined reference sections, and the exemptions included should conform with the existing exemptions under the CCPA at Civil Code Section 1798.145.

Service Providers, Contractors, and Third Parties

The requirements under Sections 7051(a) and 7053(a) for specific descriptions of services or purposes of data processing provides no greater protection to Californians than referencing contracts generically. In fact, given the potentially thousands of contracts that must be amended by a business, adding this specificity requirement will only serve to extend the time by which the business will be able to implement the required contractual amendments. The specificity requirement will frustrate an efficient means of compliance and provide absolutely no added protection to California consumers.

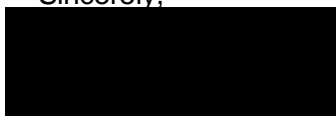
A business should not be responsible for the compliance of another entity that is not fully under their control. If there is an existing contract between two companies, one should be able to rely on a third party’s compliance with the terms of a contract unless given reason to believe that the third party is not in compliance. Section 7051(e) of the regulations places an unreasonable burden on the company to monitor third parties. This is especially true since third parties are obligated by Section 7051(d) to comply not only with the regulations, but

also the terms of the contract required by the CCPA. Section 7051(e) will only serve to mandate regular and unnecessary audit of third parties, diverting resources from more meaningful efforts to protect the privacy and security of personal information.

For insurers, the challenge of multiple regulators promulgating regulations, examining conduct, and taking enforcement actions is significant. PIFC is hopeful that the Agency will recognize the existing state and federal rules that insurers already comply with, and that avoiding unnecessary, duplicative, and conflicting regulations will be a core principle. Given the complexity and cost of compliance with CPPA and CPRA, our members also seek flexibility wherever possible and appropriate.

We look forward to working collaboratively with the Agency and Board to develop fair regulations that can be implemented in a manner that best serves Californians.

Sincerely,



Allison Adey
Legislative Advocate
Personal Insurance Federation of California



Christian J. Rataj
Senior Regional Vice President
National Association of Mutual Insurance
Companies

From: **Hayley Tsukayama** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 22:05:13 (+02:00)
Attachments: 2022.08.23 - CPPA Comments.pdf (15 pages)

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

Good afternoon,

Attached please find the joint comments of the Electronic Frontier Foundation, ACLU California Action, Privacy Rights Clearinghouse, Oakland Privacy, Media Alliance, Consumer Federation of America, Access Humboldt, and Consumer Action.

If you have any questions, please reach out to me, Hayley Tsukayama at [REDACTED] Thank you and have a wonderful day.

Sincerely,
Hayley Tsukayama

--

Hayley Tsukayama
Senior Legislative Activist
CIPP/US

Electronic Frontier Foundation | San Francisco, CA

<https://www.eff.org/>

Pronouns: she/her



Privacy Rights
Clearinghouse



**MEDIA
ALLIANCE**



Consumer Federation of America

consumer action
Education and advocacy since 1971

COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION, ACLU CALIFORNIA ACTION, PRIVACY RIGHTS CLEARINGHOUSE, OAKLAND PRIVACY, MEDIA ALLIANCE, CONSUMER FEDERATION OF AMERICA, ACCESS HUMBOLDT, AND CONSUMER ACTION

to the

CALIFORNIA PRIVACY PROTECTION AGENCY
On Proposed Rulemaking Under the California Privacy Rights Act of 2020
(Proceeding No. 01-21)

August 23, 2022

Introduction

Our groups are writing in reply to the invitation issued by the California Privacy Protection Agency (“the Agency”) seeking input from stakeholders in developing regulations as directed by the California Privacy Rights Act (CPRA), and the California Privacy Protection Act (CCPA) as modified by the CPRA.

About The Parties

The **Electronic Frontier Foundation** (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. With over 35,000 dues-paying members (with several thousand California members) and well over 1 million followers on social networks, we focus on promoting policies that benefit both creators and users of technology. EFF has engaged in discussions around privacy regulations in California and throughout the country at the state and federal level. EFF has previously submitted comments to the California Attorney General regarding rulemaking for the California Consumer Privacy Act (CCPA), both as an individual organization and in collaboration with other leading privacy advocacy organizations.

ACLU California Action protects civil liberties and civil rights, advances equity, justice, and freedom, and dismantles systems rooted in oppression and discrimination. ACLU California Action has an abiding interest in the promotion of the guarantees of individual rights embodied in the federal and state constitutions, including the right to privacy guaranteed by the California Constitution and the right to due process. ACLU California Action is a 501(c)(4) organization

associated with the three ACLU affiliates in California—ACLU of Northern California, ACLU of Southern California, and ACLU of San Diego and Imperial Counties.

Privacy Rights Clearinghouse is focused on increasing access to information, policy discussions and meaningful rights so that the right to data privacy can be a reality for everyone. Founded in 1992 to help people understand their rights and choices, it is one of the first and only organizations to focus exclusively on data privacy rights and issues. For three decades, our team has been driven by the beliefs that data privacy is a fundamental human right and essential for an equitable future, and that everyone deserves the opportunity to be informed and be heard.

Oakland Privacy is a citizen's coalition that works regionally to defend the right to privacy, enhance public transparency, and increase oversight of law enforcement, particularly regarding the use of surveillance techniques and equipment. As experts on municipal privacy reform, they have written use policies and impact reports for a variety of surveillance technologies, conducted research and investigations, and developed frameworks for the implementation of equipment with respect for civil rights, privacy protections and community control.

Media Alliance is a Bay Area democratic communications advocate. Our members include professional and citizen journalists and community-based media and communications professionals who work with the media. Our members are concerned with communications rights, especially at the intersections of class, race and marginalized communities.

The **Consumer Federation of America** (CFA) is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education. Today, more than 250 of these groups participate in the federation and

govern it through their representatives on the organization's Board of Directors. CFA is a research, advocacy, education, and service organization. As an advocacy organization, CFA works to advance pro-consumer policies on a variety of issues before Congress, the White House, federal and state regulatory agencies, state legislatures, and the courts. We communicate and work with public officials to promote beneficial policies, oppose harmful ones, and ensure a balance debate on issues important to consumers.

Access Humboldt is a non-profit, community media & broadband access organization serving the residents and local jurisdictions of Humboldt County on the North Coast of California USA, managing resources that include: streaming channel online; cable access TV channels; KZZH FM 96.7 community radio; media collection on Community Media Archive; a wide area broadband network with dedicated optic fiber connections to twenty locations serving local jurisdictions and community anchor institutions; broadband access wireless networks; a Community Media Center with studio and other production equipment and training on the College of the Redwoods campus; and ongoing operational support for public, educational and governmental access media services.

Consumer Action has been a champion of underrepresented consumers since 1971. A national, nonprofit 501(c)(3) organization, Consumer Action focuses on financial education that empowers low to moderate income and limited-English-speaking consumers to financially prosper. It also advocates for consumers in the media and before lawmakers and regulators to advance consumer rights and promote industry-wide change particularly in the fields of consumer protection, credit, banking, housing, privacy, insurance and utilities.

Data Minimization Language Rightly Centers Consumer Expectations in § 7002

Data minimization is a key tool for consumer protection, as it both ensures businesses are not over-collecting information and ensures that data collected from consumers aligns with their expectations. The Agency should set the standards for consumer rights based on consumer expectations—otherwise, such rules risk being counter to the goals of true data minimization. Establishing this frame ensures that consumers are not surprised by how their information is collected, used, or retained.

The proposed regulations language rightly establishes that the minimization standard should be “consistent with what an average consumer would expect when the personal information was collected.” Similarly, it states clearly that if businesses seek to use information for another disclosed purpose, such purpose must be “compatible with what is reasonably expected by the average consumer.”

We also appreciate the illustrative examples the Agency has outlined, which further clarify what consumers can expect in real-world applications that are easy for the average person to understand.

In particular, the example stating that a cloud-storage provider may not use personal information uploaded by a consumer to “improve cloud storage services” to “research and develop unrelated or unexpected new products or services, such as facial recognition...” without explicit consent. This is a clear and important marker to lay down in the name of consumer protection. Businesses are not the sole arbiters of what “improving” services may look like, and should have strictly limited latitude to repurpose information they have already collected for other purposes.

It is also good that the examples expressly say that businesses, such as internet service providers, that collect information to administer services, should not sell information to data brokers without a consumer's express consent. This makes clear that information is important to the consumer, and not merely another asset for a business to mark on a ledger.

While—to be most protective of consumer information—we would rather see businesses only collect information that is “necessary” or “strictly necessary” to the purposes consumers ask for, we understand that is not the standard set in current law. As such, the regulations clarify the statutory language in a way that protects consumers. Company expectations should not be the yardstick by which we measure what a related purpose may be. The proposed regulations recognize that consumer expectations should be the yardstick.

Dark Patterns Language in § 7004

We supported the proposed regulations from the California Department of Justice (DOJ) to protect against deceptive or coercive design choices, which are commonly called “dark patterns,” in their proposal published October 12, 2020—specifically at Section 999.315(h), within the third set of proposed modifications of CCPA regulations, which the California DOJ published on October 12. Specifically, these regulations:

Require opt-out processes to be “easy” and “require minimal steps.”

Ban opt-out processes “designed with the purpose or having the substantial effect of subverting or impairing a consumer's choice to opt-out.”

Limit the number of steps to opt-out to the number of steps to later opt back in.

Ban “confusing language” such as “double negatives” (like “don’t not sell”).

Ban the necessity to search or scroll through a document to find the opt-out button.

The Agency's proposed rules build on this foundation substantially by adding more detail and language responsive to how consumers are often asked to make privacy choices in the real world.

Not only must businesses make sure their instructions are easily understandable, they also must have symmetry in choice and make clear design choices. This is important to specify in regulations, as companies too often seek to confuse or even shame people into making a decision that works against their own privacy interests or preferences. It is also important for these regulations to state that exercising one's privacy rights should not be limited by unnecessary bureaucratic or administrative steps.

The Draft Regulations Inappropriately Introduce “Frictionless” and “Non-Frictionless” Processing of Opt-Out Preference Signals in § 7025(e)

Opt-out preference signals allow consumers to easily exercise their privacy choices by configuring a single setting that automatically expresses that privacy choice when they visit a business's website or use an app. This mechanism was present in the California Consumer Privacy Act (CCPA) regulations issued by then-Attorney General Becerra and was reinforced in the California Privacy Rights Act (CPRA) supported by a majority of California voters later that year.¹

Proposition 24 changes the legal relationship between opt-out preference signals and the requirements to include prominently placed “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links on the business's website.²

¹ 11 CCR § 7026(a); *see also* Cal. Civ. Code §1798.135(b)

² Cal. Civ. Code §1798.135(b)(1),(3).

The Draft Regulations state in Section 7025(e), “Civil Code section 1798.135, subdivisions (b)(1) and (3) provides a business the choice”; a business can process opt-out preference signals in a “frictionless manner” or the business can elect to include those conspicuously placed links and are then permitted to process opt-out preference signals in a “non-frictionless manner.”³ The draft regulations later describe what is permitted when businesses process opt-out preference signals in a “non-frictionless manner” by defining a “frictionless” processing in section 7025(f) as prohibiting: (1) charging a fee or requiring valuable consideration if the consumer uses an opt-out preference signal, (2) changing the consumer’s experience with the product or service, or (3) displaying a notification, pop-up, text, graphic, sound, video, “or any interstitial content” in response to an opt-out preference signal.⁴

“Non-frictionless” is not defined, but the draft regulations suggest that the “friction” could include all of these consumer-hostile tactics: charging consumers a fee, degrading their service or experience, and badgering them with pop-ups, videos, and other interstitial content.

The concepts of “frictionless” and “non-frictionless” processing are not present in the CCPA, its current implementing regulations, or the CPRA. In creating these categories, the Agency risks enshrining in regulation discriminatory and harmful business practices.

By implicitly validating “non-frictionless” processing of an opt-out preference signal, the regulations threaten to open the floodgates of deceptive and manipulative design from companies who will take every opportunity to deprive consumers of their privacy and their ability to make simple choices to protect themselves.

³ Draft Regulations § 7025(e)

⁴ Draft Regulations §7025(f)

We oppose this proposed framework and recommend striking the concept “non-frictionless processing” from the draft regulations. When a business processes an opt-out preference signal, that processing must be done in a manner that comports with the requirements and principles outlined in the law. Businesses cannot be permitted to markedly degrade the consumer experience of those using opt-out preference signals simply because the business elected to include conspicuous privacy links on their homepage and privacy policy.

“Non-frictionless” Processing in 7025(e) Authorizes Privacy Dark Patterns.

In addition, permitting businesses to interpret opt-out signals in a “non-frictionless” manner would invite the very same dark patterns that the draft regulations aim to prohibit. A business that posts the necessary conspicuous links is not subject to the prohibitions in § 7025(f). As a result, under the regulations, businesses could apparently add popups or interstitial graphics responding to a user’s opt-out signal. These popups could prompt the user that the business will charge the user a fee to continue using the website with their opt-out signal still enabled. And even after the user gets past the pop-ups, they could be redirected to a site that is different than one for a user without an opt-out signal enabled.

This user experience is not in the letter or the spirit of § 7004. This section gives us the five principles for obtaining user consent and outlines what may constitute a dark pattern. In § 7004(a)(2), the Symmetry in Choice principle states that “the path for a consumer to exercise a more privacy-protective option shall not be longer than the path to exercise a less privacy-protective option.” However, a business adding friction after recognizing an opt-out signal is not symmetrical in choice because it would make the path to a website longer for someone with an opt-out signal enabled.

Even the double-negative phrase “non-frictionless” violates the regulations caution in § 7004(a)(3) to “[a]void language or interactive elements that are confusing to the consumer,” which notes in particular, “the methods should not use double negatives.”

Further, § 7004(a)(5) states that CCPA requests should be easy to execute, and that businesses shall not add unnecessary burden or friction. However, § 7025(e) says exactly the opposite, that businesses can add friction when responding to an opt-out signal if they are authorized to do so in a “non-frictionless manner.” Finally, § 7004(c) states that a dark pattern is an interface that “has the effect of substantially subverting or impairing user autonomy, decision-making, or choice.” A user with an opt-out signal has expressed a clear intent to exercise their privacy rights. Adding friction to that process that has the effect of substantially subverting the user’s intent is a dark pattern.

For this reason and the others listed, we object to the inclusion of a “non-frictionless” form of permitted processing, which would have the effect of undermining the intent and purpose of opt-out preference signals and validate dark patterns as an approved business practice.

Definition of Disproportionate Effort in § 7001 (h)

We are concerned that the definition of disproportionate effort added to § 7001 (h) allows the projected benefit to the consumer to be completely defined by the business rather than by the consumer. This is an especially acute issue when the personal information in question is sensitive information as defined by the statute.

If inaccurate data causes a consumer to miss a business opportunity, be denied a loan or a job, the consequences or damages experienced by the consumer may be exceptionally high, if not

fundamentally unlimited, and it isn't clear that a business would be aware of, or able to accurately measure, the benefit to the consumer or the potential lifelong ramifications.

The model also sets up a power dynamic that allows the business to set the terms of the projected benefit to the consumer as measured against their own effort. We question whether having businesses "tell people" how much they benefit is consistent with the overall intention of CCPA and CPRA to put consumers in the driver's seat regarding how their personal information is handled.

We recommend that, at a minimum, the Agency consider whether setting some floors on the minimum amount of effort that can be claimed to be disproportionate to a consumer's benefit and that such a floor may not be the same for sensitive data as for non-sensitive data. Similarly, the process of using a disproportionate effort claim to refuse a consumer request should have an input mechanism for a consumer to understand the business' interpretation of the benefit to them and to add additional information if needed to understand the true nature of their request.

That said, it remains unclear to us what happens if a business informs a consumer that their request will not be fulfilled because the effort to the business is disproportionate to the benefit they will receive, and the consumer disagrees with that assessment by the business.

Financial Incentives in §7016

Section §7016 addresses financial incentives that businesses offer to consumers to hand over their personal information to the business. This practice is commonly referred to as pay-for-privacy as the net effect on the consumer is often paying a higher price for a good or service if they choose not to participate.

The potential dangers of widespread Pay-For-Privacy programs is that affluent consumers will retain the full ability to opt-in or opt-out as they choose, and less affluent consumers will be unable to afford the increased costs incurred by a choice to opt-out. We encourage the Agency to keep this dystopian scenario in mind as businesses move into full compliance with CCPA/CPRA and be prepared for further rulemaking within the limits of the statutory language to protect the rights of consumers without financial means to fully use the privacy rights granted to them without excessive financial punishment.

Pay-for-Privacy programs can range from the benign (one free latte after buying ten at your favorite coffee house) to the considerably less so: for example, Amazon's \$10 per palm print offer which trades checkout speed at Amazon Go outlets for the dubious benefit of building out a biometric database for the gigantic online retailer with its many ties to law enforcement.⁵

We were disappointed to see the draft regulations by the Agency leave mostly untouched the extreme license given to businesses to compute "the value of the customer's data" according to seemingly almost any formula or method that they choose. The lack of specific guidance will likely result in a crazy-quilt assortment of methods that will be used to measure the value of the customer's data to the business. The statute requires the incentive to be "reasonably related" to the figure the company provides, but neither the statute itself nor these regulations provide a standard to ensure that the value number itself is reasonable. For a financial incentive to be reasonably related to an unreasonable value computation seems neither reasonable nor protective to consumers.

⁵ See <https://techcrunch.com/2021/08/02/amazon-credit-palm-biometrics/>

This section of the statute is in tension with the data minimization precepts in other parts of the law. This tension is perhaps accentuated by the strong data minimization language the Agency proposed adding in these draft regulations. If no data is to be collected other than what a reasonable customer would expect is needed to provide the service and product the consumer has requested, then the value of the data to the business is, by definition, somewhat constrained.

To cite the example provided above, Amazon has assigned a financial incentive of \$10 to the opt-in acquisition of a biometric palm print to aid in rapid check-out at Amazon Go locations. The figure of \$10 is thus nominally “reasonably related” to the value of the biometric palm print to Amazon. But what does these \$10 (or thereabouts) value to Amazon consist of? Does it really benefit Amazon at a rate of \$10 per consumer to check a customer out of their store with a palm print instead of a scan of a debit or credit card? Certainly, there may be some labor savings, but they could not add up to \$10 per customer. The value is connected to the acquisition of the palm print for other business purposes besides checking out of Amazon Go stores, which then demands the question of whether those other business purposes are consistent with what a reasonable customer would expect.

We recommend that the Agency consider providing some sample computations of the value of a consumer’s data to a business, as you have provided examples in a number of other sections of the draft regulations. The examples can and should include an example of a reasonable method to arrive at a value number as well as an example of an unreasonable method. The examples should also include acceptable additional business purposes for acquired customer data that clearly meet the “reasonable consumer expectation” standard and examples of those that would not meet the “reasonable consumer expectation” standard.

Amendment Provision of CPRA

We additionally suggest the Agency create specific language to govern the future of privacy legislation more clearly in California. The ballot initiative language of “in furtherance of privacy” is very general, and we have already seen significant questions arise over various legislative proposals by the Legislature. We can only assume that will be exacerbated in coming years; especially as innovative technologies stretch existing privacy definitions. The Legislature has already passed some legislation that we are dubious met the standard of “in furtherance of privacy”, for example AB 335 in 2021.⁶

Supplemental language that addresses specifically empowering consumers to have more control over the handling of their personal information might provide a clearer frame for what kinds of legislation are included in the “furtherance of privacy” and what kinds are not. The Legislature will want and deserves some level of discretion, but the bottom line is that CPRA was a ballot initiative that promised voters that the privacy protections they were voting for could not be weakened or watered down. It is incumbent on the Agency to make sure that promise is kept.

s/

Hayley Tsukayama, Electronic Frontier Foundation

Becca Cramer-Mowder, ACLU California Action

Jacob Snow, ACLU California Action

Emory Roane, Privacy Rights Clearinghouse

⁶ See https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202120220AB335

Group Comments
re: Proceeding No. 01-21
Page 15 of 15

Tracy Rosenberg, Oakland Privacy and Media Alliance

Susan Grant, Consumer Federation of America

Sean Taketa McLaughlin, Access Humboldt

Ruth Susswein, Consumer Action

From: **Bartolotta, Kristen** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
CC: [REDACTED]; **Benway, Kathleen**
Subject: CPPA Public Comment
Date: 23.08.2022 22:08:29 (+02:00)
Attachments: CTIA - 082322 Comment on First Set of CPRA Regulations.pdf (38 pages)

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

To whom it may concern,

On behalf of CTIA, please see the attached written comments on the July 8, 2022 Proposed Regulations.

Best regards,
Kristen

Kristen E. Bartolotta
Associate
ALSTON & BIRD
950 F Street, NW
Washington, DC 20004
[REDACTED] (O)
[REDACTED] (M)

Admitted to practice in New York. Admission pending to the DC Bar.

NOTICE: This e-mail message and all attachments may contain legally privileged and confidential information intended solely for the use of the addressee. If you are not the intended recipient, you are hereby notified that you may not read, copy, distribute or otherwise use this message or its attachments. If you have received this message in error, please notify the sender by email and delete all copies of the message immediately.

Before the
California Privacy Protection Agency

In the Matter of

California Privacy Rights Act of 2020
 Rulemaking Process

)
)
)
)
)
)

Invitation for Comments on
 Proposed Rulemaking

COMMENTS OF CTIA

Gerard Keegan
 Vice President, State Legislative Affairs

Avonne Bell
 Director, Connected Life

Jake Lestock
 Director, State Legislative Affairs

CTIA
 1400 16th St. NW, Suite 600
 Washington, DC 20036
 (202) 736-3200
www.ctia.org

August 23, 2022

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION.....	4
I. A Number of Proposed Regulations Exceed the Agency’s Authority.....	7
A. § 7002: Restrictions on the Collection and Use of Personal Information (Consumer Expectations Requirement)	7
1. Notices to Consumers, not a Hypothetical “Average Consumer” Standard, are CPRA’s Means for Setting Consumer Expectations and Permissible Uses	7
2. An “Average Consumer Expectations” Test will Cause Arbitrary Enforcement unless Privacy Notices Serve as the Benchmark for What Consumers Expect.....	9
B. § 7002: Restrictions on the Collection and Use of Personal Information (Consent Requirement)	10
1. The Agency Lacks Statutory Authority to Issue a General Consent Requirement for New Data Uses	10
2. Requiring Consent for any New Uses “Unrelated to or Incompatible With” Consumer Expectations Conflicts With CPRA’s Statutory Text and Scheme, Which Uses Notices at Collection – not Consent – to Enable Consumers to Control New Data Uses	12
3. The Agency’s Consent Requirement for Data Use “Unrelated To” the Purposes for Which it was Collected Could Potentially Harm Consumers.....	13
C. § 7011: Privacy Policies.....	14
D. § 7025: Opt-Out Preference Signals	16
1. Requiring All Companies to Process Opt-Out Preference Signals – Even if they Post a “Do Not Sell/Share” Link – Exceeds the Agency’s Authority.....	16
2. The Agency has Failed to Provide Specifications for an Opt-Out Preference Signal, as well as Rules Governing Companies that Develop Opt-Out Preference Technologies. Businesses Should thus not be Required to Process Opt-Out Preference Signals.....	17
E. § 7012(g)(3): Notices at Collection of Personal Information (Third Parties that Control the Collection of Personal Information)	19

1.	The Agency’s Notice Rules for Third Parties That Control the Collection of Personal Information Conflict With CPRA, Which Only Requires Third Parties to Display Notices at Collection When Acting on Their Own Premises.....	20
2.	The Draft Regulations Do Not Let Businesses Know When They Will be Considered a “Third Party That Controls” Data Collection. The Agency’s Illustration Increases Confusion, Instead of Providing Clarity.....	21
F.	§ 7050: Service Providers and Contractors.....	23
1.	The Draft Regulations Should Clarify That the Same Company Can Provide Some of its Services as a “Service Provider,” While Also Providing Cross-Context Behavioral Advertising Services as a “Third Party.”	23
2.	Requiring Service Provider Agreements to Enumerate “Specific” Business Purposes Exceeds CPRA’s Statutory Text and may Inadvertently Interfere with Contract Negotiations.	24
II.	Agency Audit Provisions Under § 7304 Lack Specificity and Safeguards	25
A.	The Draft Regulations Have Failed to Define the “Scope and Process” for Agency Audits, as well as the Selection Criteria for Audit Subjects.....	26
B.	The Agency Should Define the Scope and Process of Audits to Enable the Agency to Confirm Compliance, while Avoiding Unnecessary Burdens on Businesses.	27
C.	All Information Produced to the Agency during an Audit – not just Personal Information – Should Receive Appropriate Confidentiality and Security.	29
III.	Rules for Consumer Rights Requests Should Protect Against Unintended Impacts	30
A.	§ 7022: Requests to Delete	30
B.	§ 7023: Requests to Correct.....	31
C.	§ 7027: Requests to Limit Use and Disclosure of Sensitive Personal Information	33
IV.	The Opt-Out Submission Process is Overly Prescriptive, and May Increase Consumer Confusion	35
A.	§ 7004: Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent.....	35
B.	§ 7015: Alternative Opt-Out Link.....	37

CONCLUSION.....39

Before the
California Privacy Protection Agency

In the Matter of)	
)	
California Privacy Rights Act of 2020)	Invitation for Comments on
Rulemaking Process)	Proposed Rulemaking
)	
)	

INTRODUCTION

CTIA¹ appreciates the opportunity to provide these comments on the California Privacy Protection Agency’s (the “Agency’s”) draft regulations (the “Draft Regulations”) to implement the California Privacy Rights Act (“CPRA”). CTIA recognizes the significant undertaking involved in drafting these regulations, and commends the Agency’s efforts in fulfilling CPRA’s rulemaking mandate.

CTIA urges that in developing the Draft Regulations, the Agency focus on clarifying CPRA rights and obligations so that businesses can drive positive privacy outcomes for consumers, rather than using the rulemaking to create new rules that go beyond the statutory text of CPRA or its rulemaking grants. If adopted in their current form, CTIA is concerned that a number of the Draft Regulations would have the opposite effect, requiring businesses to jeopardize consumers’ privacy and comply with obligations inconsistent with CPRA’s statutory text. The practical effect of aspects of the rule would be requirements that present operational challenges and major costs related to implementation without a corresponding benefit to consumers. Thus, CTIA provides comments pertaining to the following sections of the modified regulations:

¹ CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association’s members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry’s voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry’s leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

- § 7002: Restrictions on the Collection and Use of Personal Information;
- § 7004: Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent;
- § 7011: Privacy Policy;
- § 7012: Notice at Collection of Personal Information;
- § 7015: Alternative Opt-Out Link;
- § 7022: Requests to Delete;
- § 7023: Requests to Correct;
- § 7025: Opt-Out Preference Signals;
- § 7027: Requests to Limit Use and Disclosure of Sensitive Personal Information;
- § 7050: Service Providers and Contractors; and
- § 7334: Agency Audits.

I. *A Number of Proposed Regulations Exceed the Agency’s Authority*

**A. § 7002: Restrictions on the Collection and Use of Personal Information
(Consumer Expectations Requirement)**

Section 7002(a) of the Draft Regulations would give the Agency broad discretion to restrict data uses based on “what an average consumer would expect.” This exceeds the Agency’s authority and is inconsistent with CPRA’s statutory text. Inventing a concept of “average consumer expectations” will discourage innovation and result in arbitrary and unfair enforcement, unless disclosures to consumers serve as the benchmark for determining what an average consumer would expect. CTIA, thus, suggests that the Agency should remove the “average consumer expectations” standard from the Draft Regulations, or the Agency should make clear that consumers’ expectations are determined by the notices businesses have provided to them.

**1. Notices to Consumers, not a Hypothetical “Average Consumer”
Standard, are CPRA’s Means for Setting Consumer Expectations and
Permissible Uses**

CPRA permits notices at collection including businesses’ privacy policies to set consumer expectations about data uses and sharing.² In contrast to CPRA’s statutory framework, the Draft Regulations would subject all data uses to an “average consumer expectations” test. This exceeds the Agency’s rulemaking authority, is inconsistent with the Draft Regulations’ notice-at-collection provisions, and contradicts CPRA’s statutory text.

CPRA states that data collection, use, and disclosure are permitted if “reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed.”³ CPRA envisions that notices at collection are what set “the purposes for which

² Cal. Civ. Code §§ 1798.100(a), 1798.130(a)(5).

³ Cal. Civ. Code § 1798.100(c).

personal information [is] collected,” so long as those purposes are compatible with the context in which the personal information was collected.⁴ In § 7012, the Draft Regulations agree, stating: “[t]he purpose of the notice at collection is to provide consumers with timely notice ... about ... the purposes for which the personal information will be used.”⁵ With such notice, consumers are given “meaningful control” and can “choose whether or not to engage with the business, or to direct the business not to sell[] or shar[e] their personal information.”⁶

Despite these provisions, the Draft Regulations would give the Agency broad discretion to impose “expectations”-based restrictions on data uses. “To be reasonably necessary and proportionate” under the Draft Regulations, all data uses must be “consistent with what an average consumer would expect when the personal information was collected.”⁷

This “average consumer expectations” standard is not contemplated or required anywhere in CPRA’s statutory text. On the contrary, in only one place does CPRA require businesses to conform data uses to consumer expectations -- after a consumer has made a Request to Limit, the business must “limit its use of the consumer’s *sensitive personal information* to [what] is necessary to perform the services ... reasonably expected by an average consumer.”⁸ This indicates CPRA generally intends for notices to set permissible data uses, while consumer expectations only determine permissible uses when consumers make Requests to Limit. And even there, consumer expectations only limit uses of sensitive personal information, not uses of personal information generally.

⁴ Cal. Civ. Code § 1798.100(c).

⁵ § 7012(a).

⁶ § 7012(a).

⁷ § 7002(a).

⁸ Cal. Civ. Code § 1798.121(a) (emphasis added).

2. An “Average Consumer Expectations” Test will Cause Arbitrary Enforcement unless Privacy Notices Serve as the Benchmark for What Consumers Expect

Even if the Agency believes that introducing a new “average consumer expectations” test does not exceed its statutory authority, it should design the test so that businesses can know how it will apply to their practices – and thus can design their practices to comply. By itself, an “average consumer expectations” standard is vague, and will thus disincentivize innovation and lead to arbitrary enforcement for several reasons.

For example, for many data uses, there will not be a recognizable “average consumer.” Consumers have varying and often contradictory expectations about technology and how it uses personal information. More importantly, the Draft Regulations do not indicate who will decide what “average consumers’ expectations” are – or what process will be followed to formally determine what consumers expect. Presumably, the Agency will make that decision. However, the Draft Regulations do not require the Agency to conduct empirical research into actual consumer sentiments, and businesses would have no guarantee that an Agency action in the name of consumers would actually enforce “average consumers” expectations.

This could result in a disincentive to businesses to innovate. If a product, service, initiative, or technology is new, businesses would be left to guess what the Agency could decide as to what “average consumers” expects (or merely prefers) the business to do – and not do – with their data.

To avoid these unpredictable results, if a consumer-expectations test is used, businesses’ disclosures to consumers should serve as the baseline for determining what consumers expect. This will enable businesses to communicate their anticipated data uses to consumers, and innovate consistent with those disclosures. CPRA and the Draft Regulations, through their notice-at-

collection provisions, will help ensure that disclosures are timely, and will “provide consumers with the opportunity to choose how to engage with the business in light of its information practices.”⁹

**B. § 7002: Restrictions on the Collection and Use of Personal Information
(Consent Requirement)**

The Draft Regulations introduce a new consent requirement for data uses that are “unrelated to or incompatible with” prior data collection purposes by indicating that data uses must be limited to what is expected by average consumers, and characterizing all other data uses as not “necessary or proportionate.”¹⁰ For these additional, purportedly “non-necessary” data uses, the Draft Regulations would potentially require businesses to obtain “the consumer’s explicit consent.”¹¹ This consent rule exceeds the Agency’s rulemaking authority. CPRA grants the Agency no authority to institute a new “general consent” requirement, as the Draft Regulations would appear to do. Even if the Agency had authority to create a new consent requirement, the consent the Agency requires under § 7002(a) goes well beyond CPRA’s statutory language.

**1. The Agency Lacks Statutory Authority to Issue a General Consent
Requirement for New Data Uses**

CPRA’s statutory text contains only limited and defined consent requirements. Consent is required to:

- (a) opt-back-in a consumer who has made a Request to Limit¹²;
- (b) enter a consumer in a financial incentive program;¹³
- (c) transmit a consumer’s opt-out preference signal;¹⁴

⁹ § 7012(a).

¹⁰ § 7002(a).

¹¹ § 7002(a).

¹² Cal. Civ. Code § 1798.121(b).

¹³ Cal. Civ. Code § 1798.125(b)(3).

¹⁴ Cal. Civ. Code § 1798.135(b)(1).

- (d) ignore a consumer's opt-out preference signal that conflicts with other preferences;¹⁵
- (e) sell or share data of a consumer under 16 years old;¹⁶ or
- (f) sell or share data in a manner inconsistent with a clinical trial or research study.¹⁷

CPRA does not grant the Agency authority to introduce new consent requirements. Instead, CPRA narrowly cabins the Agency's consent-related rulemaking authority to regulating parameters for two specifically-enumerated consent types entirely within the context of the opt-out preference signal:

- (a) regulating a right to "selectively consent" to sales or sharing that conflicts with the opt-out preference signal;¹⁸ and
- (b) regulating a right to "subsequently consent" to sales or sharing of data after using a preference signal to opt-out,¹⁹ including via a webpage provided for this purpose.²⁰

Beyond the above, CPRA's rulemaking grant does not empower the Agency to enact new consent requirements for allegedly inconsistent data uses – it only permits the Agency to "defin[e] and add[]" to the "business purposes ... for which businesses ... may use consumers' personal information consistent with consumers' expectations."²¹ Section 7002(a)'s requirement to obtain "explicit consent" is therefore outside the Agency's rulemaking authority.

¹⁵ Cal. Civ. Code § 1798.135(b)(2).

¹⁶ Cal. Civ. Code § 1798.135(c).

¹⁷ Cal. Civ. Code § 1798.145(c)(1)(C).

¹⁸ Cal. Civ. Code § 1798.185(a)(19)(A)(v).

¹⁹ Cal. Civ. Code § 1798.145(a)(20).

²⁰ Cal. Civ. Code § 1798.145(a)(20)(C).

²¹ Cal. Civ. Code § 1798.185(a)(10).

2. Requiring Consent for any New Uses “Unrelated to or Incompatible With” Consumer Expectations Conflicts With CPRA’s Statutory Text and Scheme, Which Uses Notices at Collection – not Consent – to Enable Consumers to Control New Data Uses

As stated above, CPRA specifically delineates when a business is required to obtain consent from consumers before it can use their personal information. There is no general “catch all” consent provision, nor does CPRA provide the Agency with the authority to specify in rulemaking other instances where consent is required. Therefore, the Agency acts beyond the scope of its authority when it imposes an “explicit consent” requirement for purposes “unrelated to or incompatible with the purposes for which the personal information was collected or processed,” as it does in § 7002(a). The Agency seems to acknowledge this lack of authority to require consent in these instances, as § 7002(c) requires businesses that “intend[] to use [] personal information for additional purposes that are incompatible with [previously] disclosed purpose[s]” to “provide a new notice at collection.” These two sections of the regulations appear to be in conflict - it is unclear why consent would need to be obtained from consumers for “incompatible uses” under § 7002(a) when § 7002(c) already requires new notices at collection to be sent to consumers for such data uses. Providing a notice is appropriate in these instances as it is the same process as what would have been required at the original point of creating the customer relationship and would permit customers to “choose whether or not to engage with the business” just as envisioned by the regulations.²²

In addition to exceeding its statutory authority, the Agency’s proposed consent standard could create significant burdens and harm competition, particularly for small businesses. For

²² §7012.

example, assume that a new online retailer struggles to establish itself with consumers, but after a few years generates enough revenue to begin expanding its operations. As part of this, the retailer hires a business analyst to evaluate what its customers' typical purchase journey looks like in order to improve that experience. But, like many small businesses, when it began operations, the retailer did not expressly state in its privacy policy that customer transaction data may be used for internal analytics. It would be unreasonably burdensome – and inconsistent with § 7012 – if the retailer not only had to provide a new notice, but also obtain “explicit consent.” This would also have anticompetitive effects. The retailer's much larger competitors may very likely already conducting customer journey analytics (and thus provided this notice at collection), while the newer and smaller retailer potentially ends up barred from the same practice to a substantial extent by § 7002(a)'s consent requirement.

3. The Agency's Consent Requirement for Data Use “Unrelated To” the Purposes for Which it was Collected Could Potentially Harm Consumers.

CTIA contends that the Agency cannot introduce the concept of “unrelated uses.” The CPRA contemplates requiring additional notice for collections and uses that are “incompatible with the disclosed purpose,” but including “unrelated to” goes beyond what is permissible. There are many use cases that may be unrelated to the purpose for which the information was collected, but certainly not incompatible, including many security and fraud prevention products and services, which could potentially harm consumers.

For instance, businesses may use consumer information they collected in the past to help secure consumer accounts, such as preventing fraudulent use of a consumer's account. At the time consumer's account provided their information, account fraud prevention may not have been one of the potential uses they anticipated, and thus, arguably “unrelated to” their expectations – even

though it is readily compatible with what consumers want. The Agency’s “unrelated to” language thus, potentially bars businesses from beneficial data uses that protect consumers, and the Agency should eliminate this overreach.

C. § 7011: Privacy Policies

The Draft Regulations require uneven levels of disclosures in privacy policies. In particular, a business’s privacy policies must disclose more information about data shared with third parties than about its own data collection and data uses. Further, the Draft Regulations would require disclosures of “specific” business purpose that CPRA itself does not require. The cumulative effect of these disclosure rules will be privacy policies that are more complex, and less readily understandable by consumers, while also potentially exposing security-sensitive information to malicious actors.

CPRA requires companies’ privacy policies to disclose (a) a “list of the categories of personal information it has collected about consumers in the preceding 12 months,” and (b) “the business or commercial purpose for collecting or selling or sharing consumers’ personal information.”²³ In general, the Draft Regulations aligns with these statutory requirements. For example, the Draft Regulations require businesses to identify the “categories of personal information the business has collected” and the “specific business or commercial purpose for collecting personal information” – and to ensure the business’s description provides consumers with “a meaningful understanding.”²⁴

However, the Draft Regulations require additional disclosures about the categories of personal information that are sold, shared, or even merely disclosed for a business purpose. For “each category” of such personal information that the privacy policy identifies, businesses must

²³ Cal. Civ. Code § 1798.130(a)(5)(B)(i), (iii).

²⁴ § 7011(e)(1)(A), (C).

identify “the categories of third parties to whom” the personal information was sold, shared, or disclosed for a business purpose.²⁵

This level of granularity in disclosure of how personal information is shared is not required by CPRA, and would not be helpful to consumers, particularly for data disclosed for a business purpose. Many businesses disclose substantially all types of personal information they collect to service providers who assist with various business functions. Consumers have no right to opt-out of this sharing. It makes little sense to require detailed disclosures about common practices that consumers cannot influence.

Additionally, the Draft Regulations would require privacy policies to disclose the “specific business or commercial purposes” for data collection.²⁶ This could be read to require a one-to-one accounting of uses with specific data categories. This is not contemplated by CPRA, which only requires privacy policies to disclose “[t]he business or commercial purpose for collecting [] personal information.”²⁷

Requiring disclosures of “specific” collection purposes tied to data categories would be challenging for businesses and confusing to consumers. Privacy policies would likely be transformed into a complex, difficult-to-read data catalog, which would be inconsistent with the Draft Regulations’ mandates to keep privacy policies “easy to read,” “understandable to consumers,” and “readable [] on smaller screens.”²⁸ Further, granular detail on uses of specific data elements could be problematic from a security perspective. It could reveal details about personal information held by a company, including specific data elements used for security purposes, which could be valuable information to malicious actors.

²⁵ § 7011(e)(1)(D)-(E), (H)-(I).

²⁶ § 7011(e)(1)(C).

²⁷ Cal. Civ. Code § 1798.110(c)(3).

²⁸ §§ 7003(a)-(b), 7011(b).

D. § 7025: Opt-Out Preference Signals

1. Requiring All Companies to Process Opt-Out Preference Signals – Even if they Post a “Do Not Sell/Share” Link – Exceeds the Agency’s Authority

The Draft Regulations would require companies to process consumer opt-out preference signals even if they have posted a “Do Not Sell or Share My Personal Information” link. This requirement is contrary to CPRA’s express statutory text and exceeds the Agency’s rulemaking authority.

CPRA generally requires any company that “sells” or “shares” personal information to post a “Do Not Sell or Share My Personal Information” link on their internet homepages.²⁹ CPRA also offers companies that “sell” or “share” personal information *the option of* processing consumers’ opt-out requests received “through an opt-out preference signal.”³⁰

Per CPRA, “a business that complies with [§ 1798.135(a)]” – i.e. by posting a “Do Not Sell” link – “is not required to comply with [§ 1798.135(b)]” and execute opt-out preference signals.³¹ Instead, “a business may elect whether” to post a “Do Not Sell” link, or to process opt-outs submitted via opt-out preference signals – but does not need to do both.³²

Contrary to this clear language, the Draft Regulations require all businesses to process opt-out preference signals.³³ This proposed regulation is contrary to the clear statutory language of CPRA, and therefore exceeds the Agency’s rulemaking authority.

²⁹ § 1798.135(a).

³⁰ § 1798.135(b).

³¹ Cal. Civ. Code § 1798.135(b)(3).

³² Cal. Civ. Code § 1798.135(b)(3).

³³ § 7025(e).

2. The Agency has Failed to Provide Specifications for an Opt-Out Preference Signal, as well as Rules Governing Companies that Develop Opt-Out Preference Technologies. Businesses Should thus not be Required to Process Opt-Out Preference Signals.

CPRA requires Agency rulemaking to set forth (a) required specifications for opt-out preference signals, and (b) a number of CPRA-mandated rules for companies that develop opt-out preference technologies, such as transparency and market-fairness standards. The Agency has fulfilled neither of these rulemaking obligations. As a result, businesses should not be obligated to process opt-out preference signals until these CPRA-mandated specifications and standards are provided.

The Agency has not satisfied its rulemaking obligation to provide specifications for opt-out preference signals. CPRA requires the Agency to issue regulations that define the general specifications “for an opt-out preference signal.”³⁴ The Draft Regulations contain no such specifications. Since CPRA further states that businesses’ obligations to process opt-out preference signals are “based on” the specifications set forth in CPRA rulemaking,³⁵ businesses should not be obligated to comply with opt-out preference signals.

The Draft Regulations merely state that opt-out signals must be “in a format commonly used and recognized by businesses” – and provides as an example “an HTTP header field.”³⁶ This is an example and not a specification. By requiring companies to simply process any “format commonly used ... by businesses,” the Agency provides none of these commonly-accepted specification components. It instead merely punts the creation of specifications to industry.

³⁴ Cal. Civ. Code § 1798.185(a)(19)(A).

³⁵ Cal. Civ. Code § 1798.135(b)(1).

³⁶ § 7025(b)(1).

This will create unreasonable burdens for business because the standards for what is “commonly used” can vary materially. There is no guarantee that a “commonly used” signal format in one industry can be detected and processed by the technology used in other industries. As an example, Bluetooth arguably may be a “format” that is “commonly used and recognized” in some – but not all – industries. Would industries that do not typically detect Bluetooth need to change their technology so they can start recognizing opt-out signals sent via Bluetooth, merely because it is “commonly used” by other types of businesses? Payment terminals at retail locations often recognize Near Field Communication (NFC) but may not detect Bluetooth signals. Would payment processors be required to retrofit payment terminals to detect opt-out preference signals transmitted via Bluetooth from mobile devices that are physically present at retail locations?

CPRA also mandates that the Agency pass rules governing companies that develop opt-out preference technologies. But the Draft Regulations do not contain any of these CPRA-mandated rules. Without these, businesses cannot be assured that companies that develop opt-out preference technologies will reliably obtain informed consumer opt-out choices, or that opt-out technologies will operate fairly in all markets.

As salient examples:

- CPRA requires rulemaking that ensures opt-out preference technologies provide “settings” interfaces, which provide clear options for consumers. These “settings” pages should offer (a) a global opt-out, (b) a “Do Not Sell/Do Not Share” choice, and (c) a “Limit the Use” choice.³⁷ However, the Draft Regulations do not require opt-out technologies to provide “settings” interfaces, or the CPRA-mandated consumer disclosures or choices.

³⁷ Cal. Civ. Code § 1798.185(a)(19)(A)(vi).

- CPRA requires rulemaking to ensure opt-out preference technology is “free of default[]” settings that presuppose consumers’ intent to opt-out.³⁸ But the Draft Regulations do not contain any rules about default settings, just a rule that opt-out signal formats be “commonly used.”
- Also, CPRA requires rulemaking to “[e]nsure” that the opt-out preference technology “cannot unfairly disadvantage another business.”³⁹ Again, however, under the current version of the Draft Regulations, there is no restriction on companies designing opt-out signal technology that would disadvantage their competitors.

Until the Draft Regulations satisfy these rulemaking mandates, businesses should not be obligated to process opt-out preference signals.

E. § 7012(g)(3): Notices at Collection of Personal Information (Third Parties that Control the Collection of Personal Information)

The Draft Regulations define a new concept of “third parties that control the collection of personal information.” Under the Draft Regulations “third parties that control” data collection appear to be subject to notice-at-collection obligations, while third parties that do not “control” the collection of personal information are not.⁴⁰

This approach conflicts with CPRA’s statutory scheme for notices at collection. Under CPRA, only third parties that “control the collection” of personal information on their own premises have notice-at-collection obligations.⁴¹ The Draft Regulations, however, would expand this obligation to all “third parties that control the collection” of data, irrespective of whether they collect on their own premises. Furthermore, the Draft Regulations provide little clarity about what

³⁸ Cal. Civ. Code § 1798.185(a)(19)(A)(iii).

³⁹ Cal. Civ. Code § 1798.185(a)(19)(A)(i).

⁴⁰ § 7012(g)(3).

⁴¹ Cal. Civ. Code § 1798.100(a)(3)(b).

kind of companies are “third parties that control” collection of data – and the illustrative examples increase confusion.

1. The Agency’s Notice Rules for Third Parties That Control the Collection of Personal Information Conflict With CPRA, Which Only Requires Third Parties to Display Notices at Collection When Acting on Their Own Premises

The Draft Regulations introduce new notice-at-collection obligations for a “business that, acting as a third party, controls the collection of personal information on another business’s premises.”⁴² CPRA, by contrast, only imposes notice-at-collection obligations on businesses that, acting as third parties, “control[] the collection” of personal information on their own premises. CPRA does not impose notice-at-collection obligations on companies that “control the collection” of personal information on other companies’ premises. In § 7012(g)(3), the Agency is therefore creating a new notice-of-collection obligation that goes beyond CPRA’s statutory text.

- CPRA generally requires a business that “controls the collection” of personal information to provide a notice at collection.⁴³ This would logically mean the business with whom the consumer is interacting, such as the website whose brand is on a website or a retail store.
- CPRA further provides that if the business controlling the personal information is “acting as a third party,” it may satisfy its notice obligation by posting the required disclosures on its website as opposed to at collection, subject to one exception: notice at collection is required even of a third party where it controls the collection of information “about a consumer on its premises.”

⁴² § 7012(g)(3).

⁴³ Cal. Civ. Code § 1798.100(a).

Thus, subject to the “on its premises” exception, the CPRA deems a third party to be in compliance with its notice obligations by making the required disclosure on its website. This makes sense from a policy and practical perspective, since businesses that collect data on another business’s premises cannot control what the “owning business” will or will not display to consumers. More importantly, the Draft Regulations impermissibly contradict the CCPA by requiring a third party to provide notice at collection in circumstances where the CCPA expressly deems the third party in compliance via website disclosures.

2. The Draft Regulations Do Not Let Businesses Know When They Will be Considered a “Third Party That Controls” Data Collection. The Agency’s Illustration Increases Confusion, Instead of Providing Clarity.

The Draft Regulations provide little clarity about what a “third party that controls the collection of personal information” actually is. Although § 7012(g) introduces a concept of “third parties that control the collection of personal information,” neither CPRA nor the Draft Regulations state what it means to “control the collection” of personal information as a “third party.”

Instead of offering further definition, § 7012(g)(1) merely states that “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.” It remains unclear whether the Agency intends for every piece of third-party technology integrated into a website or app to be a “third party” that is independently “controlling” its collection of personal information.

Moreover, the examples the Agency provides in the draft regulations do not clarify the issue. The examples make broad assumptions about what party “controls” collection of personal

information, when in practice this is subject to significant variation and best determined by the parties and their contracts.

- Example A (§ 7012(g)(4)(A)) suggests that a provider of website analytics would be a “third party authorized to collect personal information.” However, analytics can readily be provided on a “service provider” basis and need not involve activities the Agency indicates confer “third-party” status, like “cross-context behavioral advertising.” CTIA respectfully suggests that the Agency clarify that the mere practice of providing analytics would not make an entity a “third party.”
- In Example C (§ 7012(g)(4)(C)), it is difficult to understand who is the first versus the third party. CTIA respectfully suggests the Agency clarify the roles of Business J and Business K in Example C so it is clear who the first and third parties are, and why each has the notice obligations the Agency concludes they have.

This lack of clarity is particularly onerous under the Draft Regulations’ expanded disclosure requirements. Under § 7012(e)(6), a “business [that] allows third parties to control the collection of personal information” must include “the names of all the third parties” in its notice at collection. Without further clarity on what constitutes a third party that controls the collection of personal information, businesses may see themselves as required to over-include partner names in notices at collection. These, in turn, would overburden consumers with overly long notices with information that is unlikely to enable consumers to “choose how to engage with the business in light of its information practices,” as the statute requires.⁴⁴

⁴⁴ § 7012(a).

F. § 7050: Service Providers and Contractors

1. The Draft Regulations Should Clarify That the Same Company Can Provide Some of its Services as a “Service Provider,” While Also Providing Cross-Context Behavioral Advertising Services as a “Third Party.”

The Draft Regulations suggest that service providers automatically become “third parties” if they provide cross-context behavioral advertising services under any circumstances. The global nature of the status change – switching completely from “service provider” to “third party” – fails to account for the fact that companies can provide multiple services to customers, and only one of which may constitute cross-context behavioral advertising. The Agency should clarify that service provider/third party status is determined on a service-by-service basis, and should not impose an overly simplistic view that removes businesses’ ability to contract in ways that accurately reflect commercial relationships.

Under the Draft Regulations, “[a] person who contracts with a business to provide cross-context behavioral advertising is a third party and not a service provider.”⁴⁵ Similarly, “[a] service provider ... cannot contract with a business to provide cross-context behavioral advertising.”⁴⁶ This suggests that if a company provides multiple services to a customer, and one of those services amounts to “cross-context behavioral advertising,” the company automatically becomes a “third party” on a global basis – and cannot be a “service provider” for its other services.

In reality, many companies provide multiple types of services to their customers at the same time. In doing so, companies can readily act in a “service provider” role for some services, while acting as a “third party” for other services. Contracts can be drafted to support this kind of service-by-service approach.

⁴⁵ § 7050(c).

⁴⁶ § 7050(c).

The Draft Regulations suggest that this nuanced approach would not be permitted, and that companies are either fully a “service provider,” or fully a “third party” – but cannot be both. This would be an unnecessarily prescriptive approach that imposes an overly simplistic and *ipse dixit* view on commercial relationships, without regard to how companies have actually contracted for services. It could also amount to a penalty on any company that includes cross-context behavioral advertising in its service offerings. The Agency should consider modifying the Draft Regulations so it is clear that “service provider” and “third party” status is determined on a service-by-service basis, not on an entity-wide basis. This would ensure companies’ ability to enter contracts that comply with CPRA and accurately reflect service provider relationships.

2. Requiring Service Provider Agreements to Enumerate “Specific” Business Purposes Exceeds CPRA’s Statutory Text and may Inadvertently Interfere with Contract Negotiations.

CPRA contains a general and flexible standard for describing business purposes in service provider agreements. Under CPRA, service provider agreements must require service providers to use personal information for “the business purposes” identified in the contract with the business.⁴⁷ CPRA contains no requirement that these business purposes be “specific” or “listed,” as the Draft Regulations would require, and instead leaves businesses flexibility to tailor contractual purpose descriptions to the relationship and service at issue.

CPRA does not grant the Agency authority to require that a business describe the specific purpose for use of personal information in service provider contracts. CPRA only permits the Agency to “further defin[e] or add[] to the business purposes” for which service providers are already permitted to process personal information under contracts with businesses.⁴⁸

⁴⁷ Cal. Civ. Code § 1798.140(ag)(1)(B).

⁴⁸ Cal. Civ. Code § 1798.185(a)(10).

Despite these limitations, the Draft Regulations would introduce a new requirement for service provider agreements to “list the specific business purpose(s)” for which they will process personal information.⁴⁹ Further, per the Draft Regulations, “[t]he business purpose or service shall not be described in generic terms, such as referencing the entire contract generally;” instead, “[t]he description shall be specific.”⁵⁰ These rules would exceed CPRA’s rulemaking grant, and be inconsistent with the more flexible approach to purpose descriptions permitted under CPRA’s statutory text.

Moreover, the Agency’s requirement for express lists of specific business purposes could inadvertently complicate contract negotiations between businesses and service providers. Providers may take a position that, since the Draft Regulations require “specific” lists of business purposes to create a valid service provider contract, negotiations must start with their standard contract language. Additionally, businesses may insist that service providers warrant their purpose descriptions are sufficiently “specific.” These issues may impede negotiation of service provider agreements and make them more burdensome. CTIA submits that a general-purpose description would be adequate under CPRA, without imposing new burdens on contract negotiation.

II. *Agency Audit Provisions Under § 7304 Lack Specificity and Safeguards*

The Agency’s audit powers under the Draft Regulations are impermissibly broad, and do not fulfill the Agency’s statutory task of defining the “scope and process” for audits. In particular, the Agency can conduct unannounced audits of practically any business, without any restrictions on scope or frequency, simply for the purpose of “ensur[ing] compliance with any provision of the CCPA.”⁵¹ In addition to investigating any “possible” violation of the CCPA, the Draft Regulations

⁴⁹ § 7051(a)(2).

⁵⁰ § 7051(a)(1).

⁵¹ § 7304(a).

let the Agency audit businesses it deems a “significant” risk to consumer privacy or security, or businesses with a “history of noncompliance” with any privacy protection law. Under the Draft Regulations, the Agency is not required to follow any defined process or procedure when conducting the audit, nor must it provide reasonable and customary confidentiality and privilege protections to audited businesses.

CTIA submits that further rulemaking is required to bring the Agency’s audit power into compliance with CPRA mandates for Agency audits.

A. The Draft Regulations Have Failed to Define the “Scope and Process” for Agency Audits, as well as the Selection Criteria for Audit Subjects.

The Agency’s audit power is much broader than what CPRA authorizes. Civil Code § 1798.185(a)(18) requires the Draft Regulations to define the “scope and process” of audits, including “criteria for selecting” audit subjects. The Draft Regulations have failed to do this.

- Section 7304 contains no defined “scope” for Agency audits. Quite to the contrary, the Draft Regulations would permit the Agency to audit as it deems fit “to ensure compliance” with the CPRA, without any temporal or process limitations.⁵² The Draft Regulations contain no limitations on duration, frequency, facilities, personnel, or otherwise.
- The Draft Regulations also contain no “process” for audits. This is in contrast to Agency investigations, for which the Draft Regulations prescribe notice and hearing requirements. For audits, however, the Agency is not required to provide advance notice, confine audits to reasonable business hours, request the minimum information necessary, or follow other procedural standards regarding duration, frequency, facilities, personnel, or otherwise that are reasonable and customary.

⁵² § 7304(a).

- Lastly, the Draft Regulations do not contain any “criteria for selecting” businesses for audits. Instead, they permit the Agency to audit any “possible” CPRA violation.⁵³ Further, the Agency can audit any company it deems to present a “significant” risk, or have a “history of noncompliance,” even if no “possible” CPRA violation is present.⁵⁴ These are unrestricted audit powers that remove any distinction between the Agency’s audit and investigatory powers. They are not “criteria” for selecting businesses for audit. Investing relatively unrestricted audit power in the Agency risks abuse of authority and unnecessary expense to both California taxpayers and businesses.

B. The Agency Should Define the Scope and Process of Audits to Enable the Agency to Confirm Compliance, while Avoiding Unnecessary Burdens on Businesses.

CTIA suggests the Agency consider the following parameters in designing procedural rules for audits which would enable the Agency to achieve CPRA’s goal for audits – i.e. “to ensure compliance with” CPRA⁵⁵ – while avoiding unnecessary burdens on businesses.

- Audits should be subject to frequency limitations. The Agency should not be permitted to audit companies more than once every 36 months. Lack of a temporal limit on the Agency’s audit frequency would not permit companies the time required to address any issue that might be raised in an audit prior to being subject to the next potential audit. When notified of potential non-compliance, companies must be given sufficient time to design, implement, and refine substantively different data practices to come into compliance. Consumers do not benefit from quickly designed and untested data practices.

⁵³ § 7304(b).

⁵⁴ § 7304(b).

⁵⁵ Cal. Civ. Code § 1798.199.40(f).

- Audit selection criteria should be made foreseeable and fair for businesses. The Agency should not be permitted to audit all conceivable “possible” CPRA violations, as § 7304(b) currently contemplates. This removes any meaningful distinction between the Agency’s investigatory power and its audit power, thus enabling fishing expeditions that will cause unfairness to companies.
- The Agency’s audit powers should not include on-site inspections. When auditing for compliance with CPRA, the Agency can adequately examine a business’ policies and procedures through requests for information, and evidence of compliance therewith. The Agency should be able to complete its audit function through these processes rather than through on-site inspection that could disrupt a business’s ongoing operations. Otherwise, businesses would be subject to Agency’s audit authority based on the bare fact that they happen to hold personal information. Merely holding personal information should not subject businesses to new audit burdens.
- Audits should require prior notice by the Agency. A general 30-day notice period should be required. Unannounced audits should not be permitted. If the Agency wishes to obtain evidence in an unannounced fashion, it has investigative authorities on which it can rely, such as those established by the § 7300 sworn complaint process and those established in § 7301 of the Draft Regulations permitting Agency investigation of all matters that do not result from a sworn complaint.
- Audits should not look back beyond the retention period that CCPA and CPRA mandate for records of compliance. For example, the existing CCPA regulations, at §7101 require a business to maintain records of CCPA consumer requests and the business’s response for

twenty-four months. Businesses subject to an audit should not be required to produce information beyond the prior two years.

In addition to the foregoing, CTIA submits that the Agency should create and make available a standard audit or examination procedure. This should begin with requests only for the information necessary for the Agency to examine a possible or alleged CPRA violation. This should include developing a formal process for follow-up requests, and if appropriate notice of alternative investigative measures. The Agency should publish the standards it will use during audits as the basis to evaluate business practices for compliance with CPRA, such as an audit handbook, manual, or checklist.

Lastly, the Draft Regulations should provide businesses with a reasonable time to cure any noncompliance identified during an audit and forego any enforcement measures against businesses that cure identified noncompliance. A cure period is fair in light of the fact that – as the Draft Regulations currently stand – audits can be announced without any suspicion of wrongdoing. Permitting businesses to cure also comports with CPRA’s statutory purpose for audits, which is “to ensure compliance with” CPRA.⁵⁶

C. All Information Produced to the Agency during an Audit – not just Personal Information – Should Receive Appropriate Confidentiality and Security.

The Draft Regulations only require CPPA to protect “consumer personal information” disclosed during an audit – not confidential, proprietary, or other sensitive information.⁵⁷ This scope of protection is too narrow. Any disclosure of information by a business in response to an Agency audit should be given protections equal to those with which the Agency treats consumer personal information. The Agency should thus provide guarantees of confidentiality and

⁵⁶ Cal. Civ. Code § 1798.199.40(f).

⁵⁷ § 7304(e).

nondisclosure (including exemptions from the California Public Records Act) for all confidential, proprietary, and sensitive data disclosed by a business in connection with an audit.

Audits also create the risk of a data security incident by requiring that access to personal and other sensitive information be provided to a third party (i.e., the Agency). In the course of an audit, the Agency may access IT systems, proprietary corporate information, sensitive employee information, and other nonpublic information in addition to consumer personal information. The Agency should be required to take steps to safeguard businesses' IT systems and information, with equal protections for consumer personal information.

III. *Rules for Consumer Rights Requests Should Protect Against Unintended Impacts*

CTIA and its members agree that the rights afforded under CPRA are important; however, CTIA members are concerned that several of the Draft Regulations could result in unintended anti-security outcomes and other operational challenges. Additionally, proposals like these could present major implementation costs that the Agency has not adequately considered.⁵⁸ The Agency should address these issues before finalizing the rules to ensure that CPRA regulations promote consumer protection, and do not introduce new avenues for potential harm to consumers by bad actors.

A. § 7022: Requests to Delete

The Agency's rules for responding to Deletion requests would potentially harm security by disclosing detailed information to bad actors. The Draft Regulations would update the CCPA rules for requests to delete, and require a business that denies a consumer's request to "[p]rovide the

⁵⁸ The CPPA submitted an economic impact estimate that concluded the cost for a typical business to comply with the Proposed Regulations would be \$127.50 (based on the estimated total compliance cost divided by the total number of businesses. *See* Notes on Economic Impact Estimates, CCPA (June 27, 2022), https://cppa.ca.gov/regulations/pdf/std_399_attachment.pdf. CTIA believes the economic impact assessment significantly underestimates the cost of implementation. The examples referenced in this section are illustrative of the unconsidered operational costs that would result from implementation with the Draft Regulations as written.

consumer a detailed explanation of the basis for the denial” – including “any ... **factual basis for contending that compliance would be impossible or involved disproportionate effort.”⁵⁹**

The existing formulation of this rule—where a business is required to “describe the basis for the denial,” but not to “provide a detailed explanation”—is a better way to balance the goals of consumer transparency and security. Moving towards more detailed requirements, on the other hand, tips the balance and could introduce new risks to security and would be operationally burdensome for businesses. For example, if a business is not able to authenticate a request to delete and suspects that the requestor is in fact an imposter, the business should not have to provide a “detailed explanation” to that bad actor, as providing the bad actor with additional information could put the consumer further at risk. Accordingly, we request that the Agency revert to the existing CCPA regulations and remove the proposal to require a “detailed explanation.”

B. § 7023: Requests to Correct

In a similar fashion, the Draft Regulations on requests to correct introduce requirements that could pose security threats to personal information, and would otherwise raise serious operational concerns. These proposed regulations are in tension with core features of the CPRA framework that have been put in place to protect consumers.

- *First*, the Draft Regulations would require that “[w]here the business is not the source of the information that the consumer contends is inaccurate ... the business shall provide the consumer with the ***name of the source*** from which the business received the alleged inaccurate information.”⁶⁰ Disclosing granular source information raises commercial confidentiality issues, and could create serious operational challenges (particularly for smaller businesses). Importantly, this type of requirement would produce unintended anti-

⁵⁹ § 7022(f)(1) (emphases added to indicate newly proposed language).

⁶⁰ § 7023(i) (emphasis added).

security consequences CPRA seeks to avoid. Indeed, CPRA consistently clarifies that source disclosure requirements involve disclosing the *categories* of sources, not specific source names.⁶¹ This is for good reason. Disclosing the categories of sources provides consumers with meaningful information about their personal information, without risking that such disclosure provides details that bad actors could leverage by exposing sensitive commercial information. As such, the Agency should revise § 7023(i) to require that businesses disclose only the categories of sources.

- *Second*, the Draft Regulations would require a business to accept post-correction “Right to Know” requests “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.”⁶² While CTIA understands this is intended to “allow[] consumers to verify independently that the contested information was in fact corrected,”⁶³ as drafted, this regulation raises serious operational and security concerns. It could potentially undermine existing security protections that CPRA, and the existing CCPA regulations, rightly have in place around Right to Know requests. In particular, this new “post-correction access right” is not explicitly linked to the existing rules that prevent disclosure of sensitive information (i.e., social security number, driver’s license number, financial account number, and the like) in response to a request to know.⁶⁴ The existing rules were established by the Attorney General to “balance a consumer’s right to know with the harms that can result from the

⁶¹ See, e.g., Cal. Civ. Code § 1798.110(a)(2) (establishing that “[a] consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer . . . (2) [t]he *categories* of sources from which the personal information is collected . . .”) (emphasis added); 1798.110(c)(2) (requiring “[a] business that collects personal information about consumers [to] disclose, pursuant to subparagraphs (B) of paragraph (5) of subdivision (a) of Section 1798.130 . . . (2) [t]he *categories* of sources from which the personal information is collected . . .”) (emphasis added)).

⁶² § 7023(j)

⁶³ CCPA Initial Statement of Reasons at 31, https://cppa.ca.gov/regulations/pdf/20220708_isr.pdf.

⁶⁴ See § 7024(d).

unauthorized disclosure of information.”⁶⁵ Any disclosure of specific pieces of personal information required under CPRA—including disclosures to facilitate the right to correct—should be subject to these same important protections. Otherwise, the Agency’s newly proposed “right to know data has been corrected” could serve as a loophole for the reasonable security parameters in place to protect against CPRA being used to harm, rather than help, consumers.

- *Third*, the proposed access provisions under the right to correct are overly broad and should be tailored to achieve its intended goal of “confirm[ing] that the business has corrected the inaccurate information”⁶⁶ – rather than creating a new access right. If the Agency retains Section 7023(j), it should clarify that it only applies to the specific pieces of allegedly inaccurate personal information relevant to the request to correct.
- *Finally*, the Agency should consider establishing a safe harbor for self-service options for correction with respect to data that was provided directly to the business by the consumer. This will best facilitate the consumer’s right to correct, while balancing operational burdens and security considerations.

C. § 7027: Requests to Limit Use and Disclosure of Sensitive Personal Information

As they currently stand, the Draft Regulations inappropriately limit how businesses can use sensitive personal information for security-related purposes without triggering Right to Limit rights. The limitations the Draft Regulations place on security-related uses of sensitive personal information go beyond CPRA’s statutory text.

⁶⁵ See OAG Final Statement of Reasons: Update of Initial Statement of Reasons, CA OAG, at 26 (June 1, 2020), <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor.pdf>.

⁶⁶ § 7023(j).

The Draft Regulations include a list of “[t]he purposes for which a business may use or disclose sensitive personal information without being required to offer consumers a right to limit” and clarify that “[a] business that only uses or discloses sensitive personal information for these enumerated purposes is not required to post a notice of right to limit.”⁶⁷ As drafted, however, these proposed regulations are in tension with the statute and risk creating confusion for both consumers and businesses.

First, the proposed regulations appear to narrow the already-permissible security-related uses of sensitive data that do not trigger the right to limit. CPRA allows consumers to limit the use of the consumer’s sensitive personal information to “that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer” – but note that uses recognized in Civil Code § 1798.140(e)(2), (4), (5) and (8) remain unaffected by the Request to Limit. Among these permitted uses, Civil Code § 1798.140(e)(2) lists “[h]elping to ensure security and integrity to the extent the use of the consumer’s personal information is reasonably necessary and proportionate for these purposes.”⁶⁸

The Draft Regulations also contain a list of permissible sensitive data uses that do not trigger the right to limit. However, the Draft Regulations define permitted security-related uses more narrowly than CPRA:

To detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information, provided that the use of the consumer’s personal information is reasonably necessary and proportionate for this purpose. For example, a business may disclose a consumer’s log-in information to a data security company that it has hired to investigate and remediate a data breach that involved that consumer’s account.⁶⁹

⁶⁷ § 7027(l).

⁶⁸ Cal. Civ. Code § 1798.140(e)(2).

⁶⁹ § 7027(l)(2).

To be sure, there are important ways that businesses use and disclose personal information to “ensure security and integrity” that go beyond “detect[ing] security incidents that that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.” Those uses should be included in the Agency’s list of purposes for which a business may use or disclose sensitive personal information without being required to offer consumers a right to limit, consistent with the statute. As such, the Agency should modify the Draft Regulations to track the CPRA’s statutory language in § 1798.140(e)(2).

IV. The Opt-Out Submission Process is Overly Prescriptive, and May Increase Consumer Confusion

CTIA recognizes the importance of the opt-out right within the Draft Regulations. For this reason, CTIA expresses that the prescriptive approach the Draft Regulations take towards opt-outs may lead to unintended consumer confusion, and thus inadvertently impair consumers’ opt-out right. CTIA suggests the Agency reconsider the opt-out requirements discussed below, and permit businesses to take a more flexible, consumer-centric approach to opt-outs.

A. § 7004: Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent

The Draft Regulations contain a number of requirements for consumer-facing opt-out submission channels. Section 7004 limits the number of clicks consumers can be required to make, the screens or webpages a consumer may scroll through, and the number of steps that can be involved in submitting an opt-out.⁷⁰ Opt-out notices must be prominent; opt-out submission must be “easy to execute;” opt-out information cannot be “manipulative;” and choices must be presented in a “symmetrical” fashion.⁷¹ Businesses may also choose to use the Agency’s alternative opt-out

⁷⁰ § 7002(a)(2)(A).

⁷¹ § 7002(a)(2).

link with “Your California Privacy Rights” or “Your Privacy Rights” alongside the proscribed button.⁷² The link must lead the consumer to a webpage where they can submit an opt-out request – but this page must incorporate the general restrictions of § 7004.⁷³

The cumulative effect of these requirements can make user-facing design difficult, and it is unclear whether executing all of the § 7004(a) requirements simultaneously is achievable in a manner that helps consumers. As an example, § 7004(a)(4)(B) states it is “manipulative and shaming” to “[r]equir[e] the consumer to click through reasons why submitting a request to opt-out of sale/sharing is allegedly a bad choice.” However, truthful and useful information regarding the impact of a consumer’s choice is not “shaming” and should not be considered manipulative or harmful. For example, if a consumer is participating in a loyalty program and would like to stop the sales/sharing of her personal information, the consumer needs to know whether opting-out would affect her ability to accumulate points, receive coupons, or receive other loyalty benefits. For consumers to make informed decisions about whether to exercise CCPA opt-out requests, consumers must be aware of how exercising an opt-out request will materially affect their future use of a product or service.

As a further example, the Draft Regulations state businesses cannot “require the consumer to ... scroll through the text of a webpage to locate the mechanism for submitting a request to opt-out of sale/sharing.”⁷⁴ This is potentially inconsistent with the Agency’s rules for the alternative opt-out link, which expressly require businesses to direct consumers to a webpage to “locate the [business’s] mechanism” for submitting opt-outs.⁷⁵ This also potentially precludes businesses from offering multiple avenues for exercising opt-out rights on a single webpage.

⁷² § 7015(b).

⁷³ § 7015(c)(2).

⁷⁴ § 7004(a)(5)(A).

⁷⁵ See § 7015(c).

Accordingly, although intended to facilitate consumers' ability to submit opt-outs, § 7004(a)'s overly prescriptive requirements may make opt-out channels less readily available, while providing less transparency to consumers in connection with opt-out choices. CTIA recommends the Agency permit businesses to take a more flexible approach to designing opt-out submission channels than the current draft of § 7004(a).⁷⁶

B. § 7015: Alternative Opt-Out Link

As CTIA discussed in prior comments submitted to the California Attorney General in November 2020, CTIA is concerned that the Draft Regulations' proposed "Alternative Opt-Out Link" remains confusing.



This icon suggests to consumers that clicking either side of the icon will effect a choice with regard to their rights. For example, a consumer can readily think that clicking on the "X" side will "stop" data sales. However, the icon pertains to two choices – the Right to Opt-Out and the Right to Limit – and neither choice can be made by clicking the icon.

Instead, the icon must direct the consumer to a webpage that includes: (i) a description of the consumer's right to opt-out of sale/sharing, (ii) a description of the consumer's right to limit, and (iii) the interactive form or mechanism by which the consumer can submit their request to opt-out of sale/sharing and/or their right to limit online.⁷⁷

⁷⁶ CTIA's suggestion to permit flexibility in designing opt-out submission channels under § 7004 also applies generally to all consumer rights under CCPA. The Draft Regulations in § 7004(a) provide standards for methods of submitting requests and, in subsection (b), expand the concept of "dark patterns" to potentially include anything not in compliance with those restrictive standards. CTIA submits that the Agency should not expand the concept of dark patterns beyond those practices that are unfair or deceptive as defined in 15 U.S.C. § 45(a)(4)(A).

⁷⁷ § 7015(c).

This needlessly misleads consumers into thinking that the button itself provides an immediate opt-out control, rather than a link to a different web page. CTIA, thus, requests that §7015 be modified to not require the inclusion of an icon that appears to contain toggle options, but serves no functional purpose as an opt-out button and risks consumer confusion about whether a rights request has been successfully submitted.

CONCLUSION

CTIA appreciates the Agency's consideration of these comments and stands ready to provide any additional information that would be helpful.

Respectfully submitted,

/s/ Gerard Keegan

Gerard Keegan
Vice President, State Legislative Affairs

Avonne Bell
Director, Connected Life

Jake Lestock
Director, State Legislative Affairs

CTIA

1400 16th St. NW, Suite 600
Washington, DC 20036
(202) 736-3200

August 23, 2022

From: [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 15:08:32 (+02:00)

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

My name is Andrew Alsup and I am a citizen of California. I would like to express my full support of the new draft CPRA regulations specifically as they pertain to the handling of opt-out preference signals. Global Privacy Control and other emerging opt-out preference signal implementations are a life raft to privacy-conscious online citizens and it is imperative that these regulations make it clear that California residents have the right for these global opt-out preference signals to be respected by businesses. I believe the proposed regulations fulfill that purpose well and I request that the proposed opt-out preference signal regulations NOT be weakened in any way prior to finalization.

Andrew Alsup

From: **Ritter, Denneile** [REDACTED]
To: **Regulations** <Regulations@cpga.ca.gov>
Subject: CPGA Public Comment
Date: 23.08.2022 22:18:19 (+02:00)
Attachments: CPRA Draft Regulations_APCIA Comment Letter_Final.pdf (12 pages)

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

Mr. Soublet,

On behalf of the American Property Casualty Insurance Association, attached please find our comments for the Agency's draft regulations. We look forward to engaging with you and your staff as you work to implement the CPRA.

Best,
Denni

Denneile Ritter

American Property Casualty Insurance Association

Vice President State Government Relations, Western Region

1415 L Street, Suite 670, Sacramento, CA 95814

P: [REDACTED] | [REDACTED]





August 23, 2022

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

Re: Response to Request for Comments – California Privacy Rights Act Draft Regulations

On behalf of the American Property Casualty Insurance Association (“APCIA”),¹ thank you for the opportunity to provide comments to the California Privacy Protection Agency (the “Agency”) rulemaking process for the California Consumer Privacy Act (“CCPA”) as prescribed by the California Privacy Rights Act (“CPRA”). APCIA members share the State’s goal of protecting the privacy of consumers. We appreciate the Agency’s efforts to provide guidance to businesses on how to comply with the CCPA and clarify the law’s requirements through the implementing regulations. We understand that the current draft proposed CCPA regulations² address the first set of topics out of the 22 topics the Agency is required to address under its rulemaking authority,³ and the insurance industry portion of the required changes (topic #21) is not yet addressed.⁴ However, we believe that, as the Agency drafts regulations, it is imperative that the Agency has context concerning the robust regulatory regime under which the insurance industry currently operates so that appropriate uses of personal information in the context of insurance operations may continue.

According to topic #21, the Agency’s rulemaking authority is to review the California Insurance Code and regulations (collectively referred to herein as “Insurance Laws”) pertaining to privacy and identify which, if any, provisions of the CCPA provide greater protection to consumers than those of the Insurance Laws. To the extent the Insurance Code does not provide greater protection to consumers, the Agency must adopt regulations for the insurance industry. It is important to note, however, that the CCPA explicitly exempts information that is subject to the Gramm-Leach-Bliley Act (“GLBA”), and its implementing regulations, and the California Financial Information Privacy Act (“FIPA”) and its implementing regulation, the Privacy of Nonpublic Personal Information regulations (“PNPI”).⁵ Nonpublic personal information (as defined in the GLBA and FIPA) that is collected and used by insurance entities in their insurance operations is not subject to the CCPA as a result of the GLBA and FIPA data-level exemption, and therefore would not fall under topic #21.⁶

¹ The American Property Casualty Insurance Association (APCIA) is the primary national trade association for home, auto, and business insurers. APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers, with a legacy dating back 150 years. APCIA members represent all sizes, structures, and regions—protecting families, communities, and businesses in the U.S. and across the globe.

² See https://cppa.ca.gov/meetings/materials/20220608_item3.pdf.

³ Cal. Civ. Code §1798.185(a).

⁴ Cal. Civ. Code §1798.185(a)(21).

⁵ 10 CCR 2689.1 et seq.

⁶ Cal. Civ. Code § 1798.145(e) provides that “This title shall not apply to personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code), or the federal Farm Credit Act of 1971 (as amended in 12 U.S.C. 2001-2279cc and implementing regulations, 12 C.F.R. 600, et seq.). This subdivision shall not apply to Section 1798.150.” This includes FIPA and PNPI. Topic #21 does not amend § 1798.185(e).

To the extent the Agency considers drafting regulations for the insurance industry in connection with the Agency's rulemaking authority per topic #21, we encourage the Agency collaborate with the California Department of Insurance (the "CDI"). As discussed more fully below, on November 8, 2021, the CDI responded to the Agency's request for comments on proposed CCPA revised regulations, requesting that the Agency work with the CDI prior to enacting any regulations applicable to the insurance industry.⁷ The CDI referenced the existing California Insurance Information and Privacy Protection Act ("IIPPA") and the PNPI, and the National Association of Insurance Commissioners' (the "NAIC")⁸ current evaluation of changes to NAIC Insurance Information and Privacy Protection Model Act ("Model Act #670") and the NAIC Privacy of Consumer Financial and Health Information Regulation ("Model Regulation #672"), upon which IIPPA and PNPI are based. Revisions to Model Act #670 and Model Regulation #672, when adopted in California, will affect the IIPPA and PNPI, which are overseen by the CDI. The comment letter stressed that close coordination between the Agency and the CDI is critical and requested that the NAIC's evaluation and revisions to Model Act #670 and Model Regulation #672 be allowed to be completed before the Agency issues insurance-specific CCPA regulations. During the recent Summer 2022 National Meeting, the NAIC Executive Committee approved a request confirming it will develop a new model to replace both Model Act #670 and Model Regulation #672. We support the CDI's recommendation and urge the Agency to closely coordinate with the CDI prior to enacting any regulations applicable to the insurance industry.

In connection with considering such collaboration efforts, the APCIA respectfully requests that the Agency consider the (i) distinct ways in which the insurance industry is regulated and uses personal information (i.e., in a manner that is necessary to allow the appropriate assessment and transfer of risk as compared to companies that rely on selling advertising as their primary source of revenue), (ii) significant existing regulations in the insurance industry concerning protection of personal information, and (iii) existing exclusion of insurance-related data from CCPA. The APCIA requests that the Agency carefully assess the existing insurance-specific privacy and cybersecurity requirements under which the industry currently operates in California before drafting any regulations applicable to the industry, and implement a formal moratorium on enforcement of the CCPA against insurance industry entities until the CDI and the NAIC complete their work.

I. The Insurance Industry Uses Personal Information Differently

The insurance industry offers products that allow individuals and businesses to transfer risk and be compensated and recover from unexpected loss events. Fundamental to a functioning insurance industry is ensuring that insurers have sufficient capital to pay losses. Although insurers utilize data, and often personal information, in their business, the primary use of such information is for the appropriate analysis and pricing of risk to offer competitive insurance products and services to consumers, while ensuring they are able to pay insurance claims. Insurers use actuarial science to determine the probability and severity of losses. Actuaries analyze mathematical models to predict or forecast the probability of an event occurring so that an insurance company can allocate funds to pay out any claims that might result from the event. For example, to calculate the probability and potential severity of future insurance claims, significant amounts of data are analyzed, including data on prior insurance claims. Third parties are often used to aggregate claims data to enable models to be created to accurately price insurance policies and understand the capital requirements necessary for the payment of claims. Insurance regulators require

⁷ See Preliminary Rulemaking Written Comments – Part 3, https://cippa.ca.gov/regulations/pdf/preliminary_rulemaking_comments_3.pdf.

⁸ The NAIC serves as a regulatory college and policy coordination body for the insurance commissioners of states and territories of the U.S. Founded in 1871, the U.S. standard-setting organization is governed by the chief insurance regulators from the 50 states, the District of Columbia, and five U.S. territories to coordinate regulation of multistate insurers.

insurance companies to retain capital and reserves based on such models. Additionally, one of the unique aspects of the insurance industry that states require consumers to obtain certain insurance coverages. For example, individuals are required to carry evidence of car insurance, and the California Insurance Code lists the minimum liability insurance requirements for private passenger vehicles.⁹ Similarly, lenders may require property or homeowners insurance for mortgage or other loans.

In addition to insurers, insurance agents and brokers (sometimes called producers) play a critical role in the insurance industry. Agents and brokers often collect and have access to personal information to assist individuals and organizations obtain the best insurance coverage at the best price. Agents and brokers are separately licensed by state regulators, and, like insurers, subject to insurance privacy laws and have legal responsibility for the protection of customer data, including personal information.

The insurance industry is regulated on a state-by-state basis, and insurers and agents are subject to the state-specific insurance regulations in each state an insurer maintains a license. Specifically, consumer privacy is embedded in insurance regulatory oversight. Insurance regulations include numerous mechanisms to protect consumers, including requiring notices concerning the use of data, requiring the opt-in or opt-out consent (as more fully discussed below) for certain uses of nonpublic personal information, and requiring responses to consumer complaints. Further, market conduct exams cover investigation by insurance regulators to determine whether insurers have been in compliance with the relevant laws relating to insurance operations, including the distribution of products to consumers. Each state department of insurance maintains an office dedicated to consumers, where individuals can file complaints against insurance companies and agents. These complaints are investigated by each state department of insurance and can result in fines and license termination of the insurer or agent.

II. Existing California Laws Specific to the Insurance Industry Provide Robust Privacy Protections to California Consumers

Since 1981 the insurance industry has been subject to a number of stringent privacy requirements in California. Insurers and producers that provide insurance products or services to individuals for their personal, family or household purposes are subject to the requirements of the GLBA as well as state laws and regulations implementing GLBA. California's GLBA implementing law and regulations – FIPA and PNPI – impose additional requirements that go beyond the federal GLBA and provide greater privacy protections to consumers than the GLBA requires. For example, whereas the GLBA requires covered entities to offer consumers the opportunity to opt-out of any sharing of nonpublic personal information (“NPI”) with non-affiliated third parties for marketing purposes, FIPA generally requires covered entities to obtain affirmative consent, or an opt-in, from California consumers prior to such sharing of NPI.

In addition to FIPA, the insurance industry operating in California is subject to the California IIPPA, enacted in 1981, and the PNPI, promulgated in 2003. These apply not only to insurance institutions but also to agents and insurance-support organizations that collect or otherwise use personal information in connection with insurance transactions. PNPI was specifically implemented to be “consistent with providing individuals the maximum privacy protections” permitted by the California Insurance Code and GLBA.¹⁰ Indeed, IIPPA and PNPI provide a number of consumer rights that are similar to those found in the CCPA, including the right to access, correct, amend, delete, and non-discrimination. However, when compared with the CCPA's requirements regarding consumer rights, such rights under the Insurance Laws differ in several key aspects, including the scope and type of information that must be provided to consumers, the method of delivery of notices, the methods by which insurers must obtain opt-in or provide opt-out of data sharing, and the timing requirements for privacy-related activities.

⁹ Insurance Code §11580.1b.

¹⁰ 10 CCR §2689.1.

IIPPA also provides individuals the right to appeal in case an individual disagrees with the insurance institution's refusal to correct, amend or delete recorded personal information,¹¹ which is not provided in the CCPA. Furthermore, FIPA, IIPPA, and PNPI require that insurers provide privacy notices to consumers, and the notice requirements include a detailed set of elements that are not required by the CCPA. For instance, the PNPI requires that the privacy notice achieve a minimum Flesch Reading Ease Score of 50 by including a specific formula in the regulations¹² and use an easy-to-read type size, specifying that the font size must be at least 10 point.¹³

The comparison chart below illustrates that the existing insurance-specific privacy laws provide consumer rights that are similar to, and in some cases, superior to, those found in the CCPA.¹⁴ Specifically:

- Highlighted in **orange** indicates certain consumer rights that are provided under the Insurance Laws but not found in the CCPA.
- Highlighted in **blue** indicates areas in which significant harmonization is needed in operationalizing consumer rights, which is discussed further in the following sections.

	CCPA	FIPA	IIPPA	PNPI
Notice	Yes	Yes	Yes	Yes
Access	Yes	No	Yes	Yes
Correct	Yes	No	Yes (Also provides the right to amend)	Yes
Delete	Yes	No	Yes	No
Portability	Yes	No	Partially yes	No
Non-discrimination	Yes	Yes	No	Yes
Know the reasons for adverse underwriting decisions	No	No	Yes	No
Right to appeal	No	No	Yes	No
Opt-out of sale of personal information	Yes	Yes	No	Yes
Limit the use and disclosure of sensitive personal information	Yes	Yes	Partially yes	Yes
Opt-out from use of automated decision-making technology	Yes	No	No	No
Opt-in consent	No	Yes (Opt-in to sell, share, transfer, or disclose)	Yes (Opt-in to disclose)	Yes (Opt-in to disclose)

¹¹ Insurance Code §791.09(c).

¹² The Flesch Reading Ease Score rates text on a 100-point scale – the higher the score, the easier it is to understand the document. 10 CCR §2689.4(a)(7).

¹³ *Id.*

¹⁴ This chart compares the core privacy concepts (e.g., individual rights, opt-in/opt-out) provided under the Insurance Laws and the CCPA. However, given that the scope of covered data is different between the CCPA and the Insurance Laws, even where the same core concept exists in the laws, the comparison is not “apples to apples” (as reflected in blue highlight).

III. Close Coordination between the Agency and the CDI in Implementing Regulations for the Insurance Industry Is Imperative

We highlight below a number of key reasons that the Agency and the CDI should closely coordinate in drafting regulations implementing the CCPA requirements in conjunction with the existing insurance-specific privacy requirements under FIPA, IIPPA, and PNPI.

- Despite the similarities in concept and the overlapping requirements under the CCPA and the Insurance Laws, the lack of consistency and alignment in these laws with respect to covered data creates the potential for significant consumer confusion, as well as onerous compliance challenges for the insurance industry. For example, although the CCPA and the Insurance Laws use the same terms, such as “personal information,” “consumer,” and “service provider,” these definitions do not cover the same scope of data or individuals. The definition of “service provider” under the CCPA is broader than under PNPI for reasons described below. The definition of “personal information” under IIPPA and “nonpublic personal information” or “nonpublic personal financial information” are more narrowly defined than “personal information” under the CCPA. As such, when regulations are drafted, key definitions that refer to the same term will require harmonization, without disrupting essential insurance operations.

Similarly, certain terms are defined differently in the CCPA and the Insurance Laws although they may refer to a similar concept. For instance, the CCPA’s definition of “sale” includes *disclosing* personal information to a third party for monetary or other valuable consideration, which is tied to the CCPA’s “Do Not Sell My Personal Information” provisions. In addition to the definition of “sale,” the CCPA separately defines “sharing,”¹⁵ which is limited to the disclosure or sharing of personal information to a third party for cross-context behavioral advertising. Under FIPA and PNPI, consumers can opt-out of *disclosing or sharing* their NPI, although these terms are not specifically defined as in the CCPA.¹⁶ FIPA also generally prohibits *selling, sharing, transferring, or otherwise disclosing* NPI to nonaffiliated third parties without obtaining an opt-in consent. If the CCPA is applied to insurance entities without harmonization of (i) overlapping terms such as “sale,” “share,” “transfer,” and “disclose” and (ii) which actions require opt-in or opt-out by consumers, there will be significant confusion for consumers.

- Operationalizing consumer/individual rights can be also a challenging task for companies in the insurance sector, as the mandatory opt-in and opt-out requirements under the Insurance Laws are similar but refer to a different scope of rights than CCPA. For example, FIPA requires insurers to obtain explicit prior (opt-in) consent from the consumer to *sell, share, transfer, or otherwise disclose* NPI to nonaffiliated third parties, except for certain specified uses.¹⁷ Further, the PNPI requires insurers to provide an opt-in for certain sharing of medical information and an opt-out before sharing any nonpublic personal financial information with a nonaffiliated third party, with a clear notice titled “Important Privacy Choices.” Under the CCPA draft regulations, an alternative *opt-out link* must be titled either “Your Privacy Choices” or “Your California Privacy Choices” in connection with the “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information.” The information that must be included, and even the

¹⁵ “Share,” “shared,” or “sharing” means “sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to a third party *for cross-context behavioral advertising*, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged (emphasis added).” Cal. Civ. Code §1798.185(ah).

¹⁶ 10 CCR §2689.8.

¹⁷ Cal. Fin. Code §4052.5.

“look and feel” requirements are different. The lack of consistency will not only have a material impact on the operations of insurance industry entities, but also can create confusion to consumers in effectively exercising their rights. Privacy policies that seek to explain and incorporate all the aforementioned requirements could confuse Californians to the point that they have no idea how to assert their rights.

- Treatment of third parties is an area that requires very thoughtful harmonization between the Insurance Laws and CCPA, in light of the granular contracting requirements with service providers, contractors, and third parties under the newer draft CCPA regulations. CCPA, and the draft CCPA regulations, are not drafted to contemplate many fundamental relationships in the insurance industry. The following are a few examples:
 - The uncertainty is especially significant with regard to independent agents. If the CCPA regulations, as currently drafted, were applied to insurance entities, insurance agents may be considered third parties of insurers, and vice versa. For example, requiring both insurers and agents, who are each regulated under the Insurance Laws, to provide a privacy notice at the point of collection does not make sense when the agent collects information to obtain multiple insurance quotes from regulated insurers—doing so will confuse consumers without gaining them any additional safety or protection.
 - The contractual requirements for “service providers” and “contractors” will require many parties to have to renegotiate existing agreements in similar but differing ways from the existing requirements of the Insurance Laws already overseen by the CDI.
 - Sharing data with other insurance industry parties, including claims aggregators that are critical to the functioning insurance market, may be more complicated if the limitations on “selling” are applied to claims data. It also may not be feasible to engage in such sharing that is necessary for the operations of the insurance industry. The use of claims data to investigate claims, detect and prevent insurance fraud, to price risk, or any other necessary uses of such data, is critical for risk transfer and capital allocation, all also overseen by the CDI. In addition, data sharing with third party service providers that aggregate claims helps satisfy many of the California’s insurance statutory reporting requirements.¹⁸ Should an individual contest or request to delete these records, it may inhibit this reporting, which is in the interest of the greater public.
 - Significant thought needs to be given to how reinsurance and renewal rights transactions will be impacted by the CCPA.
- While the CCPA exempts information that is collected, processed, sold, or disclosed pursuant to the GLBA, FIPA and PNPI,¹⁹ it does not specifically recognize IIPPA in its list of exemptions. This creates confusion as to how the CCPA applies to the insurance industry in terms of the personal information collected and used by insurers. Furthermore, the CCPA’s data-level exemption as opposed to an entity-wide exemption²⁰ brings additional compliance challenges to

¹⁸ E.g., California Earthquake Authority; auto/casualty reporting under Cal. Ins. Code §§ 1875.10-1875.18; child support services under Cal. Ins. Code §§ 13550-13555; theft and salvage under Cal. Ins. Code § 1874.6 and Cal. Code Regs. 10 CCR, § 2191.2; state fraud bureau reporting under Cal Ins Code § 1872.4; Cal. Code Regs. Tit. 10 § 2698.37; Federal NMVTIS Reporting.

¹⁹ Cal. Civ. Code §1798.145(e).

²⁰ As of date of this letter, four states other than California have passed comprehensive privacy laws –Virginia, Colorado, Utah, and Connecticut – all four states exempt both the data *and institutions* subject to the GLBA, whereas CCPA only exempts the data subject to GLBA/FIPA.

the insurance industry, without providing a corresponding benefit to consumers. This requires conducting a burdensome exercise—with no discernable consumer benefit—considering that most personal information collected and used by insurers is subject to the GLBA, FIPA, IIPPA, and PNPI, and a subset of personal information is likely subject to the CCPA’s requirements. Given the current language in Cal. Civ. Code §1798.185(a)(21),²¹ it appears that there is likely a significant amount of data subject to the exemption (i.e., data subject to the GLBA, FIPA and PNPI) that is excluded from CCPA. It is therefore appropriate for the Agency to work closely with the CDI in the manner that the CDI requested with regard to topic #21 regulations.

- As discussed above, the NAIC is in the process of soliciting regulator and stakeholder comments on revisions to its, or replacement of, privacy-related Model Acts, and as such, IIPPA and PNPI are likely to be revised. The NAIC Privacy Protections Working Group is reviewing and considering the requirements and legislative development of relevant privacy laws, including the CCPA/CPRA, GDPR, GLBA, FCRA, and HIPAA, in its efforts to update state insurance privacy protections regarding the collection, use, and disclosure of information gathered in connection with insurance transactions and will be making recommended revisions to, or replacement of, Model Act #670 and Model Regulation #672.²²

On November 8, 2021, the CDI responded to the Agency’s request for comments on proposed CCPA revised regulations, requesting that the Agency work with the CDI prior to enacting any regulations applicable to the insurance industry.²³ In light of the NAIC’s current evaluation of changes to the privacy model acts, which will affect IIPPA and PNPI, both overseen by the CDI, the comment letter stressed that close coordination between the Agency and CDI is critical.

IV. Reviewing the Additional and New Requirements in the Current Draft CCPA Regulations Are Critical

We address below specific items in the current draft of the CCPA regulations released for comment by the Agency that require careful consideration.

- § 7002 (Restrictions on the Collection and Use of Personal Information)²⁴
 - The draft regulations require that a business’s collection, use, retention, and/or sharing of a consumer’s personal information must 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 draft regulation require that such collection, use, retention, and/or sharing “must be consistent with what an average consumer would expect when the personal information was collected.”²⁵ However, this a complicated standard when applied to the insurance industry, as an average consumer

²¹ “(21) Review existing Insurance Code provisions and regulations relating to consumer privacy, except those relating to insurance rates or pricing, to determine whether any provisions of the Insurance Code provide greater protection to consumers than the provisions of this title. Upon completing its review, the agency shall adopt a regulation that applies only the more protective provisions of this title to insurance companies. For the purpose of clarity, the Insurance Commissioner shall have jurisdiction over insurance rates and pricing.”

²² See NAIC Privacy Protections Working Group, https://content.naic.org/cmte_h_ppwg.htm.

²³ See Preliminary Rulemaking Written Comments – Part 3,

https://cpra.ca.gov/regulations/pdf/preliminary_rulemaking_comments_3.pdf.

²⁴ With respect to an illustrative example (§ 7002(b)(4)), it is unclear if third party data obtained for marketing purposes would be acceptable, unless the entity collecting it provided a clear notice that the data would be used for marketing by other companies.

²⁵ § 7002(a).

may not be aware of insurers' operations, particularly as they relate to pricing risk and planning for losses. An average consumer also may not have knowledge or expectations about how insurers operate and share data with nonaffiliated third parties in the ordinary course of business. We recommend that the Agency consider the exceptions provided under Model Regulation #672, under which certain notice and opt-out requirements for disclosure of nonpublic personal financial information do not apply if insurers disclose such information "as necessary to effect, administer or enforce a transaction that a consumer requests or authorizes," or in connection with "servicing or processing an insurance product or service that a consumer requests or authorizes."²⁶

Similarly, applying an average consumer's expectation standard with respect to retention of personal information may not align with the retention period that is required under the Insurance Laws for the insurance industry to perform certain core insurance functions, such as auditing or administration of consumer disputes and inquiries. An average consumer's expectation around data retention will likely be far lower in duration than the actual retention periods that are needed to perform insurance-related functions and comply with regulatory requirements.

- § 7011 – 7012 (Privacy Policy and Notice at Collection)
 - In addition to the detailed disclosures required by the CCPA, the draft regulations add new disclosure requirements. The complexity and cost of complying with the proposed disclosure requirements will far outweigh any perceived consumer benefit. For example, insurers' experience in providing disclosures under the Insurance Laws demonstrates that consumers are overwhelmed by lengthy disclosures that provide too much detail. Rather than providing clarity with respect to a business's collection and use of personal information, consumers are more likely to ignore lengthy disclosures. Further, because many insurance customers already receive a notice relating to insurance practices, providing lengthy disclosures in addition to such notice will bring complexity and confusion to customers.
 - In connection with the notice at collection, the draft regulations require that businesses provide the data retention period for each category of personal information, or if that is not possible, the criteria used to determine the period of time such information will be retained.²⁷ However, it is complicated for insurers to provide and align the record retention period to each category of personal information, because the retention period required by Insurance Laws vary depending on the purpose of the collection and use of personal information. For example, identifier information may be retained for a longer period for underwriting purposes than for marketing.

Additionally, for businesses that collect personal information from consumers online, the notice at collection section requires businesses to provide a link that takes the consumer directly to the specific section of the privacy policy that contains the required information. The draft regulations further provide that 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 does not satisfy this standard. However, this may not provide the full or accurate context of a business's data collection to consumers as many privacy policies explain a business' data collection both online and offline locations, especially in the context of insurance. As such, we suggest that the draft regulations

²⁶ Model Regulation #672, Section 16A.

²⁷ § 7012(e)(4).

allow such notice to direct consumers to the full privacy notice instead of a specific section.

- § 7023 (Right to Correct)

- Operationalizing the right to correct requirements in the draft regulations may bring compliance challenges for businesses. The draft regulations require businesses to instruct all service providers and contractors that maintain the personal information at issue to make the corrections in their respective systems.²⁸ Specifically, with respect to data brokers, an illustrative example provides that a business must correct information that it received from a data broker when a business receives a request to correct and determines that the information is inaccurate. A business must also ensure that the corrected personal information is not overridden by inaccurate personal information subsequently received from the data broker.²⁹ This requires businesses to review the accuracy of information each time it receives information from data brokers and be responsible for correcting inaccurate information. In relation to denying a request to correct, it is also burdensome for businesses to be responsible for informing other persons with whom it discloses, shares, or sells the personal information, that the accuracy of the personal information is contested by the consumer.³⁰

Additionally, the right to correct may result in unintended consequences for the insurance industry. For example, insureds should be required to utilize existing mechanisms under the Insurance Laws to request that their claims related information and determinations be reviewed for change, instead of using the CCPA's right to "correct."

- § 7024(h) (Request to Know)

- In response to a request to know, the draft regulations require that a business provide personal information that the business's service providers or contractors obtained as a result of providing services to the business.³¹ Although the draft regulations require service providers or contractors to provide assistance to the business in responding to such requests, this requirement appears to expand the current scope of the law which may be impossible or would require disproportionate effort, particularly for large businesses. In practice, it would require a significant effort and time, which may be impractical to complete, for a large business to reach out to every service provider or contractor for each right to know request that the business receives, compile the information, and have such information delivered to the consumer within the timeline required under the draft regulations. This problem is especially acute in the insurance industry, as parties may have independent regulatory obligations as a result of overlapping relationships with consumers over time (e.g., as an insurance applicant, as an insured, as a claimant), each relationship requiring the use of different service providers. Providing such information may go beyond what an average consumer reasonably expects to receive when submitting a right to know request. As such, we recommend removing this new requirement from this section.

- § 7027 (Requests to Limit Use and Disclosure of Sensitive Personal Information)

²⁸ § 7023(c).

²⁹ § 7023(c)(1).

³⁰ § 7023(f)(3).

³¹ § 7024(h).

- We request clarification regarding a consumer’s ability to limit use and share sensitive personal information. The CCPA provides that the right to limit does not apply to “sensitive personal information that is collected or processed without the purposes of inferring characteristics about a consumer.”³² The draft regulations require businesses to provide the right to limit if a business uses or discloses sensitive personal information for purposes other than those set forth in § 7027(l). In other words, while subsection (l) recognizes certain activities that the statute indicates are not subject to providing the right to limit, this subsection does not explicitly recognize the CCPA’s exception in § 1798.121(d). As such, we request that the Agency delete or revise § 7027 to ensure that it cannot be misread as purporting to override or nullify the statutory “inferring characteristics” exception to the right to limit. Additionally, the Agency should take care in the application of such limitations to insurance operations concerning underwriting, fraud detection, and claims.
- § 7020 (Methods for Submitting Consumer Requests)
 - If a business does not operate exclusively online, the draft regulations require that the business provide two or more designated methods for submitting requests to delete, correct, and know.³³ For businesses that maintain an internet website, one of the methods for submitting these requests must be through the website, such as through a webform. Further, the draft regulations no longer recognize providing a toll-free phone number as one of the acceptable methods under this section. We recommend that the draft regulations allow businesses to utilize a telephone or toll-free number in receiving these requests from consumers. For example, insurers may provide an opt-out to consumers to limit the sharing of certain personal information as part of their GLBA, FIPA and PNPI compliance, and insurers may provide to consumers a telephone number (such as by a toll-free number), an online method (such as a website), or a mail-in form. Because many insurers already have in place a well-functioning method in receiving an opt-out request from consumers, we recommend the draft regulations allow businesses to provide a telephone number to consumers, which will allow consumers to easily exercise their rights in a single phone call. We also recommend that the draft regulations allow insurers to choose two methods that would be the most effective in honoring consumer rights, rather than requiring a webform by default. For example, for certain segments of the insurance industry, such as workers’ compensation, a webform would not be a practical method in receiving requests from many injured workers.
- § 7025 (Opt-Out Preference Signals)
 - Under the draft regulations, businesses must honor opt-out preference signals that meet certain technical requirements regarding opt-out of sale or sharing of personal information.³⁴ This presents practical challenges for businesses to implement opt-out rights given the lack of consistency and technical guidance on such opt-out preference signals. As such, we request that the Agency consider making this opt-out preference signals optional instead, but require businesses to indicate in their privacy policies whether the business processes the opt-out preference signals. This approach will be similar to how a commercial website operator is required to disclose in a privacy policy

³² Cal. Civ. Code § 1798.121(d).

³³ § 7020(b).

³⁴ § 7025(b), (e).

whether it responds to web browser “Do Not Track” signals under the California Online Privacy Protection Act.³⁵

- § 7051 (Service Providers and Contractors)
 - § 7051 (Contract Requirements for Service Providers and Contractors). The draft regulations require service provider or contractor contracts to identify the specific business purposes and services for which personal information will be processed on behalf of the business and prohibit describing such purposes in generic terms, such as referencing the entire contract generally.³⁶ Under the draft regulations, a person who does not have a contract that complies with these specific requirements is not a service provider or a contractor under the CCPA.³⁷ Businesses must update and renegotiate service provider and contractor contracts to meet these requirements, which can be a burdensome and onerous task, particularly for large organizations that have thousands or more service providers and contractors that process personal information on behalf of the business. If a business engages a service provider or contractor for processing personal information for different business purposes under a number of contracts, the business may need to amend each contract with a supplier to meet these new requirements. It is common for businesses to address the need for enterprise-wide amendments through use of blanket addenda, so as to efficiently and expeditiously address needed or desired changes. The specificity requirement will frustrate an efficient means of compliance and provide no added protection to California consumers. We request that the draft regulations would allow businesses to attach a CCPA addendum or a similar data processing agreement which makes a general reference to or incorporates all of the underlying contracts between the parties for the specific purposes for which information is being disclosed or processed.
 - § 7051(e) (Service Provider/Contractor Due Diligence). The draft regulations add a duty to conduct due diligence on service providers and contractors for the business to exercise its liability defense for the service provider’s or contractor’s CCPA violations. The draft regulations provide that if a business does not audit or test the systems of the service provider or contractor, then the business might not be able to rely on the defense that the business reasonably believed that the service provider or contractor intended to use the personal information in compliance with the CCPA and its regulations. In practice, it is almost impossible to conduct a regular audit on each service provider or contractor. Assessments are generally done in a risk-based manner, with the service providers who are considered to pose the highest risk bearing the highest scrutiny. For large businesses, it will be impossible to conduct audits on all service providers or contractors. For small businesses, they may not have the appropriate resource to conduct such audits. A business should be able to rely on a service provider’s compliance with the terms of a contract without the need for audits, absent reason to believe that the third party is not in compliance. Additionally, if the service provider or contractor is directly regulated by CCPA or the Insurance Laws (or the equivalent insurance laws in other states, or similar federal laws or regulations), the business should be able to rely on a statement of compliance. As such, we recommend removing this requirement, or in the alternative, adopting a more practical approach, such as providing an option to audit only if there is a

³⁵ BPC § 22575(b)(5).

³⁶ § 7051(a)(2).

³⁷ § 7051(c).

reason to believe that there is a potential CCPA violation by the service provider or contractor in connection with their processing of personal information.

V. Conclusion

The APCIA believes a deep understanding of the insurance industry is necessary as the Agency drafts any regulations to avoid duplicative efforts and promote certainty on consumers and regulated entities. APCIA members respectfully suggest that the Agency consider these efforts, and coordination with the CDI, when exercising its rulemaking authority with respect to topic #21.

Until the rulemaking on topic #21 is fully addressed and finalized, the APCIA respectfully requests that the Agency and the California Office of the Attorney General declare a moratorium on enforcement of CCPA and its regulations in the insurance sector. Ideally, the moratorium should include: any enforcement activity until the insurance-specific regulations are in effect, and any retroactive enforcement relative to acts and omissions prior to the effective date of the regulations. Absent this moratorium, insurers will invest significant time and resources on compliance decisions that do not meaningfully expand current consumer rights, which are already covered by existing insurance-specific privacy laws and will almost certainly need to be revisited when the insurance-specific regulations are issued. This will be confusing for Californians, who already enjoy significant privacy protections under GLBA, FIPA, IIPPA and PNPI.

We also request that the Agency consider reviewing the existing cybersecurity audit and risk assessment requirements under the PNPI in relation to topic #21 and topic #15 (cybersecurity audit and risk assessment)³⁸ in future draft(s) of the CCPA regulations. In relation to topic #16 (use of automated decision-making technology),³⁹ we note that the use of artificial intelligence (“AI”) in insurance is intensely focused on by the CDI and NAIC. In fact, NAIC’s Big Data and Artificial Intelligence Working Group has multiple ongoing workstreams, such as reviewing the use of AI and machine learning (“ML”) in the insurance business and evaluating AI/ML regulatory frameworks and governance.⁴⁰ In providing guidance on topic #16 in future CCPA draft regulations, we respectfully request that the Agency consider the need for delayed enforcement regarding businesses’ use of automated decision-making technology, given that the CCPA currently only provides a high-level conceptual overview on this issue. Significant time will be needed for businesses to understand the scope and the specific requirements on their use of automated decision-making technology, as well as to develop, implement, and operationalize a compliance program.

Thank you for the opportunity to provide comments. We look forward to continuing engagement to help develop effective CCPA regulations for the insurance industry.

³⁸ Cal. Civ. Code §1798.185(a)(15).

³⁹ Cal. Civ. Code §1798.185(a)(16).

⁴⁰ See NAIC Big Data and Artificial Intelligence Working Group, https://content.naic.org/cmte_h_bdwg.htm.

From: **Josh Stevens** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
CC: **Michele Shuster** [REDACTED]; **Alex Walker**
Subject: CPPA Public Comment
Date: 23.08.2022 22:21:17 (+02:00)
Attachments: PACE CPRA Regs. Comments (08-23-2022) .pdf (9 pages)

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

Good afternoon,

Please find attached comments on behalf of the Professional Association for Customer Engagement to the proposed regulations under the California Privacy Rights Act.

Thank you,

Josh



Josh Stevens | CECF | CIPP/US

Partner | [Mac Murray & Shuster LLP](#)

4555 Lake Forest Drive, Suite 650, Cincinnati, Ohio 45242

P: 513.563.3020 D: [REDACTED]

M: [REDACTED]

[mslawgroup.com](#)



Confidential Communication: This message contains confidential information that may not be disclosed or provided to third parties. If it has been received in error, please reply to advise the sender of the error and then immediately delete this message.



August 23, 2022

VIA EMAIL

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

RE: Comments on Proposed Regulations under the California Privacy Rights Act

Dear Mr. Soublet:

The Professional Association for Customer Engagement (“PACE”)¹ respectfully submits the following comments to the California Privacy Protection Agency’s (“Agency”) proposed regulations under the California Privacy Rights Act. PACE’s membership seeks to consistently improve the consumer experience and protect consumer preferences with regard to the use of their data and how they engage with members. PACE offers the following comments to highlight particular areas of the proposed regulations that create concern or open avenues for ambiguity that could harm consumers and businesses alike.

1. § 7002. Restrictions on the Collection and Use of Personal Information.

Subsection (a) mandates that “[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.” Such collection, use, retention, and/or sharing is “reasonably necessary” if, and only if, it is “consistent with what an *average consumer* would expect when the personal information was collected.” Thus, moving forward, courts will determine the legality of data collection, use, and disclosure using this standard two-part test.

An “average consumer” standard, however, is simply unworkable. First, consumers may have wildly differing opinions on how and why a device collects information. For example, suppose Application A and Application B are both plant identification mobile apps offering consumers the ability to take photos of plants and receive information about, including the name of, a plant. The consumer uses Application A for a while, which identifies plants in photos using an algorithm that analyzes visual similarities between the plant in the photo and other photos of plants in its database to produce an identification. The consumer learns of this identification procedure after conducting research on

¹ PACE is the only national non-profit organization dedicated exclusively to the advancement of companies that use a multichannel contact center approach to engage their customers, both business-to-business and business-to-consumer. These channels include telephone, email, chat, social media, web, and text. Our membership is made up of Fortune 500 companies, contact centers, BPOs, economic development organizations, and technology suppliers that enable companies to contact or enhance contact with their customers.

Professional Association for Customer Engagement

Application A. The consumer later begins using Application B, which uses a similar algorithm to determine visual similarity, but also collects geolocation information to narrow the possibilities based on the geographic area in which the consumer is located. The consumer, without doing research, assumes that Application B uses the same procedure for identifying plants as Application A. In fact, in their mind, all plant identification applications probably use the methodology employed by Application A because of first use bias. The consumer may not expect that their geolocation information will be collected to identify plants, and one could argue that this consumer's expectations should form the basis of an "average consumer's" expectations; however, both methodologies are legitimate ways to identify plants.

The above example illustrates not just how expectations across consumers can be different, but also how consumer technical know-how of devices, software, apps, or anything else that collects or uses data can vary significantly. The issue is not necessarily that the average consumer does not expect geolocation data to be used in a plant identification app, but that the consumer does not know (or care) how the plant identification app works. The average consumer may very well have *no* expectations.

The proposed regulation imputes too much subjectivity into a standard that will be analyzed countless times by business compliance officers, attorneys, judges, and juries. One way to remedy the different expectations across consumers is to create a standard of an informed consumer, and consumers can inform themselves of a business's data collection practices by reading the privacy policy. We propose that the regulation reads as follows:

- (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 **who has read the privacy policy and informed him/herself of the business's data collection practices** would expect when the personal information was collected. A business's collection, use, retention, and/or sharing of a consumer's personal information may also be for other disclosed purpose(s) if they are compatible with what is reasonably expected by the average consumer. A business shall obtain the consumer's explicit consent in accordance with section 7004 before collecting, using, retaining, and/or sharing the 6 consumer's personal information for any purpose that is unrelated or incompatible with the purpose(s) for which the personal information collected or processed.*

We believe this is easier to implement and analyze because it creates an objective standard, focusing on what is contained in the privacy policy, rather than what is purely in the "black box" mind of the average consumer.

2. § 7003. Requirements for Disclosures and Communications to Consumers.

Subsection (b) states that the "[d]isclosures required under Article 2 shall also: . . . [b]e available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California." Our issue with this rule arises from the term "other information," which is so broad that it could encompass any language use by a business at any time. Suppose a car dealership in California only conducts business using English, but when a Laotian-speaking customer comes in seeking to buy a vehicle, one employee, who happens to speak

Laotian, speaks with them to discuss the features of products in Laotian. When this employee tells the customer that a particular vehicle has 50,000 miles on it using Laotian, the business has given the consumer “other information” in a language other than English, meaning the dealership must now give Article 2 disclosures to the consumer in Laotian. Preparing Laotian disclosures would be unforeseen by the business, and likely a serious burden. Compare this with a more reasonable example: a grocery store that sells Korean food products in a Korean neighborhood that frequently makes advertisements and sales announcements in Korean. The use of Korean by this business would be wholly expected. This business, because it so often communicates with customers in Korean, *should* make disclosures in Korean. To accord the regulations more completely with business realities, we suggest the following change to this subsection:

(b) *Disclosures required under Article 2 shall also:*

...

- (2) *Be available in the language(s) in which the business in its ordinary course **primarily interacts with consumers** ~~provides contracts, disclaimers, sale announcements, and other information to consumers in California~~*

This language will prevent a business from preparing entirely new disclosures after incidental use of a foreign language and thereby benefit consumers by reducing the risk of businesses prohibiting consumer interactions in foreign languages entirely.

3. § 7004. Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent.

In order to provide simple mechanisms for consumers to submit a CCPA request and give consent to a business, the Agency has proposed that forms pertaining to requests and consent are (1) “[e]asy to understand”; (2) provide for “[s]ymmetry in choice”; (3) “[a]void language or interactive elements that are confusing to the consumer”; (4) “[a]void manipulative language or choice architecture”; and (5) be “[e]asy to execute.”

Clause (a)(4)(A) offers examples of “manipulative language or choice architecture”: “[w]hen 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.”

First, given the example, there is no clear delineation between manipulative and non-manipulative language. If a business paired a “Yes” choice alongside a choice that read “No, I will pay full price,” is that manipulative? Is anything other than a “Yes”/“No” dichotomy manipulative? If adopted, this proposal will force businesses to examine a large bulk of their advertising language with a microscope, yet they will have no way of knowing what marketing language complies with this highly subjective standard except through trial-and-error risking penalties.

Second, the proposal has the effect of punishing businesses who inform consumers of the consequences of their choices and thereby chilling legitimate constitutionally-protected commercial speech. If a consumer reads nothing else on the page and then reaches the point where they will make a final choice, they should, at the very least, know the direct material effect of their selection. This pairs with the first point above—a choice architecture the appears manipulative may actually have the effect

Professional Association for Customer Engagement

of assisting the consumer with their choice. Consumer choices about data sharing do not occur in a vacuum. Consumers conduct cost-benefit analyses daily in their interactions with the marketplace. An architecture does not “subvert” their choice just because it informs them that one choice has a greater economic effect than the other.

We do, however, consistent with our core principles, agree that no business should ever harass² the consumer. Additionally, providing clear opt-in/opt-out mechanisms, such that the consumer knows exactly the choice they are making, will facilitate commerce. We offer the following changes to the proposed regulation:

- (4) *Avoid manipulative language or choice architecture. The methods should not use language or wording that guilts or shames the consumer into making a particular choice or bundles consent so as to subvert the consumer’s choice. However, a statement of fact alongside the choice architecture that informs the consumer of the financial or other impact of their decision while not making a claim about the consumer’s motives or state of mind will not be construed as manipulative, guiltting, or shaming. 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. When offering a financial incentive, pairing choices such as, “Yes, I will receive [x]% off” with “No, I will pay full price” is not manipulative or shaming.*

....

4. § 7011. Privacy Policy.

Section 7011(e)(3)(F) requires businesses to insert an “[e]xplanation of how an opt-out preference signal will be processed for the consumer . . . and how the consumer can use an opt-out preference signal” into its privacy policy. This regulation makes the assumption that opt-out preference signals have the same mechanism for processing, but the truth is that these are still a nascent technology and the nuts-and-bolts of their use on browsers is not consistent across providers of these signals. In fact, the proposed regulations under § 7025 provide a multitude of examples on how and when a business should process these signals. At least for purposes of the privacy policy, it would be burdensome for a business to conceptualize all the ways they might process these signals and for a consumer to read all the possible permutations. Instead, a business should be required only to inform the consumer that they will process the signals they come across and provide a general description of how they will process the Global Privacy Control opt-out signal, the industry-leading opt-out signal:

² We also have concern with use of terms like “guilt” or “shame” which reflect a consumer’s subjective personal experience and are much less capable of objective interpretation by a court or regulator as opposed to a term like “harass” which focuses on a standard of conduct and has a substantial body of case law in other realms from which to draw understanding.

(e) The privacy policy shall include the following information:

...

3. An explanation of how consumers can exercise their CCPA rights and **what** consumers can expect from that process, which includes the following:

...

~~(F) Explanation of how an opt-out preference signal will be processed for the consumer (i.e., whether the signal applies to the device, browser, consumer 14 account, and/or offline sales, and in what circumstances) and how the consumer can use an opt-out preference signal~~ **A statement that the business will process opt-out preference signals it encounters and an explanation of how it process the Global Privacy Control (GPC) opt-out preference signal;**

5. § 7012. Notice at Collection of Personal Information.

The proposed regulations would require businesses to provide a notice of collection to consumers “at or before the point of collection,” providing information enabling them to “exercise meaningful control over the business’s use of their personal information.” The information to be contained in a notice of collection is robust. We question whether consumers will actually read the notice at the point of collection, since it will likely be almost as long as a business’s privacy policy. Additionally, if the notice is a document separate from the privacy policy, it is likely to confuse or annoy the consumer, who may not recognize the difference between the two. While the proposal gives businesses the option of placing the notice in the privacy policy and providing a link to it at the point of collection, we recommend the Agency permit the business to direct the consumer to the privacy policy, since the aim of the privacy policy is to be the singular resource that contains all of a business’s privacy practices. We believe the regulations should read as follows:

(c) ~~The **information contained in the** notice at collection shall be made readily available where consumers will encounter it at or before the point of collection of any personal information included in the business’s privacy policy.~~

...

(f) ~~If a business collects personal information from a consumer online, the **notice at collection may consumer shall** 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 (b)(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.~~

Furthermore, the regulations explain that the notice of collection must be made in offline situations, as well. Example (5) under subsection (c) provides a bizarre and wholly unrealistic scenario. It reads, “[w]hen a business collects personal information over the telephone or in person, it may provide that notice orally.” First, this example uses the word “may,” suggesting that providing the notice over the phone is optional, which seems to contravene the goals of § 7012. But more importantly, if the

Professional Association for Customer Engagement

business did in fact provide the notice orally, a miserable customer experience would ensue. Imagine suffering through a phone call as the business's representative on the other line reads-off the notice of collection.

If the Agency truly intended to make the oral disclosure of the notice optional in these circumstances, then we suggest the regulation remain in place. In fact, we recommend this be the reading of the regulation, since it is more realistic and saves the quality of the consumer's interaction. If, however, the Agency intended to mandate the oral disclosure of the notice of collection, we suggest offering alternative methods for providing it to the consumer:

(c) . . .

- (5) *When a business collects personal information over the telephone or in person, it may provide the notice ~~orally~~ **by stating the link or webpage where the privacy policy can be found or delivering the notice through electronic means, such as email or text message.***

6. § 7013. Notice of Right to Opt-Out of Sale/Sharing and the "Do Not Sell or Share My Personal Information" Link.

The notice of right to opt-out is intended "to inform consumers of their right to direct a business that sells or shares their personal information to stop selling or sharing their personal information" Much like the notice of collection, above, it will yet another lengthy document for the consumer to sift through. These regulations embrace the principle that the consumer's experience in handling their data should be frictionless, yet they continue to layer more on more notices on top of each other. The most frictionless place to provide these notices is in the privacy policy, and while the regulations give businesses the option of doing this, we recommend making it mandatory. Thus, we offer the following changes to this section:

- (e) *A business that sells or shares the personal information of consumers shall ~~provide~~ **place** the notice of right to opt-out of sale/sharing ~~to consumers as follows:~~ **in its privacy policy. The section of the privacy policy containing the notice of right to opt-out shall be titled "Notice of Right to Opt-Out." A business shall provide a link to the privacy policy section containing the notice of right to opt-out of sale/sharing, or the notice itself, to consumers as follows:***

- (1) *A business shall post **a link that leads the consumer to the privacy policy section containing** the notice of right to opt-out of sale/sharing on the internet webpage to which the consumer is directed after clicking on the "Do Not Sell or Share My Personal Information" link. The notice shall include the information specified in subsection (f).*

. . . .

7. § 7014. Notice of Right to Limit and the "Limit the Use of My Sensitive Personal Information" Link.

Our criticism of the Notice of Right to Limit follows the same line of reasoning as the notices previously discussed: adding these to the regulatory regime is inconvenient for the consumer. We suggest the regulation reads as follows:

- (e) *A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in section 7027, subsection (l), shall ~~provide~~ **place** the notice of right to limit*

~~to consumer as follows:~~ in its privacy policy. The section of the privacy policy containing the notice of right to limit shall be titled “Notice of Right to Limit the Use of My Sensitive Personal Information.” A business shall provide a link to the privacy policy section containing the notice of right to limit, or the notice itself, to consumers as follows:

- (1) A business shall post *a link that leads the consumer to the privacy policy section containing* the notice of right to limit on the internet webpage to which the consumer is directed after clicking on the “Limit the Use of My Sensitive Personal Information” link. The notice shall include the information specified in subsection (f).

....

We believe, as a general guiding principle applicable throughout these regulations, all information related to the handling of consumer data, whether by a business, the consumer, or a third party, should be placed in the business’s privacy policy. Consumers want a single point of reference for all their data management questions and needs. Abiding by this principle will ensure that.

8. § 7023. Requests to Correct.

We believe this section creates a smooth and streamlined regime that will allow consumers to easily correct their personal information. Our only objection arises out of subsection (i), which states that “[w]here the business is not the source of the information that the consumer contends is inaccurate, in addition to processing the consumer’s request, the business shall provide the consumer with the name of the source from which the business received the alleged inaccurate information.” Retrieval of this information is not as easy as this proposed regulation seems to suggest. It is not common for businesses to structure their databases in such a way that tracks the source of a particular data element. To reconfigure established databases to track the data source would often require a vast overhaul of the software underlying it, resulting in extraordinary expenses that were unanticipated by the statute. For existing data, businesses often simply will not be able to identify the source. We recommend modifying this subsection using the new “disproportionate effort” definition placed in the regulations and used in other sections:

- (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 provide the consumer with the name of the source from which the business received the alleged inaccurate information if known or capable of being known, unless this proves impossible or involves disproportionate effort.*

9. § 7025. Opt-Out Preference Signals.

As stated previously, opt-out preference signals are an emerging technology; the processes for implementing and processing these browser signals have yet to be standardized outside of the Global Privacy Control; thus, implementing and processing them amounts to a technological ordeal.

Opt-out signals present further problems when the realities of commerce come into view. These signals are digital artifacts that are utilized only when a consumer interacts with a business via a web browser—but consumers do not interact with businesses only on the web potentially creating scenarios

for conflicting opt-out preferences related to a single consumer and redundant opt-out requests. These challenges have not been fully considered and resolved.

We recommend that the Agency take three actions. First, adjust the regulations to limit the opt-out preference signals which a business must recognize to only those specifically approved by the Agency. Second, officially approve Global Privacy Control as the sole opt-out preference signal standard at this time. Third, stay implementation of any requirements related to recognizing and honoring opt-out preference signals until January 1, 2024 to allow businesses additional time to work through the unique technical challenges they pose and the Agency time to issue additional guidance to assist businesses in this regard. These steps will provide clarity for consumers as to the particular signal standard that will be honored, and allow a better-designed consumer experience.

10. § 7026. Requests to Opt-out of Sale/Sharing.

This section, which is crucial to the effectiveness of the CPRA, requires business to provide consumers with “two or more designated methods for submitting requests to opt-out of sale/sharing.” The Agency, recognizing that many businesses operate websites and brick-and-mortar stores, states in the proposed regulations that businesses “may provide an in-person method for submitting requests to opt-out of sale/sharing” Later, the regulations state that a business must comply with a request to opt-out of sale/sharing by “providing a means by which the consumer can confirm that their request to opt-out . . . has been processed by the business.” The example offered-up states that a business’s website could display “Consumer Opted out of Sale/Sharing.”

Confirmation of a consumer’s request on a business’s website will not always be possible, however, in instances where a consumer makes an in-person request. Suppose a consumer enters the retail store of a business and submits a request to opt-out via a paper form. The consumer later visits the website of the retailer, who offers the consumer the ability to create an account or browse the online store without creating an account. If this consumer is not logged-into an account that is connected to the opt-out form they previously submitted, the website has no way of knowing which consumer is browsing and consequently cannot confirm that the consumer has opted-out by displaying a message on its website, or by any other means. Through no fault of the business, it has run afoul of the regulation.

But the above example is just one of many instances where a website might be unable to confirm a consumer’s opt-out. If an opt-out preference signal is communicated to a business via the consumer’s device (connected with a specific IP address), what happens when a consumer uses a different device or a VPN? This section is especially concerning given the fairly extensive usage of public devices. The scheme contemplated by this section is completely futile if a business cannot readily identify a consumer, whether online or offline.

We recommend changing this section to require business to confirm only those opt-outs made on a web browser, since these opt-outs will be the most common consumer mechanism:

Professional Association for Customer Engagement

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

...

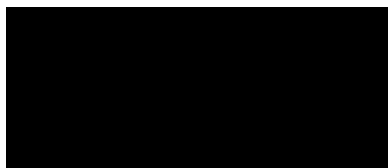
- (4) Providing a means by which the consumer can confirm that their **browser-based opt-out preference signal** request to opt-out of sale/sharing has been processed by the business. For example, the business may display on its website "Consumer Opted Out of Sale/Sharing" or display through a toggle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

11. § 7053. Contract Requirements for Third Parties.


Section 7053(c), after listing the requirements of a contract for the sale or sharing of personal information between a business and third-party in subsection (a), provides that a "[t]hird party that does not have a contract that complies with subsection (a) shall not collect, use, process, retain, sell, or share the personal information received from the business." This regulation does not anticipate that a contract may only be deemed non-compliant after lengthy litigation. A third-party may believe that their contract with a business complies with (a), but later discover, perhaps for complicated legal reasons established through case law, that it is not. These legal reasons may be completely novel, created through a case of first impression, which the business would not have a way of anticipating. We want to make sure third parties are not retroactively punished for their use of information while they operated under a contract they believed to be compliant. Subsection (c) should thus read as follows:

(c) A third party that does not have a contract that complies with subsection (a) shall not collect, use, process, retain, sell, or share the personal information received from the business. A third party collecting, using, processing, retaining, selling, or sharing personal information it received under a contract it in good faith believed to be compliant with subsection (a) shall not be liable for collecting, using, processing, retaining, selling, or sharing it engaged in prior to the time it knew such contract was noncompliant.

Respectfully submitted,



Michele A. Shuster, Esq.
Joshua O. Stevens, Esq.
Alexander T. Walker, Esq.
Mac Murray & Shuster, LLP
General Counsel of PACE

6525 West Campus Oval
Suite 210
New Albany, Ohio 43054
T: (614) 939-9955
E: 

From: **Natalie Boust** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 22:25:39 (+02:00)
Attachments: Consumer Privacy Act on Package Shipping.pdf (7 pages)

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

Dear Mr. Soublet,

Please find attached the feedback from the California Business Roundtable regarding the California Consumer Privacy Act. We appreciate the opportunity to submit comments to the Agency on this important issue.

Regards,
Natalie Boust



**California
Business
Roundtable**

Natalie Boust

Legislative Coordinator

1301 I Street | Sacramento | 95814

(916) 553-4093 | [REDACTED]

Leadership for Jobs and a Strong Economy



August 23, 2022

Via Email to regulations@coppa.ca.gov

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

Re: CCPA Public Comment

Dear Mr. Soubllet:

The California Business Roundtable (CBRT) appreciates the opportunity to submit comments to the California Privacy Protection Agency (CPPA) as part of the CPPA's rulemaking process under the California Consumer Privacy Act (CCPA). CBRT represents California's largest employers, advocating for jobs and a strong economy in our state and nationwide.

We appreciate the effort that the CPPA has dedicated to proposing regulations (the "Proposed Regulations") to further the purposes of the CCPA. We have reviewed the CPPA's proposal and respectfully submit our feedback for your consideration on behalf of CBRT.

A. THE CCPA AND THE PACKAGE TRANSPORTATION INDUSTRY

The CCPA regulates package transportation providers as businesses operating in California that collect personal information relating to California consumers. For package transportation companies, certain unique CCPA issues arise from the fact that a significant portion of the personal information processed in core, day-to-day operations is received not directly from consumers, but instead from retailers and other corporate customers. This information takes the form of addressing details and package-related information, such as package dimensions and weight (collectively, "Shipping Information").

For example, when a consumer buys a pair of shoes online, the online shoe retailer provides a package to a carrier along with associated Shipping Information. Consumers not only expect this information sharing, they in fact require it when they pay retailers and manufacturers to arrange for the shipping of products they have purchased.

The necessity of data sharing as a feature of daily package transportation operations raises several key questions under the CCPA. Our comments below relate to the issues we view as most critical:

1. Sharing Shipping Information with package transportation companies should not constitute a "sale" of personal information.
2. This is critical because a different finding would mean transportation providers receive Shipping Information only as "service providers" – a result that would be inconsistent

Leadership for Jobs and a Strong Economy

with consumer expectations and would significantly impair the transportation industry, with no corresponding consumer benefit.

B. COMMENTS OF THE CALIFORNIA BUSINESS ROUNDTABLE ON THE PROPOSED REGULATIONS

1. Sharing Data with Package Transportation Companies to Ship Packages Should Not be Deemed a “Sale” of Personal Information.

CBRT respectfully submits that it is critical to the package transportation industry to confirm that retailers and other corporate customers do not “sell” Shipping Information when they provide that information to transportation providers. This clarification is critical, due to the scope of the definition of “sell” in the CCPA, because transportation providers inherently use Shipping Information for more than simply to deliver each individual package to each individual address. Shipping Information is inherently embedded into the operations of transportation providers, similar to how an organization might consume and integrate fuel or other supplies into its operations. For example:

- Carriers use Shipping Information continuously and on an automated basis for package routing within their networks; transportation and delivery planning and optimization; and to make decisions about package network optimization (including locations of facilities, retail outlets, staffing, “drop boxes” where consumers can pick up and leave packages, and capital investment). They do not simply use the information to deliver a specific package and then forget it.
- Shipping Information constitutes a combination of information received from customers, plus information carriers append from their own historical information and operations (including very specific details of package handling, status, and routing within a package network), and information they receive from third parties. The individual elements received from customers are integrated into this data and are not reasonably capable of being pulled back out.
 - Carriers continuously and automatically update Shipping Information about individual packages with additional information concerning individual shipment attributes, and operational details and requirements for shipments meeting such attributes (e.g., handling of a particular package due to its dimensions and weight (“DimWeight”) or service level (e.g., standard vs. priority)) in order to fulfill deliveries and operate and improve the carrier’s package transportation network. Carriers do this in order to route large numbers of deliveries to the right place at the right time, to manage the transportation network, and to improve the shipping network for future deliveries.
 - One of the more prominent examples of this is addresses: annually, carriers often correct tens or hundreds of millions of addresses that customers have submitted to them using information carriers collect while delivering packages, or from data acquired from, e.g., the US Postal Service. Once an address is corrected, it enables future shipments from any other corporate customer to reach that same address as desired by the consumer(s) resident at that address.

The use of Shipping Information by transportation providers beyond the simple delivery of each individual package to each individual address, when requested not by the individual consumer but by a retailer or other corporate customer, could therefore be considered to result in a sale of that information by the retailer to the carrier, but for the exception in Cal. Civ. Code § 1798.140(ad)(2)(A) (operative Jan. 1, 2023).

- Subsection 1798.140(ad)(2)(A) provides that a business does not “sell” personal information when consumers “direct the business to . . . intentionally disclose personal information.” This is precisely what happens when consumers order goods from carriers’ corporate customers that need to be shipped.
- Specifically, when consumers buy products, they are directing retailers and other corporate customers to disclose Shipping Information to a transportation provider, instead of making their own separate arrangements with a transportation provider directly or, when applicable, retrieving the merchandise from the corporate customer’s facility. In fact, consumers generally pay a separate and extra charge for shipping, arguably affirmatively obligating the corporate customer to share information with a transportation provider for shipping purposes.
- To exempt consumer-directed data disclosures from being a “sale,” the CCPA does not require that the consumer specify precisely who should receive their personal information. Instead, the § 1798.140(ad)(2)(A) requires only that the consumer “direct” a retailer or manufacturer to “intentionally disclose” their information. Consumers who purchase merchandise from retailers or manufacturers have exactly this in mind – that their data will be provided to a carrier that will deliver the merchandise to them.

Shipping Information remains protected under the CCPA in the hands of the carrier. Carriers are businesses that determine the purposes and means of the processing of Shipping Information and must comply with the CCPA, including the various privacy obligations and protections established by the statute. This information is also protected by a longstanding federal law that regulates its handling and disclosure.¹

CBRT believes the plain meaning of the CCPA establishes that retailers and other corporate customers transfer Shipping Information to transportation providers outside the definition of a “sale” pursuant to the direction of the consumer purchasing the product. But our members are seeing certain corporate customers interpret the law differently, positioning carriers as “service providers” as defined in the CCPA, out of a concern that disclosing data to a separate “business” carries a “sale” risk. This designation would prevent package transportation providers from being able to use Shipping Information for any purpose beyond delivering each individual package – a result that will impair operations across the industry with no corresponding consumer benefit. CBRT therefore respectfully requests the CPPA to clarify the application of Section 1798.140(ad)(2)(A) to Shipping Information that transportation providers receive from businesses, pursuant to the CPPA’s rulemaking authority under Cal. Civ. Code § 1798.185(b).

¹ See 49 U.S.C. § 14908.

2. Clarifying that the Sharing of Package Information Is not a “Sale” Is Critical to the Package Transportation Industry, because Deeming Transportation Providers as “Service Providers” Would Fundamentally Impair the Industry’s Ability to Operate, with no Corresponding Benefit to Consumers.

A finding that transportation providers receive Shipping Information as “service providers,” and not pursuant to the direction of the consumer under Cal. Civ. Code § 1798.140(ad)(2)(A), would fundamentally impair transportation industry operations and would be inconsistent with consumer expectations.

a. Consumers Have Direct Relationships with Package Transportation Providers.

When an individual consumer directly hires a carrier to ship a package, that carrier clearly acts as a business with respect to the consumer, not a service provider. The carrier thus has the corresponding obligations of a business under the CCPA, such as to accept and fulfill requests to know and requests to delete.

But if carriers are deemed to constitute service providers, and not businesses, when the shipper happens to be a corporate customer, then the carrier’s obligation will be to direct a consumer submitting a request back to the corporate customer. This is an inefficient result which would create a risk of consumer confusion. Indeed, our members’ experience is that consumers continue to see themselves as having direct relationships with the individual carriers delivering shipments to them, whether in connection with tracking shipment status, submitting claims, or requesting privacy-related information.

b. A “Service Provider” Designation under the CCPA Will Create Fundamental Operational Issues for the Package Transportation Industry.

The designation of transportation providers as “service providers” would also create a more fundamental problem. This is because, as we discuss in [Part 1](#) above, transportation providers inherently use Shipping Information received about an individual package for more than simply to deliver that package to the designated destination address. Shipping Information is inherently embedded into the operations of transportation providers and is therefore used for other transportation, planning, and operational purposes in the future.

Section 7050(b) permits service providers to use personal information for several purposes beyond delivering the requested service back to the business. One such use is “[f]or internal use by the service provider or contractor to build or improve the quality of its services uses of personal information.” The regulations provide two examples, one of which references transportation companies:

(B) A shipping service provider that delivers businesses’ products to their customers may use the addresses received from their business clients and their experience delivering to those addresses to identify faulty or incomplete addresses, and thus, improve their delivery services. However, the shipping service provider cannot compile the addresses received from one business to send advertisements on behalf of another business, or compile addresses received from businesses to sell to data brokers.

But this fails to acknowledge that carriers use shipping data in the form of package level detail or “PLD” for other operational purposes beyond service improvement, such as to perform advanced route optimization and network planning. These uses are essential to the ability of carriers to compete and improve the efficiency of the flow of goods in the economy, but would be prohibited by the draft regulations if shipping companies are deemed service providers. Even if this interpretation is incorrect – which CBRT believes to be the case – we anticipate corporate customers may take a different position as a risk management measure because of concerns about other potential constructions of the law.

3. The Clarifications Requested by the California Business Roundtable are also Consistent with the Law under the European Union General Data Protection Regulation, which Provides that Package Transportation Providers Are Controllers, not Processors, as to Shipping Information.

The European Union General Data Protection Regulation (the GDPR) is arguably the most comprehensive and protective privacy law in the world. Even in the EU, under the GDPR, package transportation providers are deemed controllers that have the right to determine the purposes and means of the processing of Shipping Information.

- As the members of the CPPA will be aware, the definition of “controller” in the EU is analogous to the definition of “business” in the CCPA, in that both a controller and a business “determine[] the purposes and means” of the processing of personal information. Cal. Civ. Code § 1798.140(c)(1); GDPR Art. 4(7). The GDPR also contains the concept of a “data processor”, which, similar to a service provider under the CCPA, is defined as an entity that processes data on behalf of a controller.
- European regulators who have addressed the issue have consistently found that package transportation companies are best classified as “controllers,” not as “processors.” As an example, the United Kingdom’s Information Commissioner’s Office issued guidance in 2014 stating that a delivery service “will be a data controller in its own right in respect of any data it holds to arrange delivery or tracking ... such as individual senders’ and recipients’ names and addresses.”² More recently, the Bavarian Office for Data Protection Supervision issued 2018 guidance stating that “postal services for letter or package transportation” are generally “not data processing,” but instead “specialized services” offered by “an independent controller.”³

We respectfully suggest that the European practice reflects a recognition of the fundamental, inherent, and accepted purposes for which package transportation providers must use personal information to perform their daily operations at the level expected by both consumers and customers. We request the CPPA to take a similar approach under the CCPA by clarifying the application of Section

² See Information Commissioner’s Officer, *Data Controllers and Data Processors: What the Difference Is and What the Governance Implications Are* at 12 (June 5, 2014), available at <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf>.

³ See Bayerisches Landesamt für Datenschutzaufsicht [Bavarian Office for Data Protection Supervision], *FAQ zur DS-GVO: Auftragsverarbeitung, Abgrenzung* [GDPR FAQs: Data Processing, Distinguishing [between Controllers and Processors]] at 2 (July 20, 2018), available (in German) at https://www.lida.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf.

1798.140(ad)(2)(A) to Shipping Information that transportation providers receive from businesses, pursuant to the CPPA’s rulemaking authority under Cal. Civ. Code § 1798.185(b).

4. The CPPA Should Establish Reasonable Processes for Handling Employee Privacy Requests.

The CCPA as originally drafted applied equally to personal information concerning traditional “consumers” and employees. To address this apparent drafting error, the legislature amended the statute to exclude employee personal information used solely in the context of the employment relationship except with respect to the requirement to provide a notice at collection, and the private right of action for certain data security incidents. Cal. Civ. Code § 1798.145(h)(1). The California Privacy Rights Act retained this limited exemption, but provides that it will expire as of January 1, 2023, subjecting employee personal information to the full panoply of the CCPA’s consumer privacy standards on and after that date. Cal. Civ. Code § 1798.145(n)(3) (operative Jan. 1, 2023).

This means that, among other things, employers will have the obligation to process and fulfill requests to know, for specific pieces of information, to correct, and to delete submitted by their California workforce. CBRT is concerned about the significant new regulatory burden these standards will impose on our members for several reasons:


- Requiring employers to identify, review, and deliver copies of all personal information held about employees will require employers to expend significant new resources, through dedication of personnel and purchases of technology, to locate, catalog, process, and transmit vast new volumes of personal information in electronic and paper form. Much of the personal information businesses retain about employees is “unstructured,” difficult to locate, difficult to search, and created by the employee herself. Employers will also have an obligation to review this information carefully before producing it back to the employee to ensure the protection of other employees who may be identified or identifiable from the data.
- The right to specific pieces of information goes beyond even the rights of employees in litigation. There, discovery requests and compulsory process are at least bounded by discoverability standards and subject to judicial oversight.
- We anticipate requests to know, for specific pieces of information, and to delete will therefore primarily become litigation or pre-litigation tools, not mechanisms for employees to realize important privacy interests.

CBRT therefore respectfully requests the CPPA to exercise its rulemaking authority under Cal. Civ. Code § 1798.185(b) to clarify that the obligation of employers to produce information in response to a request for specific pieces of information is limited to categories such as worker contact, job title and duties, emergency contact, and salary information. We further request that the CPPA clarify that employers may afford reasonable self-service options for employees to request and receive copies of applicable information in response to a request.

* * * * *

We appreciate the California Privacy Protection Agency's review and consideration of our comments in this letter, and look forward to the CPPA's continued efforts through the rulemaking process. Please do not hesitate to reach out to me if you have any questions or require clarification on our comments. We thank the California Privacy Protection Agency for the opportunity to provide our views for consideration, and look forward to working with you to address the matters outlined above.

Sincerely



ROBERT C. LAPSLEY ✓
President

From: **David LeDuc** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
CC: **Leigh Freund** [REDACTED]; **Fatiha Hijazi**
Subject: CPPA Public Comment from the Network Advertising Initiative (NAI)
Date: 23.08.2022 18:34:52 (+02:00)
Attachments: PastedGraphic-2.tiff (1 page), NAI_comments_Proposed CPRA Regulations_082322.pdf (19 pages)

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

Dear Board members and staff of the California Privacy Protection Agency — Please find enclosed comments from the Network Advertising Initiative (NAI) regarding the proposed regulations updating the CCPA. We thank you for the opportunity to provide these comments, and we look forward to continuing to engage with you as you further amend and finalize these regulations.

Best regards,

David LeDuc

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
409 7th Street, NW, Suite 250
Washington, DC 20004
P: [REDACTED]



NIA

PRIVACY, TRUST & ACCOUNTABILITY

CPPA_RM1_45DAY_0741



409 7th Street, NW Suite 250
Washington, DC 20004

August 23, 2022

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

Dear California Privacy Protection Agency,

On behalf of the Network Advertising Initiative (“NAI”), thank you for the opportunity to provide comments on the proposed regulations under the California Privacy Rights Act (“CPRA”).

I. Introduction

A. Overview of the NAI

Created during the nascence of the online advertising industry in 2000, the NAI is one of the internet's longest standing and most respected industry self-regulatory programs, whose members are made up of advertising technology providers in the online advertising ecosystem. For over 20 years, the NAI has promoted strong consumer privacy protections, a free and open internet, and a robust digital advertising industry by maintaining and enforcing the highest standards for the responsible collection and use of consumer data. Our member companies range from large multinational corporations to smaller startups and represent a significant portion of the digital advertising technology ecosystem, all committed to strong self-regulation and consumer trust. As a non-profit organization, the NAI promotes the health of the online ecosystem by maintaining and enforcing strong privacy standards for the collection and use of data for digital advertising across all digital media.

All NAI members are required to adhere to the NAI's FIPPs-based, privacy-protective Code of Conduct (the “NAI Code”), which continues to evolve and recently underwent a major revision for 2020 to keep pace with changing business practices and consumer expectations of privacy. The NAI continues to monitor state and federal legal and regulatory changes, and our Code evolves to reflect—and in some cases exceed—those requirements. Member compliance with the NAI Code is promoted by a strong accountability program. NAI attorneys subject each NAI member to a comprehensive annual review of their businesses and data collection and use practices for adherence to the NAI Code. In addition, NAI staff advises companies on an ongoing basis about how to best comply with the Code and guidance, and how to implement privacy-first practices. Finally, the NAI team conducts technical monitoring and review of company opt outs and privacy tools. Enforcement of the NAI Code can include penalties for material violations, and potential referral to the Federal Trade Commission (FTC). Annual reviews cover member companies' business models, privacy policies and practices, and consumer-choice mechanisms.

B. Benefits of State Law & Enforcement Harmonization

With five comprehensive state consumer privacy laws expected to become operative in the next 12 months, and many more states considering new laws, we are likely facing an inconsistent set of rules across the United States that will confuse consumers, and a disparate set of obligations that will make compliance overly difficult for businesses. We therefore urge you to seek a collaborative approach in developing implementing regulations, and specifically to work with other states to harmonize requirements to the greatest extent possible. Colorado Attorney General Phil Weiser recently committed to harmonizing his state's regulations with other states,¹ and we hope you will engage in dialogue with Colorado and other state enforcement officials to maximize consistency in the implementation of legal requirements.

This coordinated approach will greatly benefit consumers in California and across the country, in addition to businesses trying in good faith to comply with disparate laws. It will also be to the overall benefit of the California economy, and the U.S. economy more broadly, both of which are increasingly data-driven. A consistent approach across the U.S. could also help the Agency and other state regulators minimize costly legal challenges resulting from conflicting requirements.

C. Summary of NAI Recommendations

- **Opt-out Preference Signals** — The proposed regulations should be amended in accordance with the following three objectives: (1) to reflect the foundational objectives established in the CPRA that an opt-out “[c]learly represent a consumer’s intent and be free of defaults constraining or presupposing that intent,” and to “[e]nsure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business;” (2) to establish an open and transparent review process that provides for stakeholder input to evaluate any mechanisms that propose to serve as Signals in accordance with the CPRA; and (3) to recognize that many businesses do not have the capability to recognize a consumer’s opt-out request if they previously elected to use a preference signal, and that signal is disabled or does not transmit at a later date.
- **Restrictions on the Collection and Use of Personal Information** — The proposed regulations should be amended to clarify that compatible purposes, when provided with notice in compliance with the requirements of CPRA, are subject to the law’s opt-out requirements, rather than creating a new opt-in requirement or a ban on compatible uses based on whether they may or may not meet an average consumer’s expectation.
- **Notice at Collection of Personal Information** — The proposed regulations should be amended to clarify business may comply with the CPRA’s notice requirements by providing the *types/categories* of third parties engaged in data collection, rather than having to list all of the third parties collecting personal information.

¹ See OFF. OF THE CO. ATT’Y GEN., PREPARED REMARKS: ATTORNEY GENERAL PHIL WEISER AT THE INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (April 12, 2022), <https://coag.gov/app/uploads/2022/04/Data-Privacy-Protection-A-Colorado-Perspective.pdf> (stating that through the Colorado Privacy Act (“[W]e want to make Colorado’s requirements harmonious and interoperable with requirements adopted by other jurisdictions.”); See also OFF. OF THE CO. ATT’Y GEN., PRE-RULEMAKING CONSIDERATIONS FOR THE COLORADO PRIVACY ACT (2022), <https://coag.gov/app/uploads/2022/04/Pre-Rulemaking-Considerations-for-the-Colorado-Privacy-Act.pdf>. (“The rules should facilitate interoperability and help situate the CPA alongside the competing protections and obligations created by other state, national, and international frameworks.”)).

- **Requests to Opt Out of Sale/Sharing** — The proposed regulations should be amended to conform with the requirements of the CPRA, clarifying that businesses are not required to transmit opt-out requests to third party partners and require those partners to further pass along an opt-out request.
- **Contract Requirements for Service Providers, Contractors and Third Parties**— The proposed regulations should be amended to provide flexibility in the regulations for the use of standardized industry contracts that identify specific permitted digital advertising activities, data collection and use restrictions, data safeguards, and applicable business purposes when engaging in those activities.
- **Audits and Enforcement** — The proposed regulations should be amended to permit the use of independent, third parties for required audits. Additionally, the NAI proposes the Agency clarify audit scope and implement additional guidelines for the audit process.

II. § 7025: Opt-Out Preference Signals

The NAI has a long history of promoting consumers' ability to exercise choice with respect to how companies use their data for digital advertising. Enabling consumers to express their preferences and exercise control through easy-to-use choice mechanisms is a foundational element of tailored advertising that the NAI has championed for decades.²

To this end, the text of the CPRA provides the opportunity for businesses to honor automated "opt-out preference signals" ("Signals").³ The NAI recognizes the substantial value Signals can provide to both consumers and businesses, particularly in an environment where expressing user preferences can be difficult and confusing for consumers due to the wide range of businesses, operating systems, software, and platforms. In fact, the NAI led industry efforts to provide a platform for consumers to express their preferences with respect to their data use for tailored advertising by creating and operating an centralized opt out page for consumer choice.

However, the industry's broad and consistent recognition of Signals that represent a clearly expressed choice by consumers, and that relate to the choices established by the CPRA, are dependent on effective regulations that implement foundational requirements established by the statute. Unfortunately, the draft regulations are largely inconsistent with the language and the intent of the statute, and they do not adequately facilitate meaningful or active consumer choices to opt-out from the sale and sharing of their personal information. Below, we identify key areas where Sec. 7025 of the proposed regulations need to be amended to ensure that consumers are the ones making decisions about the use of their personal information, and to preserve fair competition across the digital media ecosystem.

A. Opt-Out Preference Signals Must Be User-Enabled

The CPRA requires the Agency to issue regulations that define requirements and technical specifications of the opt-out preference signal that, "clearly represent a consumer's intent and be free of defaults constraining or presupposing that intent."⁴ The statute also explicitly directs the Agency to

² See NAI Code § II.C.1; Network Advertising Initiative, Best Practices for User Choice and Transparency (May 10, 2022), <https://thenai.org/best-practices-for-user-choice-and-transparency/>.

³ See CAL. CIV. CODE §§ 1798.135, 1798.185(a)(19-20).

⁴ CAL. CIV. CODE § 1798.185(19).

develop regulations that, “[e]nsure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business.”⁵

These are foundational principles governing the effective deployment of Signals across the marketplace. Similar requirements were also included in recently enacted consumer privacy laws in Colorado and Connecticut.⁶ Therefore, the stated goals of the Agency to harmonize with other similar state laws would also be served by regulations that adhere to these requirements.

As currently drafted, however, the proposed regulations do not achieve these statutory objectives. Instead, the proposed regulations essentially require businesses to honor *any* opt-out signal, only provided that the Signal “is in the proper HTTP format,” and that the business providing the Signal makes clear to the consumer, either through configuration or public disclosure, that it is “meant to have the effect of opting the consumer out of the sale and sharing of their personal information.”⁷ As a result, the proposed regulations would permit browsers – or any other technology platform providers, such as application or operating system providers – to implement Signals that automatically opt consumers out of the selling or sharing of their data, while only providing mere “public disclosure” and not a direct action by the consumer. Consumers very often rely on software and applications natively bundled with devices and operating systems without specific thought to restrictions placed on their activity across the internet, resulting in a wide range of signals that are likely to arise across the marketplace consumers are unaware they are even generating, let alone represent consumers’ informed choice about their personal information.

While the NAI supports the goal of empowering consumers with easy-to-use choice mechanisms, allowing a limited number of technology intermediaries to make unilateral decisions that presume user preferences creates market imbalances by putting those companies in a position to drive business models across the digital media industry. According to a 2019 NAI survey, 60% of consumers prefer to have online content sponsored by advertising, rather than paying subscription fees for individual websites and apps.⁸ The vast majority of this advertising is data-driven, utilizing various data points to show consumers more relevant and interesting ads, and making marketing decisions that provide greater value to publishers and digital service providers. Therefore, allowing Signals to be “on-by-default” is likely to dramatically curtail the predominant data-driven advertising model that promotes rich digital content today, without representing meaningful consumer choices, and to benefit certain company business models over others.

For example, while Apple’s policies and technology tools are marketed as privacy-friendly, among other marketing approaches, their limits on sharing of consumers’ personal information also promotes their own business model, which relies more on revenue derived from charging consumers and other businesses fees for using their services or operating on their platforms.⁹ This model is in contrast to

⁵ *Id.*

⁶ The Colorado Privacy Act provides that the rules must “not permit the manufacturer of a platform, browser, device, or any other product offering a universal opt-out mechanism to unfairly disadvantage another controller,” and that an opt-out mechanism “must be as consistent as possible” with the mechanisms required by other states. COLO. REV. STAT. § 6-1-1313(2)(a)(e). Similarly, Connecticut’s Privacy Law provides that an opt-out mechanism must “not unfairly disadvantage another controller” and must “be as consistent as possible with any other similar platform, technology or mechanism required by any federal or state law or regulation[.]” CONN. GEN. STAT.

§ 6(e)(A)(ii).

⁷ CAL. CODE REGS. tit. 11, § 7025(b)(proposed).

⁸ NETWORK ADVERTISING INITIATIVE, NAI CONSUMER SURVEY ON PRIVACY AND DIGITAL ADVERTISING, NETWORK ADVERTISING INITIATIVE (Oct. 22, 2019), <https://www.networkadvertising.org/blog-entry/nai-consumer-survey-privacy-and-digital-advertising/>.

⁹ Apple’s service business, which includes revenues from its advertising (and specifically App Store search ads) grew by 24% in the 2021 fiscal year, for a record \$19.5 billion in revenue. Such growth has been possible in part because of

many other digital media businesses that rely more heavily on data-driven advertising and marketing, and it gives Apple a clear market incentive to increase revenues derived from fee-based apps and first-party advertising, rather than third-party ad-supported apps that comprise the majority of apps used by consumers today.

At the same time, Apple has also recently increased their use of first-party advertising, which allows them to bypass the same permission prompts they require of other businesses across their mobile app marketplace, while not necessarily increasing consumer privacy.¹⁰ This is just one example of how the proposed regulations would enable a dominant technology company to usurp true user choices to their own market advantage. If the regulations are not amended to better reflect the protections required by the CPRA, the marketplace is likely to see a proliferation of other technology companies developing and deploying Signals for their own purposes, rather than as a genuine choice tool for consumers. Even if this were a goal of the Agency in developing the regulations, it does not necessarily protect consumers from harms, including privacy harms, that may result from collection of their personal information by a business with which they interact. Instead, it would merely limit that business from selling or sharing. Any first-party company, particularly a dominant technology platform such as Apple, could still collect and use a consumer's data to perform personalized, data-driven advertising across their own broad ecosystem of products and services that compete with smaller competitors who at the same time are precluded from leveraging consumer data to provide tailored advertising.

The NAI always has been, and continues to be, supportive of innovative tools and solutions that implement privacy by design. Companies should be incentivized to create competitive products and services that protect consumer data while maintaining a fair, competitive marketplace. To best achieve both consumer protection and a competitive marketplace, the Agency should not create opportunities for technology intermediaries to impose legal compliance obligations on covered businesses if these do not genuinely reflect consumers' informed decisions about the collection and use of their data.

The NAI appreciates and concurs with the Agency's goal of enabling various platforms and technology providers to develop Signals that genuinely enable consumer choices, rather than seeking to promote a singular technology standard or Signal that would be specific to the state of California and the CPRA. However, this approach is not without challenges to the marketplace. That is, digital businesses operating across different technologies and platforms quite possibly will be challenged by the need to identify and comply with a wide range of different Signals, particularly as they seek to determine which Signals genuinely reflect consumer choices, and which are merely Signals activated by the technology intermediaries. Ultimately, many businesses will challenge and reject Signals that do not reflect consumer choices, therefore unfairly disadvantaging their businesses.

The regulations can help provide clarity and fairness for businesses across the marketplace that will receive these signals—indeed, this is consistent with the direction of the statute. The best way to achieve these goals is for the Agency to establish an open and transparent review process that provides for stakeholder input to evaluate any mechanisms that propose to be recognized as Signals

Apple's App Tracking Transparency privacy changes, which forced advertisers running mobile app ads to recalibrate and shift spending to the App Store—where Apple can directly collect money. See Nina Goetzen, *Apple Ad Revenues Skyrocket Amid Its Privacy Changes*, Insider Intelligence (Jan. 31, 2022), <https://www.emarketer.com/content/apple-ad-revenues-skyrocket-amid-its-privacy-changes/>.

¹⁰ See Samuel Axon, *Apple Ad Exec Wants to More Than Double Ad Revenue with New Ads Across iOS*, ARSTECHNICA (Aug. 15, 2022), <https://arstechnica.com/gadgets/2022/08/report-apple-is-exploring-in-app-ads-for-maps-podcasts-books-and-beyond/>; see also Sara Fischer & Scott Rosenberg, *How Apple Pushed Its Ad-vantage*, AXIOS (Aug. 21, 2022), <https://www.axios.com/2022/08/21/apple-advertising-privacy-tracking-iphone>.

in accordance with the CPRA. This review process should be ongoing, providing the Agency with the opportunity to periodically evaluate and test Signals deployed in the marketplace to ensure that they continue to be administered fairly. To assist in the review process, the Agency should seek input from stakeholders, particularly those businesses to which the Signals are directed.

- **NAI Recommendations:**

The proposed regulations pertaining to opt-out preference signals should be amended to achieve the CPRA's requirements to, "[c]learly represent a consumer's intent and be free of defaults constraining or presupposing that intent," and "[e]nsure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business."

The proposed regulations should also be amended to establish an open and transparent review process that provides for stakeholder input to evaluate any mechanisms that propose to serve as Signals in accordance with the CPRA. The review process should be ongoing, providing the Agency with the opportunity to periodically evaluate and test Signals deployed in the marketplace to ensure that they continue to be administered fairly. To assist in the review process, the Agency should seek input from stakeholders, particularly those businesses to which the Signals are directed.

Amend § 7025 as follows:

(b) A business shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing:

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

(2) The platform, technology, or mechanism, ~~whether in its configuration or in disclosures to the public,~~ that sends the opt-out preference signal shall make clear to the consumer 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 in accordance with the CPRA. The configuration or disclosure does not need to be tailored only to California or to refer to California, but both the configuration and disclosure must be clear to the consumer and receiving businesses that it applies to the specific choices provided by the CPRA and activated by the consumer.

(3) The platform, technology, or mechanism that sends the opt-out preference signal shall require the consumer to activate the signal, in accordance with (b)(2). Consumer activation of a signal can be done through the use of a clear, conspicuous and easy to use mechanism by which the consumer can exercise choice, such as a dropdown menu or main settings menu.

(4) The signal is formally recognized by the Agency as compliant with the requirements established by the CPRA and in § 7025, in accordance with an open review process through which stakeholder review and input is solicited to evaluate the signal(s).

B. Honoring Preference Signals No Longer Present

The proposed regulation provides "[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 sharing of personal information.”¹¹ While we agree that the absence of a Signal should not be interpreted by a business to indicate that a consumer has affirmatively opted-in, the regulations should be clarified to recognize that a business cannot reasonably be expected to have the capability to recognize a consumer’s opt-out if they previously elected to use a preference signal, and that signal is disabled or does not transmit at a later date.

In many instances, businesses cannot reasonably associate an opt-out signal with an individual consumer after switching browsers or devices, etc. Ultimately, if a consumer elects to deploy an opt-out preference signal, and then the signal disappears or is no longer visible to the business, the business should not be expected to maintain an opt-out for that user.

- **NAI Recommendations:**

The proposed regulations should be amended to recognize that many businesses do not have the capability to recognize a consumer’s opt-out request if they previously elected to use a preference signal, and that signal is disabled or does not transmit at a later date.

Amend § 7025 as follows:

(c) When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b):

(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, however the business shall also not be required to process an opt-out for any consumer if the business is not able to associate the previously detected opt-out preference signal with a specific consumer, after such time as any opt-out preference signals becomes absent.

III. § 7002: Restrictions on the Collection and Use of Personal Information

In Sec. 1798.100, the CPRA provides that a business’ collection, use, retention, and sharing of personal information be “*reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.*”¹² The CPRA therefore provides essentially two tests for the collection, use and sharing of consumers’ personal information—whether such uses are “reasonably necessary and proportionate” and whether any additional use or processing is “compatible” with the purposes for which it is collected. Related to these, the CPRA also establishes use and sharing limitations based on the disclosure obligations of the businesses that control this data collection, stating, “[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.”¹³ The emphasis throughout the statute is to provide for businesses to clearly disclose the uses of consumers’ personal information at collection.

¹¹ CAL. CODE REGS. tit. 11, 7025(c)(5) (proposed).

¹² CAL. CIV. CODE § 1798.100(c) (emphasis added).

¹³ CAL. CIV. CODE § 1798.100(a)(1) (emphasis added).

The NAI agrees with the statute's emphasis on clear notice requirements and we agree that businesses should not collect, use, and share personal information for purposes incompatible with these notices—this construct is at the core of the CPRA's mandate for businesses to facilitate consumer choices established by the CCPA. However, Sec. 7002 of the proposed regulations appears to deviate from the law and hinge compatibility more on the expectations of consumers, stating “[a] business’s collection, use, retention, and/or sharing of a consumer’s personal information may also be for other disclosed purpose(s) *if they are compatible with what is reasonably expected by the average consumer.*”¹⁴

As currently drafted, the proposed regulations rely disproportionately on the expectations of the consumer about their use of their personal information, rather than recognizing, as the statute establishes, that businesses are required to provide notice for compatible uses and provide an opt-out. The CPRA makes reference to the “average consumer” standard in multiple instances, but it does not use this test in determining what collection, uses and sharing are, or are not, compatible. As referenced above, the CPRA instead applies the concept of “compatible” to the context of collection, rather than consumer expectations, stating that the business collection can be for, “*another disclosed purpose that is compatible with the context in which the personal information was collected.*”¹⁵

The regulations also require opt-in consent before collecting, using, retaining, and/or sharing the consumer’s personal information for any purpose that is unrelated or incompatible with the purpose(s) for which the personal information is collected or processed.¹⁶ The NAI agrees that not all categories of personal information should be treated equally, and our Code reflects this, by requiring enhanced, explicit notice requirements beyond a privacy policy in situations involving certain categories of personal information, including precise geolocation and sensitive health information, among others.¹⁷ While the proposed regulations are in some ways consistent with the NAI’s long standing—and now widely accepted—industry standard for notice about collection and use of precise location information and other sensitive personal information, they are unclear as to how a business should apply this as established by the CPRA and Sec. 7002 as drafted, particularly with respect to the CPRA’s opt-out requirement for sensitive personal information.

Data-driven advertising and marketing has been used to support the promotion and sale of products and services of all types for decades, even predating online data collection. It therefore should clearly be recognized as compatible with the collection of a consumer’s personal information, as long as the data collection and use is reasonably necessary and proportionate to perform the advertising and marketing, is properly disclosed, and consumers have a right to object to this collection. However, in one of the illustrative examples, an online retailer collecting the personal information of shoppers would seemingly be prohibited from using a consumer’s personal information to market other products to them without consent, even if this practice clearly disclosed at the point of collection.¹⁸ At a minimum, the Agency should also make clear that the hypothetical online retailer would be permitted to market other businesses’ products and services if such use was disclosed in the consumer notices required by the law.

¹⁴ CAL. CODE REGS. tit. 11, 7002(a) (proposed).

¹⁵ CAL. CIV. CODE § 1798.100(c)

¹⁶ CAL. CODE REGS. tit. 11, 7002(a) (proposed).

¹⁷ NAI Code § II.C.1.

¹⁸ CAL. CODE REGS. tit. 11 § 7002(b)(4) (proposed).

- **NAI Recommendations:**

The proposed regulations should be amended to clarify that compatible purposes, when provided with notice in compliance with the requirements of 1798.100, are subject to the law's opt-out requirements, rather than creating a new opt-in requirement or a ban on compatible uses based on whether they may not meet an average consumer's expectation.

Amend Sec. 7002 as follows:

(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, or for another disclosed purpose that is compatible with the context in which the personal information was collected. Whether a business's collection, use, retention, and/or sharing is reasonably necessary and proportionate, or compatible with the context, depends on several factors, including: the expectations of a reasonable consumer when providing their personal information; the nature and sensitivity of the personal information collected; and whether the business disclosed the use, retention, or sharing of personal information at the time it collected the personal information from the consumer. To be reasonably necessary and proportionate, the business's collection, use, retention, and/or sharing must be consistent with what an average consumer would expect when the personal information was collected. A business's collection, use, retention, and/or sharing of a consumer's personal information may also be for other disclosed purpose(s) if they are compatible with what is reasonably expected by the average consumer. A business shall obtain the consumer's explicit consent in accordance with Sec. 7004 before collecting, using, retaining, and/or sharing the consumer's personal information for any purpose that was not disclosed when the personal information was collected or is otherwise unrelated or incompatible with the purpose(s) for which the personal information was collected or processed.

(b)(4) Business D is an online retailer that collects personal information from consumers who buy its products in order to process and fulfill their orders. Business D's provision of the consumer's name, address, and phone number to Business E, a delivery company, is compatible and related to the reasonable expectations of the consumer when this personal information is used for the purpose of shipping the product to the consumer. However, Business E's use of the consumer's personal information for the marketing of other businesses' products would not be necessary and proportionate, nor compatible with the consumer's expectations unless Business E provides appropriate notice to the consumer and provides the opportunity to opt out; such notice and subsequent use would constitute a compatible use. Business E would have to obtain the consumer's explicit consent to do so.

IV. § 7012: Notice at Collection of Personal Information

We appreciate and concur with the regulations' explicit recognition of the third-party collection scenario, which is commonplace across the digital media industry, particularly for small publishers and other businesses that rely on third party businesses to provide tailored advertising services. However, the proposed regulations' requirements for notice at collection of personal information are unclear in instances where a first-party business engages and allows a third party to "control" the personal information of a consumer. We fear that if left as-is, the proposed regulations could be interpreted as a requirement for enhanced notice at collection of consumer data that is both unhelpful for consumers and impractical for businesses.

As currently drafted, the proposed regulations address these scenarios in two areas. First, the draft regulations direct applicable first-party businesses to include in their notices at collection “the names of all the third parties” that the first party allows to collect personal information from the consumer, or “[i]n the alternative, information about the third parties’ business practices.”¹⁹ These alternatives are flexible and practical, providing multiple options to allow for consumers to be effectively informed regarding the collection of their data at the point of such collection, while also providing a pragmatic alternative for the business to achieve this outcome.

However, the proposed regulations create confusion by providing elsewhere that in cases where a first party allows another third-party business to control the collection, there is a choice for either the first party to “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,” or in the alternative, for the third-party business controlling the collection of personal information “to provide the first party information about its business practices for the first party to include in the first party’s notice at collection.”²⁰ This provision could be interpreted to require that the choices available for businesses are for the first-party business to list *all* third parties collecting, or each and every third party to provide their own notice to the consumer, which in many cases is not practical, or even possible.

The outcome of requiring a first party to list all third parties would diverge from current practices under the CCPA and the intent of the CPRA as we understand it, and it would be cumbersome for consumers while providing limited practical value.²¹ That is, it would not be substantially valuable or desirable for consumers to see a list of actual third parties, which they are not likely to know, understand, or distinguish between these companies. At the same time, such a requirement is not practical for businesses, particularly small publishers, who engage with a wide range of third-party partners and would regularly be required to update a list of each specific entity they are working with for each digital advertising partnership. Such a requirement is likely to encourage businesses to employ cookie banners and pop-up consent mechanisms that have been broadly panned by businesses and privacy advocates alike. Not only does the CPRA not embrace such an approach, there is no indication that the Agency sees this as reflecting sound policy.

- **NAI Recommendations:**

The NAI proposes the Agency clarify the alternative presented in the draft regulations (§ 7012 (g)(2)), making clear that the law’s requirements can be satisfied by the first party providing the *types/categories* of third parties engaged in data collection, rather than having to list all of the third parties collecting personal information. Absent a practical interpretation for third party data collection notification, covered businesses, and particularly smaller publishers would face onerous and impractical obligations in reporting the names of all third-party data collectors, ultimately limiting choice for consumers. To accomplish this, we suggest the following amendment to the text of the implementing regulations.

Revise § 7012 as follows:

(g)(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, or information about the types/category of third parties and their business practices. In the

¹⁹ CAL. CODE REGS. tit. 11, § 7012(e)(6) (proposed)

²⁰ CAL. CODE REGS. tit. 11 § 7012(g)(2) (proposed)

²¹ CAL CIV. CODE § 1798.115(a)(d).

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 or if they have the opportunity, may elect to provide notice at collection directly to the consumer.

V. § 7026: Requests to Opt-Out of Sale/Sharing

The CPRA empowers consumers to express choices to businesses individually via a clearly labeled opt-out link directed specifically to those businesses. Additionally the CPRA provides for the opportunity for consumers to utilize Signals, which have the effect of automating opt-out requests, and therefore providing a default for all businesses with which they interact where the consumer does not provide an opt-in. However, these requests to opt out still *only* apply to the business with which the consumer is interacting, at the time, rather than extending to all of that businesses' partners.

As currently drafted, the proposed regulations threaten to extend beyond the statute, potentially also requiring businesses to send a chain of opt-out requests to other parties to which the business partners with and transfers personal information.²² The NAI views it as inconsistent with the spirit and requirements of the CPRA for businesses to be required to notify "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."²³

For example, a publisher that receives an opt-out request from a consumer can reasonably be expected to stop sharing that consumer's personal information with any partners they work with. The proposed regulations also accurately establish a first-party business' obligation to ensure that third parties who control collection of personal information on their digital property recognize and honor an opt-out or Signal. However, the regulations accidentally expand this requirement by mandating that a first-party publisher convey a consumer's opt-out choice to all of their partner businesses, and also requires those businesses to further recognize an opt-out request for that user. This could potentially also be wrongly construed to create a requirement for businesses to send opt-out requests to business that it no longer partners with, which wouldn't even be possible.

The CPRA by design enables a consumer to allow some businesses to share their personal information, while also preventing data processing or sharing by other businesses with which they have a different relationship, or specifically those who they do not trust. The proposed regulations' new flow down requirements directly contravene this.

With respect to consumer deletion requests, the CPRA takes a different approach, clearly requiring businesses to send these requests to contractors, service providers, and third parties.²⁴ The existence of the requirement to forward deletion requests to other parties while the same requirement is absent for opt-out requests further suggests that the CPRA does not intend to impose an opt-out flow down requirement on businesses.

²² CAL. CODE REGS. tit. 11, §§ 7026(f)(2) & (3) (proposed).

²³ CAL. CODE REGS. tit. 11, §§ 7026(f) (proposed).

²⁴ CAL CIV. CODE § 1798.105(c)(1).

- **NAI Recommendations:**

The proposed regulations should be amended to clarify that businesses are not required to transmit opt-out requests to other parties. To accomplish this, we suggest the following amendment to the text of the implementing regulations.

Amend § 7026(f) (proposed) as follows:

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

(1) Ceasing to sell to and/or share with third parties the consumer's personal information as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. Providing personal information to service providers or contractors does not constitute a sale or sharing of personal information.

(2) Ensuring that all third parties whom the business allows to control the collection of consumers' personal information on their digital property, receive the consumer's opt-out request, and require them to honor that request and cease to sell and/or share with other third parties the consumer's personal information as soon as possible, but no later than 15 business days from the date the business receives the request.

~~(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.~~

VI. §§ 7051 & 7053: Contract Requirements for Service Providers, Contractors, and Third Parties

The NAI acknowledges and agrees with the objectives of the CPRA to ensure that Service Providers, Contractors, and third parties should be bound by clear contractual guidelines, including specifying the applicable "business purposes." However, we are concerned that the language in §§7051(a)(2) and 7053(a)(1) is overly prescriptive and could be interpreted in to require that businesses implement and maintain individual, customized contracts with all of their various service providers, contractors, and third party partners, for a set of business purposes that is consistent across a wide range of industry participants. This would be onerous, costly, and impractical for virtually all businesses, particularly small online publishers and advertisers that lack substantial legal and financial resources (and time) to negotiate and manage all of these contracts. This attention to creating and negotiating bespoke contracts, as a practical matter, also may come at the expense of attention to substantive compliance, which does not further the CPRA's goals.

Rather, the NAI encourages the CPPA to provide flexibility in the regulations for the use of standardized industry contracts that identify the specific permitted digital advertising activities, data use restrictions, data safeguards, and applicable business purposes when engaging in those activities. Significantly, this approach would also enable companies, and the CPPA, to more effectively perform due diligence and audits of digital advertising industry participants, rather than having to review and assess hundreds or likely thousands of individualized contracts across the industry. In short, this approach would appropriately balance the sensible goals driving the proposed rule with the practicalities of implementation.

- **NAI Recommendations:**

The proposed regulations should be amended to provide flexibility in the regulations for the use of standardized industry contracts that identify the specific permitted digital advertising activities, data use restrictions, data safeguards, and applicable business purposes when engaging in those activities.

Amend § 7051 as follows:

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

- (1) Prohibit the service provider or contractor from selling or sharing personal information it receives from, or on behalf of, the business.
- (2) Identify the specific business purpose(s) and service(s) for which the service provider or contractor is permitted to 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).~~
- (4) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business for any commercial purpose other than the business purposes specified in the contract, including in the servicing of a different business, unless expressly permitted by the CCPA or these regulations.
- (5) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider or contractor shall be prohibited from combining or updating personal information received from, or on behalf of, the business with personal information that it received from another source, except for as expressly permitted by the CPRA as defined in Civil Code section 1798.140(e), or these regulations, whereby a service provider or contractor may combine personal information to perform limited business purposes.
- (6) Require the service provider or contractor to comply with all applicable sections of the CCPA and these regulations, including providing the same level of privacy protection as required by businesses by, for example, cooperating with the business in responding to and complying with consumers' requests made pursuant to the CCPA, and implementing reasonable security procedures and practices appropriate to the nature of the personal information received from, or on behalf of, the business to

protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.

(7) Grant the business or other party acting on its behalf, the right to take reasonable and appropriate steps to ensure that service provider or contractor uses the personal information that it received from, or on behalf of, the business in a manner consistent with the business's obligations under the CCPA and these regulations. ~~Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular assessments, audits, or other technical and operational testing at least once every 12 months.~~

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

(9) Grant the business or the party acting on its behalf, the right, upon notice, to take reasonable and appropriate steps to stop and remediate the service provider's or contractor's unauthorized use of personal information. ~~For example, the business may require the service provider or contractor to provide documentation that verifies that they no longer retain or use the personal information of consumers that have made a valid request to delete with the business.~~

(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.

(b) A service provider or contractor that subcontracts with another person in providing services to the business for whom it is a service provider or contractor shall have a contract with the subcontractor that complies with the CCPA and these regulations, including subsection (a).

(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) A service provider or contractor shall comply with the terms of the contract required by the CCPA and these regulations.

(e) Whether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that does not conduct due diligence of its service providers and contractors ~~never enforces the terms of the contract nor exercises its rights to audit or test the service provider's or contractor's systems~~ might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.

Revise § 7053 to the following:

(a) A business that sells or shares a consumer's personal information with a third party shall enter into an agreement with the third party that:

(1) Identifies the limited and specified purpose(s) for which the personal information is permitted to be sold or disclosed. ~~The purpose shall not be described in generic terms, such as referencing the entire contract generally.~~ The description shall be specific.

(2) Specifies that the business is disclosing the personal information to the third party only for the limited and specified purposes set forth within the contract and requires the third party to only use it for those limited and specified purposes set forth within the contract and requires the third party to only use it for those limited and specified purposes.

(3) Requires the third party to comply with all applicable sections of the CCPA and these regulations, including providing the same level of privacy protection as required by businesses by, for example, only collecting and using personal information for purposes an average consumer would reasonably expect or other disclosed purposes compatible with the context in which it was collected, complying with a consumer's request to opt-out of sale/sharing forwarded to it by a first party business, providing the required disclosures identified in section 7010, and implementing reasonable security procedures and practices appropriate to the nature of the personal information received from the business to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.

(4) Grants the business the right to take reasonable and appropriate steps to ensure that the third party uses the personal information that it received from, or on behalf of the business, in a manner consistent with the business's obligations under the CCPA and these regulations. For example, the business may require the third party to attest to their compliance with subsection (a)(3).

(5) Grants the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information. For example, the business may require the third party to provide documentation that verifies that they no longer retains or uses the personal information of consumers who have had their request to ~~opt-out of sale/sharing~~ delete their personal information forwarded to them by the first party business.

(6) Requires the third party to notify the business ~~no later than five business days~~ promptly after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.

(b) A business that authorizes a third party to collect personal information from a consumer through its website either on behalf of the business or for the third party's own purposes, shall contractually require the third party to check for and comply with a consumer's opt-out preference signal unless informed by the business that the consumer has consented to the sale or sharing of their personal information.

(c) A third party that does not have a contract that complies with subsection (a) shall not collect, use, process, retain, sell, or share the personal information received from the business.

(d) A third party shall comply with the terms of the contract required by the CCPA and these regulations.

(e) Whether a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that ~~does not conduct due diligence 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.

VII. Audits and Enforcement

While the CPRA grants broad audit authority to the Agency,²⁵ the proposed regulations do little to clarify the scope and process of such audits. Expanding on our CPRA Preliminary Comments²⁶, the NAI recommends reasonable boundaries on CPPA audit capabilities. The following recommendations would ensure predictability and practicality for businesses of all sizes operating in California, while also providing for the most efficient and streamlined use of Agency resources.

A. Use of Independent, Third-Party Auditing

The Agency should implement regulations providing that an announced or unannounced audit, pursuant to Sec. 7304 of the proposed regulations, may be conducted by independent third-party auditors. As stated in our CPRA Preliminary Comments, we again recommend that:

“businesses should retain the ability to either select independent third-party auditors of their choice in accordance with a set of qualifications established by the Agency or to conduct internal audits provided there are policies and other safeguards in place to ensure independence. On the latter point, California law already contemplates the ability of companies to conduct independent yet internal audits in the insurance context.”²⁷

Specifically, we recommend that the agency allow for recognized third party auditors, at the election of the business that the agency seeks to audit, to conduct an audit of the business, or to submit results of a previously conducted audit voluntarily performed by the business. This approach would ensure consistency and predictability across audit types, and correspond with the annual cybersecurity audits required by the CPRA to be performed independently.²⁸ For businesses faced with multiple data audits per year, whether regarding cybersecurity measures or general data privacy, interfacing with the same third-party auditor would provide for familiarity, and thus a quicker and more efficient investigation overall. Furthermore, leveraging third-party independent auditors for any audit would also be less resource-intensive for the CPPA as an agency, freeing up valuable limited

²⁵ See CAL. CIV. CODE § 1798.185(a)(18).

²⁶ See *Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act*, NETWORK ADVERTISING INITIATIVE (2021), <https://thenai.org/preliminary-comments-on-proposed-rulemaking-under-the-california-privacy-rights-act/>

²⁷ *Id.* at 4. (citing CAL. INS. CODE §900.3 (2021))

²⁸ See CAL. CIV. CODE § 1798.185(a)(15)(a) (Providing that Agency regulations shall require cybersecurity audits “on an annual basis” and establish a process “to ensure that audits are thorough and independent.”).

resources for the Agency to ensure compliance broadly, rather than getting bogged down in a lengthy, overly labor-intensive audit process.

B. Limit Audit Selection Criteria

As to the scope of the audits, the NAI recommends the Agency limit the criteria for selection only to *suspected violations of substantive provisions of the CCPA*, rather than a “history of noncompliance” with “any other privacy protection law.”²⁹ The currently proposed language is overly broad, and may encompass privacy laws that do not generally apply to businesses within California, such as the European General Data Protection Regulation (“GDPR”) or other state privacy laws in Virginia, Colorado, Utah, or Connecticut. Limiting the scope to suspected CCPA provisions will provide predictability for businesses, and also will allow the CPPA to enforce its own regulations, utilizing its expertise most effectively.

However, if a history of noncompliance with other privacy protection laws is to remain, the regulations should make clear in Sec. 7304(b) that the scope of this criteria only includes other *California* privacy laws, or federal privacy laws that give enforcement authority to California Attorney General, such as COPPA or HIPAA.³⁰ Without such a distinction, complying with inapplicable laws outside of California, for fear of an audit, may become impracticable for smaller businesses already struggling to compete in the digital marketing ecosystem.

C. Implement Clear, Pre- and Post-Audit Processes

The proposed regulations provide the Agency with fairly wide latitude to conduct audits on its own initiative, “announced or unannounced.”³¹ This potential for unannounced audits, without clear guidelines, may prove overly burdensome for both the Agency and the business being audited. The NAI thus encourages the Agency to add pre and post-audit processes to the proposed regulations, such as clarifying how the selection process might work³² and requiring the opportunity for a “meet and confer” prior to any next steps.³³ A guaranteed “meet and confer” process, following the announcement of a formal investigation, for example, would allow for Agency personnel to further clarify the scope and next steps for the business involved. On the other side, the business personnel would also have an opportunity to resolve any uncertainties the Agency might have about its data collection practices. Altogether, this type of required process would prove conducive to an efficient and collaborative rollout of the new regulations.

When it comes to the language pertaining to the recommended measures above, the NAI again encourages the Agency to look to Federal Trade Commission regulations, and incorporate language requiring “sufficient definiteness and certainty” to any questionnaires or responses requested as part of an audit or investigation; to prescribe a reasonable deadline; and to identify an Agency or

²⁹ CAL. CODE REGS. tit. 11, § 7304(b) (proposed)

³⁰ 15 U.S.C. § 6504; 42 U.S.C. § 1320d-5

³¹ CAL. CODE REGS. tit. 11 § 7304(c) (proposed)

³² On its website, the U.S. Dept. of Health and Human Services made clear its audit pool sampling process for HIPAA compliance review in 2016-17. Interested parties could review the information to locate audit timelines, understand selection criteria, and fill out a pre-screening questionnaire. See U.S. DEPT. OF HEALTH AND HUMAN SERVICES, HIPAA PRIVACY, SECURITY, AND BREACH NOTIFICATION AUDIT PROGRAM (2017), <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html>. Clarity like this would be useful for California businesses concerned about the scope of a potential CPPA Audit.

³³ See 16 CFR 2.7(k) (describing the required “meet and confer” process for Federal Trade Commission investigations). Businesses might already be familiar with this Federal process, and would benefit from consistency with California regulations.

independent custodian “to whom such reports or answers to questions shall be submitted.”³⁴ In addition to the pre and post-audit processes themselves, this recommended language would make sure audits and investigations remain consistent, clear, and limited in scope, further ensuring a predictable process for all parties involved.

- **NAI Recommendations:**

The proposed regulations should be amended to permit the use of independent, third parties for required audits. Additionally, the NAI proposes the Agency clarify audit scope and implement additional guidelines for the audit process.

Revise Sec. 7304 (proposed) to the following:³⁵

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

(b) Performance. Audits may be performed by recognized third party auditors, at the election of the business that the Agency seeks to audit. For the purposes of this section, results from a previous audit voluntarily undertaken by the business also may be acceptable, to the extent that the audit was completed within the prior 12 months.

(bc) Criteria for Selection. The Agency may ~~conduct~~require an audit to investigate possible violations of the CCPA. Alternatively, the Agency may ~~conduct~~require 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.~~that the California Attorney General has the authority to enforce.~~

(ed) Audits may be announced or unannounced as determined by the Agency. The Agency shall publish and maintain on its website a timeline for the audit process. The website shall also provide information about its selection process.

(e) Agency demands for written responses or other material, as part of an audit, shall include sufficient definiteness and certainty as to permit such material to be fairly identified, prescribe a reasonable return date providing a reasonable period of time within which the material so demanded may be assembled and made available for inspection and copying or reproduction, and identify the Agency's custodian to whom such material shall be made available.

(f) Post Audit. The Agency shall meet and confer with business staff prior to any next steps by the Agency, including enforcement and investigation proceedings, to discuss compliance and to address and attempt to resolve any issues or uncertainties that arise from the audit. The meet and confer session may be in person or virtual.

(dg) 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.

³⁴ 16 CFR 2.7(b)(3)

³⁵ Revisions (e) and (f) of the recommendations in this section rely heavily on existing language in 16 CFR 2.7 pertaining to Federal Trade Commission investigations.

(eh) 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 1977, Civil Code section 1798, et seq.

VIII. Conclusion

Again, the NAI appreciates the opportunity to submit comments to the Agency on the proposed regulations for the CPRA. If we can provide any additional information, or otherwise assist your office as it continues to engage in the rulemaking process, please do not hesitate to contact me at [REDACTED], or David LeDuc, Vice President, Public Policy, at [REDACTED].

Respectfully Submitted,

[REDACTED]

Leigh Freund
President and CEO
Network Advertising Initiative (NAI)

From: **Dylan Hoffman** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
CC: **Lia Nitake** [REDACTED]
Subject: CPPA Public Comment - TechNet CPRA Comments
Date: 23.08.2022 15:42:39 (+02:00)
Attachments: FINAL TechNet CPRA Comments.8.23.22.pdf (16 pages)

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

Hi Mr. Soublet,

Please find TechNet's comments in response to the notice of formal rulemaking under the California Privacy Rights Act of 2020. Please let me know if you have any questions about our comments.

Best,

--

Dylan Hoffman
Executive Director | California & the Southwest
TechNet | The Voice of the Innovation Economy
(c) [REDACTED]

Twitter: @TechNetSouthwest



TECHNET
THE VOICE OF THE
INNOVATION ECONOMY



TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

25th
ANNIVERSARY

TechNet Southwest | Telephone 505.402.5738
915 L Street, Suite 1270, Sacramento, CA 95814
www.technet.org | @TechNetUpdate

August 23, 2022

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

Re: TechNet Comments in Response to Notice of Formal Rulemaking Under the California Privacy Rights Act of 2020

Dear Mr. Soublet,

TechNet appreciates the opportunity to provide comments and feedback to the California Privacy Protection Agency as part of the formal California Privacy Rights Act (CPRA) rulemaking process.

TechNet is the national, bipartisan network of innovation economy CEOs and senior executives. Our diverse membership includes dynamic American businesses ranging from revolutionary start-ups to some of the most recognizable companies in the world. TechNet represents over five million employees and countless customers in the fields of information technology, e-commerce, sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

TechNet members know trust is fundamental to their relationships with consumers. Our companies recognize that to be successful they must have responsible practices for the collection, use, and sharing of personal information. TechNet members are committed to providing consumers with strong privacy protections and control over their personal information. TechNet supports consumer privacy laws that provide consumers with important choices and control over their personal information and businesses with clear and consistent guidance to comply with the law.

TechNet members support many of the privacy concepts within CPRA, such as a robust compilation of consumer rights like access, correction, deletion, transparency, and consumer choice, and we believe our suggestions enhance these rights, allow them to be accessed consistently across state lines, and allow for businesses to comply with clear and dependable guidelines for consumer privacy protections.

§7025. Opt-Out Preference Signals

The draft regulations' mandate to honor global opt-outs is contrary to the text of CPRA, exceeds the Agency's rulemaking authority, and the regulations should address the specifications and requirements in the statute for opt-out signals.

We encourage the Agency to use the rulemaking to help develop standards for the still nascent concept of a global opt-out option or signal. At this time there is significant uncertainty for businesses about how to honor such signals. It is critical to develop interoperable principles, standards, and specifications to address the creation, implementation, ubiquity, and limitations of a global opt-out signal.

First, and most critically, the proposed regulations interpret the preference signals to be mandatory, despite clear statutory text that businesses have an option to either comply with the requirements for a Do Not Sell or Share link pursuant to Section 1798.135(a) *or* allow consumers to opt-out through an opt-out preference signal. See, Section 1798.135(b). The Agency does not have the authority to override the statute.

Moreover, the Agency achieves its interpretation that opt-out preference signals are mandatory through a strained interpretation of the CPRA that is further designed to obviate the clear statutory intent to create an option. To arrive at its interpretation that honoring the signals is mandatory, the Agency proposes an interpretation of the CPRA that would make the placement of the Do Not Sell or Share Links on a website optional if a business honors an opt-out signal in a "frictionless manner." Not only does this contradict the statute, but it is largely unachievable. For example, the draft regulations state that a business can only process the signal in a frictionless manner if it allows the preference signal to fully effectuate the consumer's request without requesting more information from the consumer. However, proposed section 7025(c)(2) plainly states that a business cannot require a consumer to provide this information. As a result, browser-based opt-out signals can't be honored in a frictionless manner because a business will not be able to connect that signal to a known consumer without additional information. The certainty of that outcome nullifies the interpretation of the "option" by the agency, which the statute expressly offers. This exceeds the agency's authority.

Secondly, the proposed regulations do not address the requirements and specifications set forth by the CPRA. The proposed regulations are silent on the requirements and fail to define any technical specifications that the statute directs the agency to ensure are met with respect to any opt-out signal. See, Section 1798.185(a)(19)(A)(i)-(vi). The limited information in the proposed regulations – stating only that the signal must be in a commonly used format such as an HTTP header – does not give businesses useful guidance concerning which signals they should look for, much less the technical means businesses should use to honor such signals. Rather than expanding on how an opt-out preference signal can meet these

statutory criteria, the proposed regulations issue a mandate for any such signal that meets two criteria created by the Agency rather than the statute. Neither of the two Agency-created criteria meet any of the statutory specifications for opt-out preference signals. Indeed, the second criterion created by the Agency directly contradicts the statutory standards in a number of ways. See, Proposed Section 7025(b). As just one example, it would wrongly allow a signal even if it fails to “clearly represent a consumer’s intent” by permitting the opt-out without any disclosures about the parameters of the opt-out right in California (including any limitations to this). This contravenes Section 1798.185(a)(19)(A)(ii) and (iii). As a result, if finalized as proposed, the regulations would allow signals that are non-compliant with the statutory standards. Moreover, by bypassing this, the regulations are creating two rules for consent: one for opt-out signals and one required by businesses. Not only does this not make sense, but it risks consumer confusion.

We strongly encourage the agency to ensure that the regulations address how opt-out signals can comply with the statutory requirements, as contemplated in the CPRA’s grant of rulemaking authority. The Agency should draft the regulations to ensure a consistent approach to both transparency and informed consumer choice in the implementation of all CPRA requirements, including opt-out preference signals.

Lastly, the proposed regulations should permit businesses to honor consumers’ business-specific privacy choices that conflict with an opt-out preference signal. Proposed sections 7025(c)(3)-(4) address conflicts between a consumer’s business-specific privacy settings and opt-out signals with a regulatory presumption that consumers 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 consumer’s stated preferences. The requirement at (c)(3) creates an unnecessarily burdensome requirement for businesses in their direct interactions with consumers when a preference signal creates a general conflict. It would require businesses to build new mechanisms to detect conflicts, honor the signal when a conflict is present, and then permit a business to seek consent to reenact choices that consumers have already made. This forces the business to clear up the confusion created by the opt-out mechanism, which is made even more unreasonable in the context of the Agency’s failure to issue any of the “requirements and technical specifications for an opt out preference signal” required by Section 1798.185(a)(19) of the statute. Further, the proposed requirement for (c)(3) is unclear as to what businesses must do upon receipt of a signal when they cannot identify a consumer. In that instance, the business cannot determine if there is a conflict. The regulations should expressly note that in such circumstances a business need not assess if there is a conflict. Otherwise, the regulations would force businesses to collect more data to identify the consumer but prohibit the business from requiring the consumer to provide the data. This requirement is

antithetical to privacy protections by encouraging the excessive collection of personal data and prevents businesses from complying with the regulations.

The requirement at (c)(4) is even more problematic with respect to disclosures for financial incentive programs by mandating that businesses build a consent structure to ensure consumers can remain in a program that they have already elected to participate in. These provisions create costly compliance obligations for businesses and usurp consumer choice.

Finally, the risk of consumer confusion is exacerbated by the Agency's choice, at least in this initial proposal, to override the statutory specifications for the opt-out signal that require meaningful disclosures to consumers about the effect of the opt-out. Without the statutory requirement, consumers are unlikely to understand, based on the current criteria, that an opt-out mechanism will override their choices with businesses they directly interact with and result in the degradation of their consumer experience. The regulations should not attempt to override the will of the voters and instead keep consumers in control of their choices.

§ 7002. Restrictions on Collection and Use of Personal Information

The proposed regulations should align with other existing standards and the plain statutory text of CPRA to provide businesses with the reasonable ability to use data for compatible purposes as disclosed to consumers. CPRA Section 1798.100 clearly allows the collection of information that is compatible with purposes disclosed to the consumer and requires notice for any incompatible purposes. This standard, which is interoperable with the standards enacted in Virginia, Colorado, and Connecticut, sensibly ties a consumer's expectations to what is disclosed to them.

Proposed section 7002 of the draft regulations states that a business's collection of personal information must be "reasonably necessary and proportionate", which is defined to mean "what an average consumer would expect when the personal information was collected." This "average consumer" standard is nowhere in the text of CPRA and conflicts with the plain meaning of "reasonably necessary and proportionate to achieve the purposes for which the personal information is collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected" This creates significant ambiguity since a business, consumer, and regulator may differ on what an average consumer expects, and it transforms the CPRA's transparency requirements into a nullity – even if a business is transparent, that simply isn't enough.

We encourage the Agency to remove the consumer expectations standard because it is subjective and almost impossible to apply to the complex technical processing that powers the internet, mobile apps, and connected devices. It also threatens to

prohibit even otherwise legally permissible processing, such as creating new services or improving existing services.

The regulations also require that if the collection, use, or retention of personal information is not consistent with what the average consumer would expect when the personal information was collected, then opt-in consent is needed. This contradicts the statute and flips the current requirements in California Consumer Privacy Act (CCPA) on their head as the CCPA and CPRA have always been opt-out regimes, except in limited circumstances not applicable here. This contravenes the plain statutory text and the Agency does not have the authority to rewrite the statute through the rulemaking process.

The illustrative examples in proposed section 7002(b) are also exceedingly narrow and threaten to suffocate innovation. For instance, the regulations assume that the primary function of a service should be the exclusive function. An example in proposed section 7002 states that a cloud storage services business may not “use personal information to research and develop unrelated or unexpected new products or services, such as a facial recognition service, without the consumer’s explicit consent” because such a use is not reasonably necessary, proportionate, or compatible with the purpose of providing cloud storage services. Applying this example to other use cases, it is concerning how this could affect machine learning models, including training those models with data collected for the improvement of services. Taking a step back, the larger concern is that a reasonable company may not be able to collect personal information, even if they provide proper notice at the time of collection and in their privacy policy, if the Agency determines that the collection or use is not reasonably necessary and proportionate and in line with consumer expectations.

Injecting the “average consumer” standard, instead of the plain language of CPRA, leads to value judgments that will disfavor innovation and lead to inconsistent enforcement. We suggest striking the “average consumer” standard as used in proposed section 7002(a). The Agency should instead revise the regulations to state that any collection should be reasonably necessary and proportionate and not materially inconsistent with the disclosed purposes of the collection.

§§ 7050. Service Providers and Contractors, 7051. Contract Requirements for Service Providers and Contractors, 7053. Contract Requirements for Third Parties

The regulations should allow businesses to define their relationships with service providers and third parties through appropriate contractual safeguards.

First, the Agency lacks the authority to determine categorically that the provider of cross-contextual behavioral advertising must be a third party (§ 7050(c)). The

terms of a contract negotiated between a business and its service provider should define this relationship. Given the contractual safeguards for the protection of personal information in place with services providers and consumers' ability to opt out of cross-contextual behavioral advertising, there are sufficient protections for consumers.

Second, the example noted in proposed section 7050(c)(1) of the draft regulations purports to prohibit a form of advertising based on email addresses. This example is inconsistent with the text of CPRA, including Section 1798.140(e)(6), (j)(1)(A)(iv), and (ag)(1)(D), and thus exceeds the Agency's authority. The Agency cannot substitute its advertising policy preferences for the clear meaning of the statute. The Agency should remove this example and make clear that service providers should be able to provide any advertising services that comply with the text of the CPRA, as the advertising described in this example would. In other words, a service provider to a business should be able to serve advertisements to the business's own customers, even if the service provider is using information not provided by the business that enables the service provider to deliver that advertisement to the business's customers.

The Agency's proposed regulations on this also fail to take into account the difference between first party and third-party data and the particular nuances of the advertising ecosystem. This myopic view leads to these narrow and confusing examples. Furthermore, the Agency cannot substitute its advertising policy preferences for the clear meaning of the statute. The Agency should remove this example because it contradicts the statute and raises new questions and uncertainty for businesses beyond those called out in the example.

Regarding proposed sections 7051 and 7053 of the draft regulations, we caution the Agency against creating a de facto requirement that businesses audit the data practices of their service providers and contractors regularly. See, section 7051(a)(6),(e). Proposed sections 7051(e) and 7053(e) create a de facto requirement that a business must conduct due diligence and audits on its service providers, contractors, and third parties. The proposed regulations require businesses to include extremely prescriptive provisions for all agreements with service providers and third parties. Failure to address all of these provisions (ten requirements in service provider agreements and six in contracts with third parties) would subject the business to substantial penalties, even for trivial missteps. The statute already addresses core requirements for service provider agreements (see Section 1798.140(ag)) and does not instruct the Agency to issue regulations concerning third-party agreements. Proposed sections 7051 and 7053 of the draft regulations create an onerous compliance regime for businesses with little to no corresponding protection for consumers. To the extent the Agency promulgates regulations on when the exemption in §1798.145(i) applies, they should be limited to factors that affirmatively indicate that the external party is violating its

obligations—and not impose additional burdens on a business to confirm the absence of violations.

While a requirement for vendor due diligence makes sense, the suggestion that reasonable privacy vendor due diligence *mandates* ongoing manual reviews, automated scans, technical testing, and audits once every twelve months is unduly burdensome. First, the regulation does not take into account the risk associated with the service provider. Nor would this one-size-fits-all requirement make sense in practice. Rather, the regulations should clearly state that a business has an obligation to examine the vendor's practices if it has reason to believe there is a violation. Even the suggestion of what reasonable due diligence requires (i.e., stating in the regulations that audits, manual reviews, etc. "may" be required) will turn those suggestions into the de facto standard and increase the burden on businesses considerably.

Audits are resource-intensive exercises that are not warranted for most providers on a regular basis, absent indications that personal information is not managed appropriately. Third-party audits are burdensome and expensive, making a mandate inappropriate as the burden and expense would be disproportionate to any downstream consumer benefit, and the result would likely be increased consumer costs. Instead, businesses should be incentivized to take reasonable measures to oversee service providers' compliance with contractual requirements.

Similarly, a business's reasonable measures to oversee compliance by a third party with contractual requirements should be sufficient to protect it from liability for that third party's mismanagement (§7053(e)). If a business has a contract with a third party that separately controls collection of consumer personal information, it should not be required to identify this party upon collection. This requirement would be burdensome and cause consumer confusion, and it is only necessary if the business will use data for different purposes (§ 7012(e)(6),(g)).

Additionally, section 7051(a)(2) adds unnecessary and impractical compliance obligations that go beyond the language of the statute, fails to consider how businesses execute contracts, and provides no additional protections to consumers. This provision prohibits businesses from cross-referencing another contract generally to define the specific business purposes for which the business is disclosing personal information. This requirement misunderstands that master agreements to which data protection addenda apply permit parties to purchase various types of services over many years and ensure that appropriate privacy protections apply to all such services. This type of contracting would be upended by this provision by requiring businesses to redraft and renegotiate millions of master agreements and data protection addenda. Regardless of how the contracts are drafted, consumers are sufficiently protected.

Finally, proposed section 7051(a)(8) imposes a very short period (five business days) in which a service provider or contractor must notify a business that it can no longer meet its obligations. We suggest extending this timeline to ten business days.

§§ 7014. Notice of Right to Limit and the “Limit the Use of My Sensitive Personal Information” Link, 7027. Requests to Limit Use and Disclosure of Sensitive Personal Information

Many companies use information to improve the quality of service for all customers. The proposed regulations should align with the CPRA’s express allowance for businesses to use sensitive personal information for operational and beneficial purposes.

In order to more closely align with other jurisdictions such as Colorado, Connecticut, and Virginia, we propose clarifying proposed sections 7014 and 7027 such that businesses are not required to provide a “notice of right to limit” or honor “requests to limit” if the business obtains opt-in consent prior to processing sensitive personal information and provides consumers with a mechanism of withdrawing such consent. A business should not be required to offer this opt-out if it only collects sensitive information with opt-in consent. This approach allows business to comply with rules in other jurisdictions and also is consistent with the aims of the CPRA, which is to provide consumers with choice and control over their data.

We are encouraged that the proposed regulations would allow a business to present the consumer with choices for specific use cases. We would caution the Agency, however, against implementing a standard that the single option must be presented more prominently than other choices. This would serve only to subvert consumer choice and unnecessarily impede the sharing of truthful and accurate information with consumers. It also contradicts the CPPA’s proposed standards for consumer choice architecture set forth in proposed section 7004. In this instance the Agency would be directing unreasonable asymmetry in choice architecture. The presentation of specific use cases or options for consumers should align with the same general choice architecture requirements otherwise proposed by the rules. See, Section 7027(h).

In addition, the proposed rules contemplate that an authorized agent can submit a request to limit the use of sensitive information when given written permission from the consumer, but only permit a business to deny such a request if the agent does not provide the business with the signed permission document. Businesses should also be able to deny such requests if there is a reasonable suspicion that it is a fraudulent request, or the written document was obtained fraudulently. See, Section 7027(i).

Furthermore, proposed section 7027(l)(3) only allows a business to use or disclose sensitive personal information without posting a right to limit the use or disclosure of sensitive personal information when the information is being used to “resist malicious, deceptive, fraudulent, or illegal actions *directed at the business.*” (emphasis added). This should not be limited only to such actions “directed at the business” but should include all efforts to “resist malicious, deceptive, fraudulent, or illegal actions”. Geolocation information, for instance, can be highly indicative of potential fraud.

§§ 7022. Requests to Delete, 7023. Requests to Correct

The CPRA sets out procedures for fulfilling requests for deletion and access, including appropriate authentication measures to help prevent fraud (Cal. Civ. Code § 1798.130). In setting out procedures and limitations on correction, the CPPA should adopt similar procedures to help provide both individuals and businesses with clarity through uniformity.

The right to delete and right to correct can be important tools for consumers to control their information and when necessary to correct inaccurate information that may be preventing them from accessing housing, job or educational opportunities. But outside of those defined areas it could impose a significant burden on businesses. New compliance obligations for consumers’ rights to delete or correct their personal information should be justified with clear benefits to consumers.

We agree that a business should be required “to make reasonable efforts to notify service providers and third parties” of a consumer’s request to delete personal information. However, more onerous requirements for businesses are not commensurate to consumer benefit. Businesses should not be required to provide a consumer with detailed explanations as to why it cannot notify all third parties (§ 7022(b), (c)), why it cannot delete all personal information (particularly when a legal exception applies) (§ 7022(f)(1)), why it cannot provide personal information beyond a 12-month period (§ 7024(h)), and when denying correction requests (§ 7023(f)).

Requirements like these impose unnecessary burdens on the business to act as a middleperson between the consumer and any external party that receives the consumer’s personal information. While it may be appropriate for a business to pass on a deletion request in certain instances (§ 7022(b)(3)), the business should not have the additional burden of relaying detailed explanations from service providers and contractors to the consumer about the status of the deletion request (§ 7022(c)(4)), which also brings little corresponding benefit to the consumer. This is simply impossible at scale. Thus, we suggest striking the requirement that a

business needs to provide a detailed explanation from the service provider or contractor to a consumer.

The draft regulations should also extend the disproportionate effort analysis to a business's obligation to delete. Currently, the draft regulations contemplate a disproportionate effort analysis only for businesses that are responding to a request to correct (§ 7023(f)(2)) or request to know (see § 7024(h)), or where a business is required to notify all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information (§ 7022(b)(3)). Further, a business's obligation to delete should not extend to personal information contained in unstructured data where compliance with such deletion would involve a disproportionate effort, such personal information is not sold or used for any commercial purpose, and retention of the personal information in the unstructured data would not impact the consumer in any material manner.

Regarding a consumer's right to correct, the draft regulations require the business to notify other service providers and contractors that have previously received the data that the data have been corrected. This is a significant operational burden that is not specifically required in the statute itself and can create challenges especially if the data were transferred a long time prior to the correction request. Also, just because a service provider or contractor has received the data, the fact that the data were subsequently corrected is not necessarily relevant. This requirement should be removed. To the extent the Agency maintains this requirement, the disproportionate effort standard from 7022(c)(4) should be included.

Additionally, proposed section 7023(h) also requires a business to provide an explanation as to why it believes a request to correct is fraudulent or abusive. Businesses should not be required to explain to fraudsters or bad actors seeking to abuse our sites how to evade our fraud and abuse detection mechanisms. This requirement should be stricken. Similarly, a business should not be required to provide the consumer with the name of the source of inaccurate information (§ 7023(i)).

Lastly, proposed section 7023(j) should also be stricken because it is duplicative of existing access and transparency requests. Permitting consumers to submit an additional access request to confirm that a business has properly processed a correction request puts an onus on businesses to process repetitive requests in a manner inconsistent with the statute.

§ 7012. Notice at Collection of Personal Information

Proposed section 7012(d) requires that if a third party controls collection on behalf of a first party, then both the third party and the first party have to give notice at

collection. Dual notices are duplicative and will be confusing to consumers. A single notice by the first party that discloses categories of parties where data may be shared is both sufficient and meaningful to consumers. The consumer will not be served by receiving multiple notices if this creates an additional operational burden where there is not a direct relationship with the consumer. This subsection likewise requires that the first party notice shall include the names of all the third parties that may be collecting on behalf of the first party. This should be categorical only (i.e., describing the business practices or processing purposes carried out by third parties) instead of having to name multiple parties to avoid having to disclose confidential information. This would also avoid periodic updates to privacy notices each time a first party substitutes a third party, which would be confusing and overwhelm consumers.

Additionally, proposed section 7012(f) requires that if a business collects information from a consumer online, the notice at collection must take the consumer *directly* to the *specific section* of the business's privacy policy that contains the CCPA and CPRA required provisions regarding: categories of information collected, purposes of use, retention, etc. This requirement is unrealistic in practice and unmanageable at scale, especially for global businesses that have users around the world. A business would have to collect more information in order to *identify* all California users and link to its CPRA privacy notice for those users, and then ensure that all other users are directed to their regular privacy policy. Alternatively, the business could combine its California privacy notices into its main policy, and then for *every* point of collection of personal information send the user to the specific section that covers their jurisdiction based on the location of the visitor. This requires businesses to continuously collect or infer the geolocation of all visitors to their website. Either solution is unmanageable at scale. Additionally, sending individuals to a specific section in the privacy policy deprives users of the full context of the policy, which may help them understand a business's data handling practices and certain global definitions, thus further confusing users. This requirement has *no corollary* in any other jurisdiction, likely for the reasons stated above.

Finally, for third-party businesses that control the collection of data on another business's premises, proposed section § 7012(g)(3) should permit that third-party business to provide notice in a "reasonable" manner that takes into account the method of the data collection. For instance, if a store or restaurant employs a third-party voice assistant device that does not contain a physical display, then a notice directing the consumer to the third-party device's website should be sufficient.

§ 7004. Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent

We agree with the intent of proposed section 7004, which is to ensure that consumers are presented with methods to submit their rights requests and to give consent to data practices that are free from unlawful dark patterns and attempts to manipulate those choices. However, the proposed symmetry choice standard for a dark pattern is overly broad and likely unworkable because it mandates an overly rigid approach. Every user interface requires a designer to consider an infinite range of choices that will impact user behavior. Instead, the regulations should define “dark patterns” to focus on design practices that amount to consumer deception. This approach would target those design practices that deceive consumers into taking a desired action, such as by misleading customers about the consequences of providing or refusing consent.

For example, the proposed symmetry choice standard for a dark pattern is overly rigid by requiring essentially “perfect” symmetry and is therefore likely unworkable. Illustrative Example A, for instance, proposes that the processing for submitting an opt-out request cannot be more steps than a request to opt-in. While we agree with the aim of this example in principle, there could be instances where an additional step is necessary to provide a consumer with the full information about the impact of an opt-out. Provided that the extra step is reasonable, it should not fail the symmetry standard set forth in the regulations. The Agency can account for this by revising the proposed regulation to prohibit *unnecessary* extra steps.

If the CPPA insists on the symmetry in choice standard, it should modify the draft rules to focus on reducing practices that harm consumers rather than prescribing specific design practices. Alternatively, using a reasonableness or principles-based standard would help avoid overbroad applications or outcomes that dilute the intentions of the CPRA to give consumers meaningful choices.

§ 7013. Notice of Right to Opt-Out of Sale/Sharing and the “Do Not Sell or Share My Personal Information” Link

Generally, we suggest refining the regulations to strike a proper balance between appropriate disclosures and information overload.

The regulations require that a business shall provide the notice to opt out of the sale or sharing of data in the same manner in which it collects the personal information for that purpose (§ 7013(e)), yet this goes beyond the statutory requirements. With respect to businesses that have an online presence, the statute requires only that the business disclose the consumers’ right in its online privacy policy or on its internet website. § 1798.130(a)(5). Extending the notice obligations

will impose significant burdens on businesses that maintain a website but collect personal information by other means.

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

Additionally, § 7013(h) should be clarified to require affirmative consent to sell or share data collected prior to the opt-out notice, while limiting it to data collected *after* the notice requirement goes into effect.

§§ 7302. Probable Cause Proceedings, 7303. Stipulated Orders, 7304. Agency Audits

The regulations should incorporate more flexibility into the Agency’s enforcement process and place limitations on its audit authority. The Agency should incorporate a range of enforcement mechanisms into the regulations, consistent with Cal. Civ. Code § 1799.199.45, as other California enforcement bodies have done.

First, the Fair Political Practices Commission (FPPC) 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 for a reply, after which a probable cause hearing officer determines if there is probable cause to proceed. We suggest formalizing the CPRA audit process in proposed section 7302 by modeling it after the FPPC’s process and requiring the Agency to serve a respondent a written probable cause report summarizing the evidence supporting a finding of probable cause for each alleged violation of the act and providing 30 days for a respondent to submit a written response before a probable cause proceeding can take place.

Similarly, the Agency can model a progressive enforcement system on the California Public Utilities Commission (CPUC). The CPUC implements progressive enforcement, characterized as “an 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). The auditor issues a draft audit report with findings, which provides an opportunity for a business to respond, followed by a final audit report with findings. 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.” (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 (8-9). There is the possibility to propose a negotiated settlement, to adopt an Administrative Consent Order, to follow a Citation and Compliance Program (10-12). There is the possibility of an Order to Show Cause why a CPUC action should not be taken (14). The flexibility of a progressive enforcement system would be beneficial for businesses and the Agency in order to provide an opportunity resolve differences of interpretation without the need for additional enforcement actions.

Finally, although the CPRA authorizes the Agency to conduct compliance audits, the regulations must place some parameters on this power. An audit is a resource-intensive exercise for both the Agency and the business. Without clear limitations and parameters, the Agency could conduct broad investigations through audits, leading to mounting pressure to find some basis for an enforcement action. We suggest amending proposed section 7303 to provide businesses with written notice at least 30 days in advance of any audit, including the date of the audit, the matters or areas the Agency intends to audit, and the Agency’s basis for auditing the identified matters or areas. We also suggest including a requirement to complete the audit within 180 days from the audit’s start date unless otherwise agreed to by the parties. In addition, the rules should clarify that auditing a business permits access to information but does not automatically grant access to a business’s physical premises. Consistent with our suggestion above, to the extent the Agency plans to submit an audit report, the regulations should require the Agency to provide the audited business with a draft audit report with findings, and provide the business with an opportunity to respond prior to the issuance of a final report.

§ 7026. Requests to Opt-Out of Sale/Sharing

Proposed section 7026(f)(4) creates a new requirement that businesses provide a means by which a customer can confirm that the business has processed their opt-out request. This exceeds the statutory requirements and will increase compliance costs for businesses and cause confusion for consumers. If required to display preference, the business should have the option to show preference within privacy settings. The business should not be required to display the preference directly on the website as that could clutter the consumer’s user experience on certain sites, platforms, or applications.

§ 7015. Alternative Opt-Out Link

Under the current CCPA regulations, section 7013(f), the opt-out icon “may be used in addition to posting the notice of right to opt-out, but not in lieu of any requirement to post the notice of right to opt-out or a ‘Do Not Sell My Personal Information’ link”. Under the draft regulations, section 7013(f) has been removed, and the opt-out icon is now moved to proposed section 7015(b) with the requirement to use the icon if the business chooses an alternative opt-out link. The business is required to title the link, “Your Privacy Choices” or “Your California Privacy Choices”. We suggest maintaining the permissive standard from CCPA regulations section 7013(f).

Reasonable Implementation and Enforcement Period

Final CCPA regulations were completed in March 2021 and our member companies have taken action to comply with those rules. However, this proposed rulemaking, which has been delayed, contemplates significant new compliance measures for companies. The current proposed regulations do not even address all of the Agency’s statutorily mandated topics for rulemaking. Notably absent, for example, is any meaningful guidance regarding the requirements and technical specifications for opt-out preference signals. See, section 1798.185(a)(19). Considering the Agency has failed to meet its statutorily required deadline of July 1, 2022 for final regulations it should provide in the proposed regulations, or, at a minimum, voluntarily agree to not undertake enforcement actions with respect to any violations that occur within a 12-month period from the date of the final regulations (as contemplated by Section 1798.185(d)).

Under Section 1798.85(d), the CPRA regulations were to be finalized by July 1, 2022. While we understand the difficulties the Agency has faced to both start and complete the rulemaking in that timeframe, the result of the delay is a difficult compliance landscape. The burden, costs, and the time necessary to achieve this is compounded by the proposed rules contemplating standards that exceed the underlying statutory text. To ensure that companies have sufficient time to comply, the Agency should ensure a reasonable period between implementation and enforcement as the CPRA intended in Section 1798.185(d).

Conclusion

We appreciate your consideration of these critically important issues. As privacy laws proliferate throughout the United States, it is even more crucial to enhance the clarity and interoperability of laws and regulations that will allow companies to comply with the requirements set out by various locales. We believe the comments outlined above balance industry operability not only with the CPRA, but with

existing omnibus privacy legislation throughout the world. If you need any further information or have any questions about our comments, please contact Dylan Hoffman at [REDACTED].

Sincerely,

[REDACTED]

Dylan Hoffman
Executive Director, California and the Southwest
TechNet

From: **Keir Lamont** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 18:43:58 (+02:00)
Attachments: [FPF] CPPA Public Comment.pdf (10 pages)

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

Please find attached the CPPA Public Comment of the Future of Privacy Forum.

Cheers,

--



Keir Lamont
Senior Counsel
Future of Privacy Forum
[REDACTED] | www.fpf.org |
1400 Eye Street NW, Suite 450, Washington, DC 20005



August 23, 2022

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

RE: Future of Privacy Forum CPPA Public Comment

Dear Mr. Soublet and Members of the California Privacy Protection Agency:

The Future of Privacy Forum (“FPF”) welcomes the opportunity to comment on the proposed regulations to implement the California Privacy Rights Act of 2020 (“CPRA”) amendments to the California Consumer Privacy Act of 2018 (“CCPA”).¹ FPF is a non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies in the United States and globally.² FPF seeks to support balanced, informed public policy and equip policymakers with the resources and tools needed to craft effective regulation.

While FPF has a broad remit and expansive expertise across the field of consumer privacy, our comments here are focused on § 7025 of the draft regulations regarding opt-out preference signals (“signals”) and are informed by an FPF review of mechanisms to convey ‘Global Privacy Control’ (“GPC”) signals currently in the marketplace.³ As the Agency’s rulemaking process advances, we look forward to commenting on other important consumer privacy rights and business obligations established under the CPRA, including the definition and scope of “sensitive personal information.”

The development and deployment of technological signals that communicate an individual’s privacy choices to businesses can enable people to exercise their rights on an automated basis, significantly easing the burdens of privacy self management. The draft regulations resolve many ambiguities about the implementation, exercise, and impact of signals pursuant to the CCPA and reflect a nuanced understanding of both the opportunities and inherent limitations of such tools as they currently exist.

¹ California Privacy Protection Agency, “Text of Proposed Regulations”

https://cppa.ca.gov/regulations/pdf/20220708_text_proposed_regs.pdf.

² FPF’s comments do not necessarily reflect the views of FPF’s supporters or Advisory Board.

³ The Global Privacy Control has 7 “Founding Organizations” (two browsers: Brave, Firefox and five browser plug-ins: Abine, Disconnect, DuckDuckGo, OptMeowt, Privacy Badger) that transmit the signal, each with different user interfaces and different disclosures. <https://globalprivacycontrol.org/>. Additional, non-affiliated mechanisms can also transmit the signal, including the plug-ins Crumbs, Startpage Privacy Protection, and GPC Enabler.

As the California Privacy Protection Agency (“the Agency”) proceeds in rulemaking under the statutory interpretation that the recognition of qualifying signals by covered entities is required by the CPRA amendments, addressing the following outstanding matters will help to ensure that Californians can reliably and easily exercise their CCPA rights through this emerging class of privacy controls.

A. Adopt rules for opt-out preference signals that provide clarity for websites while encouraging innovation in privacy controls for emerging digital and physical contexts.

In the fragmented consumer data ecosystem of web, mobile, smart TVs, Internet of Things, connected vehicles, immersive tech, and other emerging technologies, it is unlikely that a single, ‘universal’ signal specification will be developed that can effectively apply across all the digital (and physical) contexts in which individuals interact with businesses. For example, while specifications that transmit consumer privacy preferences through a web browser or browser plug-in, such as the GPC, are well-suited for conveying preferences to websites, additional signal specifications and mechanisms will be required to effectively invoke CCPA rights with other platforms and technologies, such as mobile applications and the range of consumer data platforms listed above.

FPF recommends that the Agency ensure that the final regulations and statement of reasons are sufficiently technology neutral to allow for and encourage the development of preference signals for non-website contexts. For example, draft regulation § 7025(a) provides that the purpose of preference signals is to enable the exercise of CCPA rights by “consumers interacting with businesses online.” However, the CCPA’s rulemaking grant does not specify that qualifying signals may only be developed or exercised in “online” contexts (see Civ. Code § 1798.185(a)(19),(20)). Final regulations should ensure that qualifying signals will not necessarily be applicable only to websites, but may be developed for mobile apps, connected products, and potentially govern data collected offline (such as from ‘digital out of home’ billboards).

Non-website privacy opt-out signals may seem far away, but in fact many are already in use or development. For example, the iOS and Android mobile operating systems have historically both provided the “Limit Ad Tracking” feature, involving a decentralized signal that communicates an individual’s privacy preferences to mobile apps.⁴ Similarly, researchers at Carnegie Mellon have developed a mobile privacy management tool designed to convey privacy signals to IoT devices.⁵

⁴ See Bennett Cyphers, “How to Disable A ID Tracking on iOS and Android, and Why You Should Do It Now,” Electronic Frontier Foundation (May 11, 2022), <https://www.eff.org/deeplinks/2022/05/how-disable-ad-id-tracking-ios-and-android-and-why-you-should-do-it-now>.

⁵ Daniel Tkacik, “New infrastructure will enhance privacy in today’s Internet of Things” CyLab (Feb. 19, 2020), <https://cylab.cmu.edu/news/2020/02/19-privacy-assistant.html>.

As user activity and data collection increasingly shifts to mobile and other non-website interactions,⁶ innovations in privacy self-management tools will also continue.

Given the complexity and importance of establishing new specifications and processes governing data collection and sharing by traditional websites, it may be practical for the Agency's first set of regulations to address signal requirements as they apply to websites, browsers, and browser plug-ins (particularly through illustrative examples). However, in doing so, the Agency should ensure the promulgation of clear, non-technology specific principles that can encompass new privacy tools, including multimedia tools that can be recognized in emerging contexts and privacy dashboards that can provide pathways to multiple signal mechanisms.

B. Clarify and streamline requirements for businesses that “process” qualifying opt-out preference signals to avoid loopholes and ensure that disclosures are meaningful to average consumers.

FPF recommends three clarifications to the draft regulations concerning the requirements for how businesses are expected to respond to qualifying signals. First, the draft regulations should ensure that a business's leeway to ignore qualifying signals in order to respect a consumer's ongoing participation in a financial incentive program is appropriately tailored. The draft regulations establish a necessary 'consent hierarchy' for responding to signals that are in tension with other expressions of consumer choice. However, § 7025(c)(4) would create a potential loophole by permitting businesses to “ignore the opt-out preference signal” of a known consumer who does not affirm their intent to withdraw from a financial incentive program upon receiving notice of the conflict. The regulations should be clarified to specify that in such circumstances, a business may ignore a qualifying signal ***only with respect to that consumer's participation in the financial incentive program***, and not to any unrelated present or future sales or sharing of that consumer's personal information.

Second, the draft regulations should clarify the disclosures that businesses must provide regarding their receipt, processing, and implementation of opt-out requests. § 7025(c)(6) provides that a business “***should*** display whether or not it has processed” a consumer signal (emphasis added). The language appears permissive, especially when read in conjunction with other requirements in § 7025 that provide requirements for how a business “***shall***” respond to a valid signal. However, the Agency's Initial Statement of Reasons suggests that this provision is intended to be mandatory.⁷ Final regulations should clarify whether or not businesses are required to display a signal status.

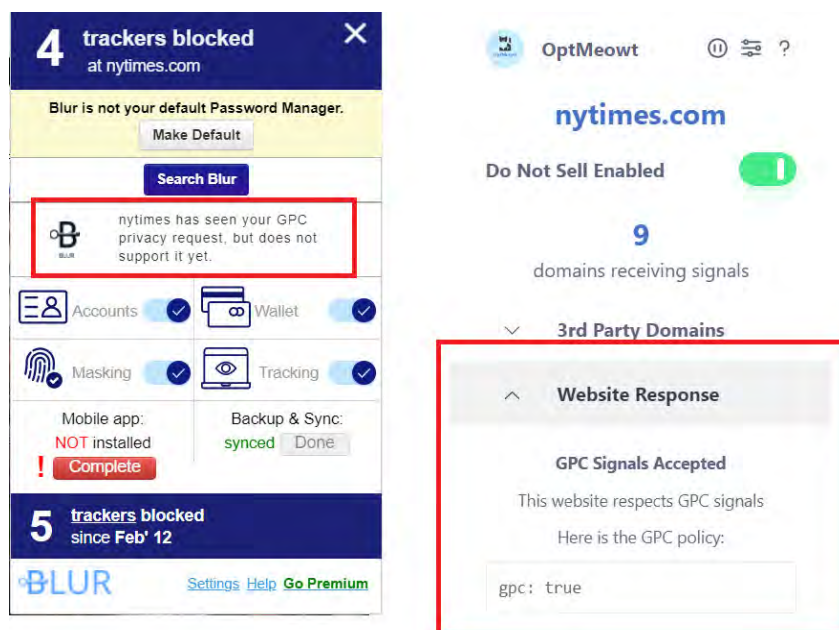
⁶ For example, more Americans own a smartphone than a laptop or desktop computer. Pew Research Center, “Mobile Fact Sheet” (Apr. 7, 2021), <https://www.pewresearch.org/internet/fact-sheet/mobile/>.

⁷ California Privacy Protection Agency, “Initial Statement of Reasons” at 37: “Subsection (c)(6) requires a business to display whether a consumer's opt-out preference signal has been accepted, and provides exemplar language for how a business can communicate this information to the consumer” https://cppa.ca.gov/regulations/pdf/20220708_isr.pdf.

Third, final regulations should clarify how § 7025(c)(6) displays will interact with the related requirement under § 7026(f)(4) to allow consumers to confirm whether an opt-out request has been “processed,” including through a display or toggle on the business’s website.⁸ For consumers, there will likely not be a meaningful distinction between displays indicating that: (1) a signal has been processed and (2) a request to opt-out has been processed. The regulations should avoid requiring businesses to unnecessarily ‘conspicuously’ clutter digital products and services by providing duplicative, potentially confusing displays regarding consumer opt-outs. Furthermore, the information on such disclosures could convey inconsistent information, as a business may “process” a signal set to opt-out of certain CCPA rights, but not implement it, if an expression of choice higher on the ‘consent hierarchy’ is present.

A simpler, more user-friendly approach would be for regulations to encourage businesses and signal providers to confirm a consumer’s opt-out status directly through a signal mechanism, a feature that is already present in some GPC plug-ins, including OptMeowt and Blur (see Figure 1). These two plug-ins, in addition to displaying whether a signal was sent, also provide information on whether a recipient website respects or honors that signal. However, at present the disclosures can be inconsistent, possibly given that such browser tools remain in an early stage of development with respect to this particular signal and its legal status in California.

Figure 1: Blur and OptMeowt Plug-ins Display How a Website Responds to the GPC signal. All screenshots taken August 19, 2022 on Chrome browser, Version 104.0.5112.81



⁸ § 7026(f)(4) “Providing a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business. For example, the business may display on its website “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.”

C. Encourage the further development of signal mechanisms that permit granular or business-specific consent choices.

In order to ensure informed consumer choice in the exercise of signals and as directed by the CPRA amendments' grant of rulemaking authority, final Agency regulations should provide guidance on mechanisms for enabling consumers to selectively consent for particular businesses to sell or share their personal information.⁹ While the draft regulation's 'consent hierarchy' would establish processes for obtaining consumer consent that would override a qualifying signal in both non-frictionless (§ 7025(c)(3)) and frictionless (§ 7025(f)(3)) interactions, as envisioned these processes would occur separately from a signal or signal mechanism. Furthermore, § 7025(c)(5) of the draft regulations would prevent businesses from responding to a user's website-specific decision to disable a global opt-out signal. The regulations should encourage signal providers to develop controls that permit consumers to exercise their privacy preferences with respect to particular businesses.

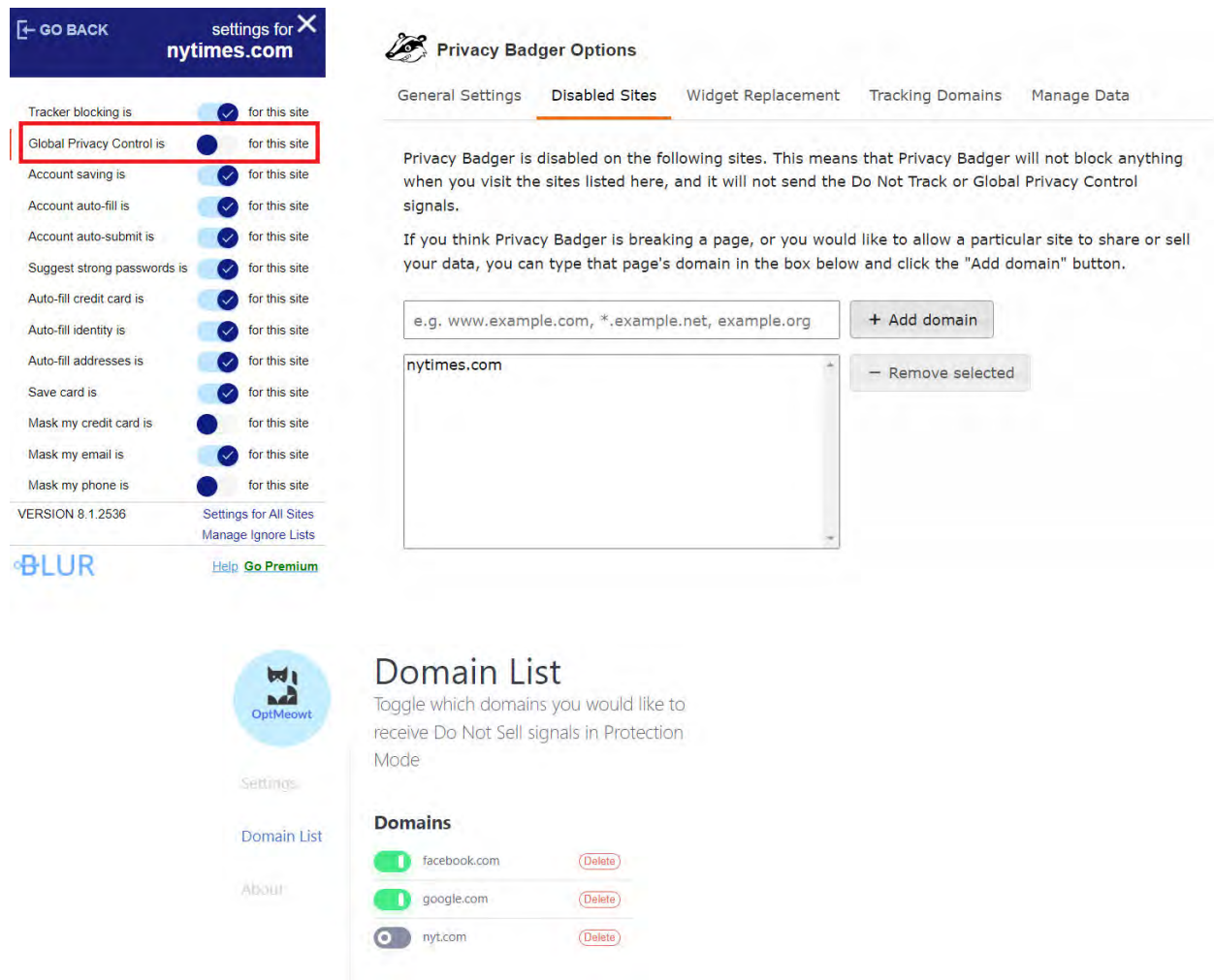
As drafted, the regulations would restrict the ability of signal providers, such as browsers and plug-ins, to offer granular, website-specific choice mechanisms to consumers, because § 7025(c)(5) holds that a business cannot interpret the absence of a previously received signal as consent to opt-in to the sale or sharing of personal information. In many cases this is a desirable policy outcome because simply visiting a website from a new browser or device without a signal mechanism installed or enabled should not override a previous expression of intent to opt-out. However, where an individual with a 'global' signal enabled engages with a business and then affirmatively chooses to disable that signal for that particular business, the regulations should permit the business to respect and implement that choice. The principle that affirmatively disabling an opt-out signal will have the impact reversing the signal's effect is intuitive, symmetrical, and easy to execute, consistent with the proposed requirements for consent contained in draft regulation § 7004. In fact, a requirement that if a consumer affirmatively disables a signal that action may not have the impact of disabling the signal would likely constitute an Agency-mandated "dark pattern," subverting user autonomy, decision making, and choice.

Notably, several plug-ins that have implemented the Global Privacy Control specification permit users to granularly enable or disable the signal for a particular business, website, or pages of a particular domain, including OptMeowt, Privacy Badger, and Blur (see Figure 2). Such controls can include functional buttons or toggles (for default-off signals) or a 'allowlist' of websites or domains

⁹ Civ. Code § 1798.185(a)(19)(A)(v): "The requirements and specifications for the opt-out preference signal should be updated from time to time to reflect the means by which consumers interact with businesses, and should... Provide a mechanism for the consumer to selectively consent to a business' sale of the consumer's personal information, or the use or disclosure of the consumer's sensitive personal information, without affecting the consumer's preferences with respect to other businesses or disabling the opt-out preference signal globally."

(for default-global signal settings). Final regulations should support rather than override the existing ability for signal mechanisms to empower consumers to exercise their rights selectively.

Figure 2: Examples of Browser Plug-ins that Allow Domain-Specific Granular Controls (Blur, PrivacyBadger, and OptMeowt). All screenshots taken August 19, 2022 on Chrome browser, Version 104.0.5112.81.=



D. Revise the Initial Statement of Reasons to reflect CCPA requirements for ensuring consumer intent in the exercise of signals.

The CPRA amendments state that implementing regulations for signal requirements and specifications should “clearly represent a consumer's intent and be **free of defaults constraining or presupposing such intent**” (Civ. Code § 1798.185(a)(19)(A)(v)) (emphasis added). However, the Agency’s Initial Statement of Reasons contains a unique suggestion, not reflected in the draft

regulations, that businesses may be required to recognize “a privacy-by-default opt-out mechanism that is built into a platform, technology, or mechanism.”¹⁰

In practice, whether or not a “privacy-by-default” setting in a browser or browser plug-in can be objectively determined to reflect a consumer’s intent consistent with the requirements of the CCPA will be a context-specific inquiry. In making this determination and establishing guidance, the Agency should consider the browser or plug-in’s primary advertised purpose, disclosures made to the user before and after installation, and whether the signal is configurable. Downloading a plug-in that has a primary advertised primary purpose that is unrelated to information privacy (such as a password manager, screen reader, or user-interface add-on) would be unlikely to satisfy CCPA’s criteria if it were to incidentally send opt-out signals by default. However, a browser plug-in that is explicitly marketed as a tool to exercise consumers’ legal rights to opt-out of the sale or sharing of personal information could satisfy the CCPA’s requirement that signals clearly represents a consumer’s intent. For example, the plug-in OptMeowt is currently described in the Chrome Store download page as allowing “Web users to make use of their rights to opt out from the sale and sharing of personal data” and has no functionality unrelated to sending the GPC specification.¹¹

Browsers, unlike plug-ins, may require a more holistic analysis, given their necessary intermediary role between users and websites, the fact that most users have fewer options to choose from, and the multitude of reasons for which average users choose and continue to rely on their preferred browsers. Based on our analysis of the CCPA, it is unlikely that a browser, operating system, or multi-purpose device, even one that markets itself as generally protective of individual privacy, could enable an opt-out signal on behalf of its users in a way that would meet the Act’s statutory requirements that signal mechanisms shall be free of defaults constraining or presupposing consumer intent. In general, the decision to adopt or use a particular browser is often based on a wide variety of factors including generally protecting privacy, but also features such as ad blocking, speed, user interface design, security, and safety.¹² It would be impracticable to infer, from objective factors, that an individual has chosen to use a browser or similar multi-purpose intermediary product due to a default ‘do not sell or share’ signal feature. Furthermore, the default enabling of signals by intermediary platforms would threaten to “unfairly disadvantage” other businesses, potentially selectively, in violation of Civ. Code § 1798.185(a)(19)(A)(i).

This is an important issue for the Agency to address because at least one existing web browser currently transmits the GPC by default without notice to users either on its download page or in

¹⁰ ISOR at 34.

¹¹ Chrome Web Store, OptMeowt download page:

<https://chrome.google.com/webstore/detail/optmeowt/hdbnkdbhglahihjdbodmfefogcjbpgbo?hl=en-US>.

¹² See e.g., Michael Muchmore, “Edge, Firefox, Opera, or Safari: Which Browser is Best?” PC Mag (Apr. 4, 2022), <https://www.pcmag.com/picks/chrome-edge-firefox-opera-or-safari-which-browser-is-best>.

the browsers' settings, contrary to the CCPA's statutory requirements.¹³ As browsers increasingly compete on privacy, the Agency should not look to whether a browser has obtained market dominance or widespread adoption before assessing whether its integration of opt-out preference signals unfairly disadvantages other businesses. Rather, the Agency should establish principled, objective factors – including, for example, examining the advertised purposes of a browser or tool, disclosures to users before and after download, and whether a setting is configurable, in determining qualifying opt-out signals.

E. Final regulations should enable users to exercise granular control over their privacy rights through opt-out preference signals.

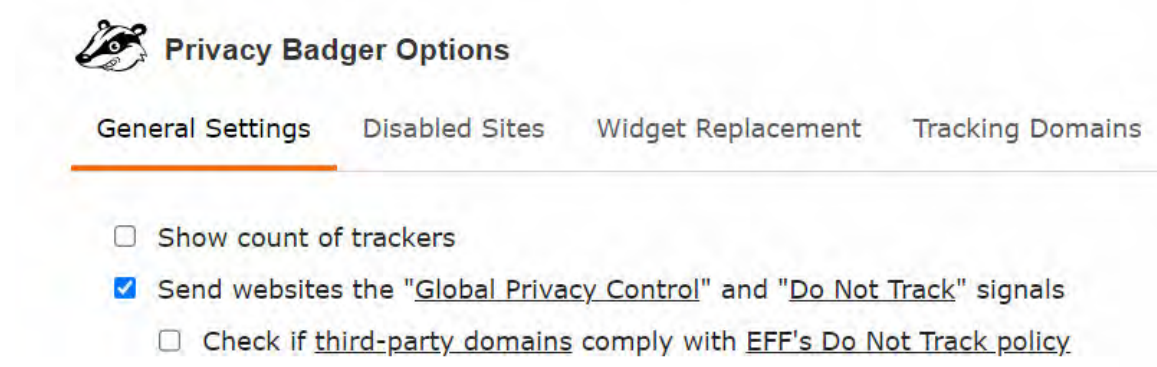
The amended CCPA establishes three distinct consumer rights that may be exercised through opt-out preference signals, the rights to: (1) opt-out of data sales, (2) opt-out of data sharing, and (3) limit the use and disclosure of sensitive personal information (Civ. Code § 1798.120-121). The invocation of each of these rights may have different effects and potentially impact the functionality of products and services enjoyed by consumers in different ways. Therefore, it can be anticipated that consumers may wish to exercise different combinations of these rights through signals on either a global or selective (business-by-business) basis. Regulations should support such granularity of choice in a manner that is consistent, clear, and not overwhelming for users.

However, the current GPC specification, as developed for the CCPA prior to the CPRA amendments, only conveys whether the signal is enabled or not; it does not permit the granular exercise of underlying rights. Meanwhile, there are inconsistent disclosures in the current marketplace about what rights the GPC is intended to invoke. Some providers specify that the GPC will opt consumers out of data sales, while others portray that the signal will jointly invoke the right to opt out of both sales and sharing.¹⁴ Furthermore, some plug-ins, such as the Privacy Badger, may constrain user autonomy by bundling the Global Privacy Control with other settings such as the 'Do Not Track' ("DNT") specification, without functionality that would permit users to disaggregate these features (see Figure 3).

¹³ The Brave browser "does not require users to change anything to start using the GPC to assert your privacy rights. For versions of Brave that have GPC implemented, **the feature is on by default and unconfigurable**" (emphasis added). Peter Snyder, "Global Privacy Control, a new Privacy Standard Proposal," Brave (Oct. 7, 2020), <https://brave.com/web-standards-at-brave/4-global-privacy-control/>.

¹⁴ For example, Disconnect's help page (linked through the plug-in) states that: "The Enable GPC checkbox sends a Do Not Sell signal under the CCPA to sites you visit. The Global Privacy Control signal is experimental and non-binding." Alternatively, hovering over the GPC toggle on the Blur plug-in displays a statement that says "Requesting a site to not share or sell your data."

Figure 3: Privacy Badger Plug-in “General Settings.” All screenshots taken August 19, 2022 on Chrome browser, Version 104.0.5112.81.



Recognizing that the Agency has postponed promulgating regulations on some statutorily-directed aspects of opt-out preference signals,¹⁵ FPF encourages future Agency regulations to allow consumers to exercise granular control over their California privacy rights.

F. Establish an authoritative, multistakeholder process for the review and approval of qualifying signals and transmitting mechanisms

As signal specifications are developed and refined over time, new questions will arise as to whether a particular signal or signal-transmitting platform, technology, or mechanism meets the requirements of the CCPA and its implementing regulations. Consequently, FPF reiterates the suggestion in our November 2021 pre-rulemaking comments that the Agency establish an open, multistakeholder process for the ongoing review and approval of new signal mechanisms over time.¹⁶ This process should include engagement with regulators in other jurisdictions that provide for the recognition of opt-out signals (particularly Colorado and Connecticut) in order to support as much interoperability as possible given underlying statutory differences in consumer rights, signal specifications, and consent hierarchies.

In addition to providing clarity for regulated businesses, active ongoing engagement from the Agency is uniquely important for California consumers and the developers of signal mechanisms. For consumers, public approval of either specific mechanisms (such as browsers and plug-ins) or the criteria for such mechanisms will allow them to have confidence that the specific tools they choose to enable will have real legal effect. It will also allow them to file complaints with the Agency for enforcement when they perceive that their requests are not being honored. For developers of platforms, intermediaries (browsers), and plug-ins, active Agency involvement will

¹⁵ ISOR p. 33.

¹⁶ Future of Privacy Forum “Comments PRO 01-21” at 9 (Nov. 8, 2021), <https://fpf.org/wp-content/uploads/2021/11/Future-of-Privacy-Forum-Comments-PRO-01-21.pdf>

allow them to continue competing on privacy while detecting and implementing qualifying signals in a way that meets California's legal requirements.

At the same time, it is important to recognize that a regulated entity that receives a signal may not be able to determine its specific source or transmitting mechanism (for example, whether the signal came from a user's browser, specific plug-in, a device setting, or other tool). In such cases, the signal source is relevant because the same specification or signal, such as the Global Privacy Control, could be implemented by providers or provided to consumers in ways that either do or do not meet the CCPA's requirements – and the receiving entity may have no way of distinguishing. In this situation, the Agency should actively discourage the non-compliant implementation of an otherwise qualifying signal while ensuring that businesses do not use the existence of non-compliant implementations of a small percentage of the total signals in the market as a justification to ignore all such signals.

Thank you for this opportunity to provide input on the Agency's initial draft implementing regulations for the California Privacy Rights Act amendments. We welcome any further opportunities to provide resources or information to assist in this important effort. If you have any questions regarding these comments and recommendations, please contact Keir Lamont at [REDACTED]

Sincerely,

Keir Lamont
Senior Counsel

Jason Snyder
FPF Policy Intern

From: **Ben Isaacson** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 15:45:53 (+02:00)
Attachments: IHP CPPA Public Comment.pdf (5 pages)

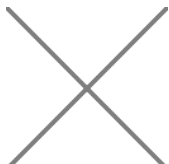
WARNING: This message was sent from outside the CA Gov network. Do not open attachments unless you know the sender: [REDACTED]

Mr. Soublet,

Please find the attached comments on behalf of In-House Privacy, Inc.

Sincerely,

--Ben



Ben Isaacson

Principal | In-House Privacy, Inc.

CIPP/US, CIPP/E

m. [REDACTED]

w. www.inhouseprivacy.com

e. [REDACTED]

August 23, 2022

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

RE: In-House Privacy, Inc. CPPA Public Comments

Dear Mr. Soublet and Members of the California Privacy Protection Agency:

In-House Privacy appreciates the opportunity to comment on the proposed regulations to implement the California Privacy Rights Act of 2020 (CPRA). In-House Privacy is a boutique privacy law and consulting practice, serving a diverse set of companies ranging from early-stage startups to large public enterprises. While we provide a broad range of privacy counsel and consulting services, our core practice is advising companies who provide advertising and marketing services. To learn more, visit www.inhouseprivacy.com.

Our comments are focused primarily on areas that may impact business services that the California Privacy Protection Agency (Agency) may not have contemplated, with particular emphasis on the mobile application ecosystem.

§ 7002. Restrictions on the Collection and Use of Personal Information

The draft regulations propose an ‘average consumer expectation’ test to determine whether the personal information processing is reasonably necessary or proportionate to the business use. The draft regulations provide numerous examples, but do not provide any type of ‘balancing test’ or other objective guide for companies to follow in determining whether any such processing activities could be ‘compatible’ with a business purpose.

For example, many businesses supporting online advertising and marketing services engage in activities that are viewed as ‘essential’ by the advertiser or media company in order to justify their advertising value, such as measuring advertising performance, but these services may not be expected by a consumer and thus not viewed as ‘necessary and proportionate’ from a consumer perspective. Another common example is where two businesses wish to jointly market a product or service, and need to share certain information to either validate the value proposition, or engage in the joint marketing campaign. Any such ‘sharing’ or ‘combination’ of personal information is unlikely to be viewed as ‘compatible’ with the original purpose, but is intended to provide a new benefit or opportunity for the consumer.

We recommend that the Agency carefully review this potential regulation, and consider;

1. Re-shaping the regulation to reflect a more objective balancing test such as the types used by companies in order to comply with Europe’s General Data Protection Regulation (GDPR) through ‘Data Protection Impact Assessments’ or ‘Legitimate Interest Assessments’. An

objective test would include an analysis of the potential information uses described prior to information collection, and in compliance with the transparency and disclosure requirements inherent in the text of the law and other regulations, notably Sections 7003, 7010, 7011 and 7012;

2. Adding additional exemptions for common business activities, notably engaging in any 'business purposes' by contracted service providers;
3. Modifying the 'explicit consent' requirement for new activities where there is a direct and material benefit to consumers, and where the business provides individuals with advanced notice and a list of privacy or other preferences where they can choose to limit or opt-out of those new activities; or
4. Removing this proposed regulation and rely upon its authority to enhance and enforce other regulations requiring specific disclosures, notably in Sections 7003, 7010, 7011 and 7012 that mandates the necessary information to be presented to California consumers so that there are no 'unexpected' or 'disproportionate' processing activities.

§ 7050. Service Providers and Contractors

The draft regulations includes the following statements in §7050(c);

"A service provider or contractor cannot contract with a business to provide cross-contextual behavioral advertising."

"A person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor."

The draft regulations do not clarify or enumerate the scope of 'cross-contextual behavioral advertising' (CCBA) in this context. As a result, companies that have been engaged as service providers under the 'advertising and marketing services', 'analytic services', or other business purposes of the CCPA may be required to determine whether they are legally able to continue to operate as service providers following enactment of the proposed regulations.

Specifically, the law includes within the definition of CCBA *"the targeting of advertising to a consumer"*¹. The draft regulations do not clarify whether "targeting" is limited to the process of 'identifying' an individual or device in order to serve a cross-contextual behavioral ad to, the 'decision-making' process of which advertiser or advertisements are allowed to deliver an ad, or broadly whether CCBA may incorporate all the potential activities supporting or adjacent to the cross-contextual behavioral ad delivery, viewership and click activity, or the post-ad engagement activities measured by the advertiser or their service providers.

We request that the Agency clarify that CCBA is limited to only those entities where a business 'identifies or decides' the individuals or devices that receive cross-contextual behavioral ads, and expressly excludes any businesses that may collect and/or combine information about the individual or device following the delivery of, or engagement with, the cross-contextual behavioral ad. To be clear, we request that any service providers engaged in 'advertising and marketing' or 'analytic services'

¹ 1798.140(k)

business purposes that support cross-contextual behavioral advertising activities, before or after the cross-contextual behavioral ad is delivered, be allowed to continue operating as service providers. These services include, but are not limited to;

1. Determining whether the ad recipient was not a 'bot' or otherwise engaged in potentially fraudulent activities;
2. Limiting a potential ad recipient from receiving an ad based on prior delivered ads, ad engagements, or other behavioral activities (ie; 'frequency capping' or 'suppression'); and
3. Measuring ad performance, including receiving and combining the impressions, clicks, and associated business engagement activities in order to provide reporting to the business.

Further in the same Section 7050(c), it states;

"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."

There is significant ambiguity in the 'shall not combine' business requirements. Specifically, if a business receives an opt-out request, and is utilizing a measurement service to collect information on ad performance from the advertising networks or media providers, then it may be incumbent on the mobile measurement service to 'combine' that opt-out information with any other information about that device in order to maintain the interests of that individual in being suppressed from any additional processing of their personal information. In other words, the combination of the opt-out with other information may be essential in order to effectuate the opt-out and suppress the individual from being associated with measurement activities, or other opt-out processing requirements.

Moreover, § 7051 of the proposed regulations go into extensive detail on the contractual requirements for service providers, which may also include 'combining' opt-out information from disparate sources on behalf of a business, which would be in direct conflict with the text of the law and proposed regulations. In order to be classified as a service provider in compliance with the proposed § 7051 regulations, it would seem to be the intent of the CPRA authors to enable service providers to effectuate opt-out requests in every possible use case where those requests are required to be administered.

As a result, we recommend that the Agency clarify the scope of 'combining' information and provide an exemption for service providers who may combine CCBA-related information for the express purpose of completing or maintaining an opt-out request.

Provide A Temporary Exemption For Existing Service Providers

We recognize that the Agency is working towards finalization of the draft regulations in advance of the 2023 deadlines for enactment and enforcement. Businesses that currently operate as service providers under the ‘advertising and marketing’, ‘analytic services’, or other business purpose that provides services in support of certain CCBA activities are under immediate pressure from clients and business partners to modify or re-establish the terms of their agreements in order to continue their business relationships in 2023. Much of these potential legal terms modifications stem from the proposed regulations, which will determine whether these businesses may continue operating as ‘service providers’. With the completion of the final regulations being so close to the end of the year, it is likely that these businesses will be forced to expedite legal terms changes, which could be a significant burden for businesses to complete prior to the end of the year.

As a result, we request that the Agency consider granting a temporary exemption for existing service providers to continue operating under their current terms as service providers for a one-year period following the issuance of the final regulations.

§ 7004. Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent

The proposed regulations go into great detail about the required form, methods, and processes to effectuate consent for businesses to ‘sell or share’ personal information. As applied to the mobile ecosystem, it is important to note that the businesses operating mobile applications often do not control the primary form, methods, and processes for acquiring consent from end users. Instead, the mobile operating systems providers, namely Apple and Google/Android, determine these activities.

In 2021, Apple released its ‘AppTrackingTransparency’ framework (‘ATT’), which mandated to app developers on the Apple App Store the specific mechanisms they must use in order to properly acquire consent from individuals for sharing their Identifier for Advertisers (IDFA). Apple’s prescribed processes require app developers to present an affirmative consent ‘pop-up’ with two choices; a) “Ask App Not To Track”, or (b) “Allow” (‘tracking’), with very little customizable text for the app to clarify their business rationale for this request. In compliance with the CCPA, advertisers or advertising supported apps on the Apple App Store who ‘sell or share’ personal information primarily do so by sharing the IDFA with their designated advertising service providers, third parties or business partners. In order to share the IDFA, each consumer must confirm their consent through the ‘Allow’ option presented by both the advertiser and the ad supported app. In other words, for mobile advertisers or ad supported apps on iOS to deliver a cross-contextual behavioral ad, they both must receive consent from the recipient of the ad.

Apple iOS app developers are unable to modify the consent choices mandated by the ‘ATT’ developer terms, and apps are afforded very little copy to be presented alongside the consent choices. As a result, there are numerous conflicts presented between the proposed §7004 regulations, and Apple’s (and to an extent, similar Google/Android’s) requirements. Specifically, these conflicts include;

1. Not enough text available for apps to disclose that the Apple iOS ‘Allow’ choice is equivalent to a consent for the app to ‘sell or share’ the individual’s personal information. The small number

of characters Apple allows for apps to customize text alongside the 'Allow' choice is insufficient to communicate all of the requirements inherent in §7004, including providing granularity in choice to the end user.

2. There is no 'symmetry in choice' in the presentation of Apple's specified consent choices as prescribed by §7004. Whereas most 'symmetry in choice' would enable customized language and placement of choices (eg; font type, length, or choice positioning), or additional options for individuals to click through and 'learn more' before agreeing to consent, no such customization is currently available in the Apple iOS 'ATT' developer tools.
3. The process currently required by Apple (and to an extent, Google/Android) does not clarify for individuals that the 'Ask App Not To Track' is not the equivalent of a 'Do Not Sell or Share My Personal Information', or even an opt-out of cross-contextual or other types of behavioral ads, nor is 'Allow' the equivalent to an opt-in or 'explicit' consent request to enable businesses to 'sell or share' their personal information.

As a result, businesses that wish to comply with the CCPA will likely present California consumers with a secondary privacy preferences menu of choices following their previous Apple or Android-specific preferences requests, which will result in a less user-friendly mobile app experience, and will negatively impact the mobile app ecosystem.

We request that the Agency consider additional rules or enhancements to §7004, such as:

1. Require mobile operating systems to subjugate their mandatory advertising or 'tracking' consent mechanisms to enable certified or otherwise approved alternative consent mechanisms by businesses that have demonstrated mechanisms designed to be more compliant with §7002 and 7004 for California consumers. These may include the use of approved 'Consent Management Platforms' (CMPs), or other consent user interface guidelines that the mobile operating system may put forth; or
2. Clarify in a final §7004 regulation that individuals who accept a mobile operating system consent for sharing a unique identifier intended for use with cross-contextual behavioral advertising or other potential 'sales or sharing' activities can do so without the need for the app to present a secondary consent request for the 'sale or sharing' of their personal information.

We appreciate your consideration of the above comment, and am available if you would request any further clarity at [REDACTED] .

Sincerely,

[REDACTED]

Benjamin Isaacson
Principal, In-House Privacy, Inc.
www.inhouseprivacy.com

From: **McArthur, Webb** [REDACTED]
 To: **Regulations** <Regulations@cpha.ca.gov>
 CC: **Eric Ellman** [REDACTED]
 Subject: CPPA Public Comment
 Date: 23.08.2022 22:51:13 (+02:00)
 Attachments: CDIA CPPA CPRA Rulemaking Comment Letter Aug 2022.pdf (7 pages)

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

Good afternoon,

Attached are the comments of the Consumer Data Industry Association (CDIA) on the Proposed CCPA Regulations Rulemaking. We appreciate the opportunity to participate in this rulemaking process.

Out Of Office: Please note that I will be out of the office and offline from August 28 through September 7, 2022.

Webb McArthur
 Partner | Admitted in the District of Columbia, Maryland, and Virginia
 Hudson Cook, LLP
 Direct: [REDACTED] | Cell: [REDACTED]
 1909 K St., NW | 4th Floor | Washington, DC 20006



The information contained in this transmission may be privileged and may constitute attorney work product. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact Webb McArthur at [REDACTED] or [REDACTED] and destroy all copies of the original message and any attachments.

* * * *



Consumer Data Industry Association 1090
Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

P 202 371 0910

Writer's direct dial: [REDACTED]

CDIAONLINE.ORG

August 23, 2022

Via Electronic Delivery to
regulations@coppa.ca.gov

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

RE: COPPA Public Comment in response to Notice of Proposed Rulemaking on proposed amendments to regulations concerning the California Consumer Privacy Act

Dear Mr. Soublet,

The Consumer Data Industry Association submits this comment letter in response to the California Privacy Protection Agency ("COPPA") Notice of Proposed Rulemaking on proposed changes to California Consumer Privacy Act ("CCPA") regulations related to the California Privacy Rights Act ("CPRA").

The Consumer Data Industry Association ("CDIA") is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity all over the world, helping ensure fair and safe transactions for consumers, facilitating competition, and expanding consumers' access to financial and other products suited to their unique needs.

CDIA members have been complying with laws and regulations governing the consumer reporting industry for decades. Members have complied with the Fair Credit Reporting Act ("FCRA"), which has been called the original federal consumer privacy law. The FCRA governs the collection, assembly, and use of consumer report information and provides the framework for the U.S. credit reporting system. In particular, the FCRA outlines many consumer rights with respect to the use and accuracy of the information contained in consumer reports. Under the FCRA, consumer reports may be accessed only for permissible purposes, and a consumer has the right to dispute the accuracy of any information included in his or her consumer report with a consumer reporting agency ("CRA").

CDIA members have been at the forefront of consumer privacy protection. Fair, accurate, and permissioned use of consumer information is necessary for any CDIA member client to do business effectively.

CDIA appreciates the CPPA's invitation to comment on this important rulemaking process. As we describe in greater detail below, CDIA members provide, among other services, identity verification, fraud detection and prevention, and other security and integrity services to their customers. These services involve the processing of personal information, including sensitive personal information. Among other topics discussed greater detail below, CDIA strongly urges the CPPA to ensure that CCPA obligations do not interfere with these security and integrity activities, businesses may make incompatible secondary use of personal information upon notice and extension of springing consumer rights, businesses continue to have flexibility in verifying household information requests, and third parties will be permitted to make their own assessments in responding to forwarded consumer requests.

CDIA also strongly encourages the CPPA to postpone enforcement of the CPRA until one year after regulations are finalized. The CPRA required the CPPA to finalize regulations by July 1, 2022, providing one year until enforcement would begin, on July 1, 2023. Because the regulations were not finalized as provided in the CPRA, enforcement should be postponed to one year after the regulations are finalized.

To assist the agency in finalizing clear and effective regulations that allow businesses to best support customers and consumers, CDIA offers the following comments on the proposed revisions:

I. Restrictions on the Collection and Use of Personal Information

Proposed section 7002(a) provides that a business' collection, use, retention, and/or sharing of consumer personal information must be necessary and proportionate to achieve the purpose or purposes for which the personal information was collected or processed. The proposed section goes on to state that "[t]o be reasonably necessary and proportionate, the businesses's collection, use, retention, and/or sharing must be consistent with what an average consumer would expect when the personal information was collected" unless (1) the further use is disclosed to the consumer and compatible with the expectations of the "average consumer" or (2) the business obtains the consumer's "explicit consent" as detailed at proposed section 7004.

First, the CPRA does not provide for any "average consumer" standard to assess whether a particular processing activity is necessary and proportionate to achieve the purposes for which the personal information was collected and processed. Instead of an "average consumer" standard, the CPRA sets a reasonableness standard. Businesses, consumers, and regulators may have differing views on who the "average consumer" is and what they would expect, which could result in different standards applied to different industries and contexts. Such a standard is unworkable in practice and contrary to the statute. Accordingly, CDIA urges the CPPA to remove the "average consumer" standard entirely and provide, consistent with the CPRA, that businesses

may use personal information for purposes other than those that are disclosed at collection so long as they are compatible with a disclosed purpose.

Second, the CPRA, at section 1798.100(a)(1), prohibits a business from using personal information collected for purposes incompatible with those disclosed at collection without “providing the consumer with notice.” The CPRA does not require the business to obtain explicit consent, and this proposed rule is inconsistent with the text of the statute. The CPRA permits use for additional purposes upon notice because it provides consumers with specific rights, including to request that use of sensitive personal information be limited, to opt out of the sale or sharing of personal information, and to delete personal information. CDIA therefore urges the CPPA to remove this “explicit consent” requirement for uses incompatible with the initially disclosed purposes.

Third, the proposed section also provides an illustrative example, at subsection (b)(2), of a cloud storage services provider collecting personal information to provide the cloud storage services to consumers, noting that the business would not be able to use the personal information to research and develop unrelated or unexpected new products or services without the consumer’s consent. Additionally, illustrative example (3) details that an internet services provider might collect geolocation information to provide its services but would not be permitted to sell or share the geolocation information with data brokers without explicit consent.

Setting aside the issue of whether the CPRA might require “explicit consent,” we would encourage the CPPA to expressly provide that using personal information to detect or prevent fraud is permissible because such a use would not be unrelated to the product or service provided the consumer, nor would such a use be incompatible with the purpose for which the information was collected. Without clarification, there may be uncertainty about whether providers of fraud detection and prevention services may use personal information to prevent and detect fraud as well as what kind of disclosure or consent would be necessary.

II. Requirements for Disclosures and Communications to Consumers

Proposed section 7003(c) requires businesses to place links on websites required under the CCPA in a similar manner as other links used by the business on its homepage, providing an example that the business is to use a font size and color that it at least the approximate size or color as other links on the website. Although presented as an example, this requirement is overly prescriptive and does not take into account the various ways websites may be styled. A site’s logo may be a live link and could require CCPA links to be very large or in complex color patterns. CDIA urges the CCPA to emphasize the flexibility in this font size and color requirement. In particular, we suggest the CCPA links be expected to be the same size and font as other links in close proximity (e.g., the bottom of the page).

III. Privacy Policy

Proposed section 7011 would require that businesses provide a comprehensive description of the business’ online and offline practices regarding the collection, use, sale, sharing, and retention of personal information. Online privacy practices typically are meant to

communicate the privacy practices of a website operator with regard to the personal information collection, use, sharing, and security of those visiting the website. Requiring disclosure of the offline personal information privacy practices of businesses represented on a particular website could cause confusion to visitors of the website, particularly where online and offline data practices vary.

Further, proposed section 7011 would require businesses to make affirmative statements regarding minor personal information processing and opt-out signal receipt, even where a business may be unable to confidently make such statements. CDIA urges the CPPA to require these online disclosures, described at subsections (c)(1)(G) and (3)(F), only to the extent that the business knows or has reason to know the subject of the disclosure.

IV. Notice at Collection of Personal Information

Proposed section 7012 provides that the notice at collection must be made readily available where consumers encounter it at or before the point of collection of any personal information, with examples of a link to the notice posted on the introductory page of the website and on all pages where personal information is collected as well as in close proximity to any webform. These examples add confusion as to whether a business may satisfy the notice at collection requirement by posting an online privacy policy with all required content, whether the privacy policy must be linked on all pages of the website, and when the content of the policy must be placed on various pages instead of just being provided by way of a link. CDIA urges the CPPA to clarify how these examples interact with the ability to satisfy the notice at collection requirement by posting and linking to the online privacy policy.

V. Requests to Delete

Proposed section 7022(b) requires businesses to notify service providers, contractors, and third parties to whom the business has sold or shared personal information of a consumer's request to delete personal information. However, the proposed rule includes no limitations on this notification requirement, such as limiting the notification requirement to where there is an active service provider or contractor relationship or where the business sold or shared personal information within the previous year. CDIA encourages the CPPA to provide for reasonable limits so that businesses are not required to retain records of the personal data, transfers, and uses indefinitely simply to comply with this notification requirement.

VI. Requests to Correct

Proposed section 7023 states, in part:

“(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.”

Businesses that retain information for the purpose of detecting and preventing fraud, identity theft, or security incidents need to be able to retain personal information in its original form, despite any request to correct. For example, if a consumer contacts a business, verifies

their identity, and updates their address, businesses need the flexibility to retain the former address for use in future identity verification needs, rather than being required to update it and delete the old information. Further, businesses need to be able to retain previously-collected personal information for other reasons, particularly complying with legal obligations (for example, legal holds), complying with contract obligations (for example, updating information through third-party sources like USPS address change notifications), processing the information for other limited internal uses not incompatible with previously disclosed purposes. This proposed section does not clearly permit businesses to retain information it updates as previous data points, and CDIA urges the CPPA to explicitly permit retention of personal information for the purposes already detailed in the CCPA for the right to delete, at Cal. Civ. Code § 1798.105(d).

Additionally, the proposed “totality of circumstances” test provides new and broader criteria for business to consider when determining whether to deny a consumer’s request to correct personal information. In particular, the proposed rule provides that in the case that the business is not the original source of the personal information, “the consumer’s assertion of inaccuracy may be sufficient to establish that the personal information is inaccurate.” Under the proposed test, businesses would be required to accept, review, and consider any documentation that the consumer provides and explain the basis for denial to the consumer. This would prove challenging to businesses that do not have direct interaction with the consumer in question. These challenges would be particularly acute with regard to the requirement to provide a detailed explanation of the basis for the denial and could create confusion for consumers. CDIA thus respectfully requests that businesses be granted the option to treat a request to correct in the same manner as a request to delete.

VII. Requests to Know

Cal. Civ. Code § 1798, as amended, provides that “[t]he [right to know] disclosure . . . shall cover the 12-month period preceding the business’ receipt of the verifiable consumer request” and that “a consumer may request that the business disclose the required information beyond the 12-month period, and the business shall be required to provide that information unless doing so proves impossible or would involve a disproportionate effort.”

Proposed section 7024 states, in part, that “a business shall provide all the personal information it has collected and maintains about the consumer on or after January 1, 2022, including beyond the 12-month period preceding the business’s receipt of the request, unless doing so proves impossible or would otherwise involve disproportionate effort.”

The draft regulation may be read to imply that businesses would be required to provide personal information beyond the 12-month lookback period as a default, even if the consumer does not request it. Such a requirement would contradict the statutory provision. CDIA would urge the CPPA to clarify that the requirement to provide personal information beyond the 12-month lookback period only applies if the consumer requests it, such as by adding “if the consumer so requests” after “the business’s receipt of the request.”

Further, the processes required for requests to know differ from other consumer requests, requiring businesses to set up unique flows to process different requests that arise

under the CCPA, let alone flows required by different state laws. CDIA urges the CPPA to provide for flexibility, consistency where possible, and uniformity with other state laws in terms of evaluation processes, consumer responses, denial explanations, and third-party notifications.

VIII. Requests to Limit Use and Disclosure of Sensitive Personal Information

Proposed section 7027(l)(3) permits businesses to use and disclose sensitive personal information in order to resist malicious, deceptive, fraudulent, or illegal actions directed at the business without requiring those businesses to offer consumers a right to limit. However, this exception does not extend to a business' efforts to prevent fraud or other malicious, deceptive, or illegal actions on other businesses. Conversely, the CPRA, at Civil Code, § 1798.121(a), provides for a broader exception, permitting the use and disclosure of sensitive personal information to help to ensure "security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes." Cal. Civ. Code § 1798.140(e)(2).

CDIA members provide "security and integrity" services, like fraud detection and identity verification services, to their business customers. Providing these services may involve comparing inquiry data with data available elsewhere, detecting anomalies in provided data, and otherwise analyzing multiple data sets, all with the goal of detecting—and thus preventing—identity theft, fraud, and other illegal actions on businesses and consumers. These efforts reduce business costs and protect consumers, whether such consumers are business customers or not, and thus further consumer privacy.

If fraud prevention and services providers are unable even to use sensitive personal information to prevent fraud on third parties, consumer privacy may be affected significantly and detrimentally. CDIA strongly urges the CPPA to expand this exception to align with the CPRA and allow businesses to use sensitive personal information for fraud prevention and detection services related third parties to further consumer privacy and identity theft prevention efforts.

IX. Requests to Know or Delete Household Information

Section 7031 is proposed to be deleted in its entirety. This section provides for requirements under which consumers may provide requests with regard to household information, which is personal information under the CCPA. These requirements ensure that all members of the household agreed to such request, that the identity of all members would have to be verified, and that the members would have to be confirmed as current members of the household. Without this guidance, it is unclear how businesses would be expected to process household information requests, and whether businesses could deny such requests if they are unable to perform these reasonable checks to ensure the privacy of household members.

X. Service Providers and Contractors and Contract Requirements for Service Providers and Contractors

Proposed section 7051(a)(1) restricts service providers from selling or sharing personal information they receive from or on behalf of the businesses to which they provide services.

Brian Soublet – California Privacy Protection Agency (CPPA)

August 23, 2022

Page 7

Other subsections impose other restrictions, including on retaining, using, or disclosing personal information other than those specified in the service provider agreement, “unless otherwise permitted by the CCPA and these regulations,” like subsection (a)(3). CDIA members provide fraud detection and prevention services and may do so, in some contexts, as a service provider to a business. Those services may involve the disclosure of personal information received on behalf of the business to third parties in relation to providing fraud detection and prevention services. CCPA regulations—notably proposed section 7050(b)(5)—specifically permit service providers to process data in their position to “detect data security incidents or protect against malicious, deceptive, fraudulent, or illegal activity.” In order to ensure that fraud prevention and detection service providers can continue to provide their important services related to minimizing identity theft and fraud on consumers and businesses, CDIA strongly urges the CPPA to add “unless otherwise permitted by the CCPA and these regulations” to subsection (a)(1), as it does with other contract requirements.

XI. Third Parties

Proposed section 7052(a) requires third parties to comply with deletion requests provided to them by the business from which they received the personal information, and that the only way the third party may retain the personal information would be to become a service provider or contractor with regard to the personal information. However, this provision does not expressly permit the third party to decline to delete the personal information for reasons listed under Cal. Civ. Code § 1798.105(d) independent of the business’ determination. As an example, a third party may have received data from a business partner to offer a product or service to the consumer, and the originating business would not be able to assess whether the third party needs to retain the information to perform under a contract between the business and the consumer. In this case, the third party needs to be able to decline to delete the personal information under a legal basis where the originating business passed to the request. It also appears unclear whether contract requirements for third parties are applicable to third parties not located in California, assuming the business does business in California. CDIA urges the CPPA to clarify in proposed section 7052(a) that third parties may decline requests to delete passed on to the third parties for bases described at Cal. Civ. Code § 1798.105(d).

* * *

Thank you for the opportunity to share our views on the anticipated rulemaking under the CPRA. Please contact us if you have any questions or need further information based on comments.

Sincerely,



Eric J. Ellman

Senior Vice President, Public Policy & Legal Affairs

From: **Randy Powell** [REDACTED]
 To: **Regulations** <Regulations@coppa.ca.gov>
 Subject: CPPA Public Comment
 Date: 23.08.2022 22:56:02 (+02:00)

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

Dear Board Members,

Although it appears that the writing of the proposed privacy rules may already be complete, I would none-the-less like to make a suggestion based on my experience with a credit card provider who had solicited my business via USPS mailers.

Often, as consumers, we are restricted (in fact or by obscurity) in how we can contact a commercial entity - especially if already in an existing business relationship - and in particular if trying to express a grievance or end that relationship. However when initially engaging with the entity, they usually make it *extremely easy to sign up*, commit to a relationship, and/or establish a billing relationship. Some past examples of this include business such as AOL, cable TV providers, and ISPs.

In my case I had received frequent written solicitations from Capitol One credit card services. At one point the mailer included a very favorable interest rate. Needless to say, the written invitation included few contractual details. The only mode presented in the mailer to find out about those details was to call a 1-800 phone number. Since I wanted to investigate the details, I had no choice but to call that number.

When I called the number, I initially heard a common notification that my call might be recorded - but no option was given to disallow that recording. Once I was connected with a live representative, I first requested that the call NOT be recorded.

The representative emphatically said NO to my request. It is my understanding that under current law, they can do that. So at that point, I said to him that I too was going to record the call (in actuality my phone line is not equipped to record anything other than an incoming voicemail message).

His angry response was "You can't do that!". I insisted that I would do so, *since all parties were aware that the call could be recorded*. Shortly thereafter HE hung up on me.

While I recognize that some of the individual elements in my situation are beyond your agency's purview, it seems to me that *if commercial recording is permitted and announced, both parties should have the right to record the call*.

This is especially true if the commercial entity finds that their recording of the call does not support their position, claims, or assertions - after which they might claim that the call was not recorded, that the recording had been routinely deleted, or was "lost". The essential result of a two-way recording option should be similar to situations wherein a police officer wears a body camera, but civilians have the right to also make a video and or audio recording of an incident - as long as they do not interfere with police carrying out their activity.

While my suggestion does not *restrict* a commercial entity from recording a call (with proper notification), this sort of allowance would provide greater transparency regarding the discussion and place all participants on a more even playing field.

Thank you for your consideration, and for your prior and continuing work on improving

privacy rights for the residents of California.

Sincerely,
Randy Powell

From: **Lindsey Stewart** [REDACTED]
To: **Regulations** <Regulations@cpha.ca.gov>
Subject: CPHA Public Comment
Date: 23.08.2022 19:04:04 (+02:00)
Attachments: CPRA Regulations Comment Letter (ZoomInfo 8.23.22).pdf (5 pages)

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

Please find the attached CPRA Regulation Comment letter from ZoomInfo.

Thank you,

Lindsey

--

Lindsey Stewart (she/her/hers)
Sr. Manager, Privacy & Public Policy

M: [REDACTED]
E: [REDACTED]

805 Broadway Street, Suite 900
Vancouver, WA 98660

zoominfo.com



zoominfo



805 Broadway St, Suite 900
Vancouver, WA 98660

866.904.9666
zoominfo.com

August 23, 2022

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

RE: Draft CPRA Regulations

Dear Members of the California Privacy Protection Agency Board and Staff:

Thank you for the opportunity to submit comments as part of the rulemaking process for the California Privacy Rights Act. ZoomInfo is a software and data intelligence company that provides information for business-to-business sales, marketing, and recruiting. We support consumer privacy rights and are pleased to submit the following comments.

Section 7012(i) (Data Broker Notice)

7012(i) A data broker registered with the Attorney General pursuant to Civil Code section 1798.99.80 et seq., ~~that does not~~ where it collects personal information ~~from a source other than~~ directly from the consumer, does not need to provide a notice at collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out of sale/sharing.

We recommend the foregoing grammatical clarification. As drafted, this section appears to apply only if a registered data broker *never received any* data directly from a consumer, even if it also collects third party data as a registered broker. Of course, a data broker may also have a website that in some instances collects data directly from a consumer, and in those instances, normal notice at collection obligations should apply. This section should apply only *to the extent that* the data broker obtains data from a source other than the consumer.

Section 7012(g)(1) (Third Party Notice at Collection)

7012(g)(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. A single notice at collection should be provided on behalf of all such businesses, and each such business shall be responsible for the compliance of such notice with the CCPA and these regulations.~~

We recommend the foregoing change, because two notices will not help consumers and there is no logical opportunity for two different notices to be provided “at collection.” Whoever controls the point of collection may be acting at the direction of or in concert with another person, so it makes sense for all obligated persons to be responsible. But it is not clear how a second notice would be provided or how that second notice would help consumers.

The confusion is elucidated by the first example provided (Section 7012(g)(4)(A)). If Business G is authorized by Business F to collect data on Business F’s website, the only notice the consumer would see is on Business F’s website. As the example suggests, Business G’s only option would be to post a notice on its homepage, but it is difficult to see (1) how that would constitute a notice at collection or (2) how it would help consumers.

Sections 7012(e)(6) & (g)(2) (Third Parties that Control the Collection of Personal Information)

7012(e) A business shall include the following in its notice at collection:

~~**(e)(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 third parties’ business practices.**~~

7012(g) Third Parties that Control the Collection of Personal Information.

~~**(g)(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.**~~

We recommend deleting Sections 7012(e)(6) and (g)(2). A third party collecting personal information on the first party’s behalf is already subject to the law as a service provider. And to the extent that data is transferred to such parties *other than for the purposes of the first party business*, such transfer would be deemed a sale, share, or disclosure and be subject to additional disclosure requirements and other protections.¹

Requiring such parties to be listed in the notice at collection provides little benefit to the consumer, but risks making the notices needlessly complex. The suggestion in the oddly worded second sentence of 7012(g)(2) (and similar language in 7012(e)(6)) that the business might also describe the business practices of such third parties risks making the notice overwhelming and therefore unhelpful to consumers.

¹ See, e.g., CPRA Section 1798.100(a) and (d) (notice; contracts with transferees); CPRA Section 1798.110(c) (disclosure of categories of transferees); CPRA Section 1798.115(c) (disclosure of categories personal information transferred); CPRA Section 1798.130(5) (disclosure of categories of transferees, categories of personal information transferred); Draft Regulations Section 7026(f)(3) (notice to transferees of opt-outs); Section 7027(g)(4) (notice to transferees regarding sensitive data); Section 7022(b)(2)-(3) (notice to transferees of deletion requests); and Section 7023(c) (notice to transferees of correction requests).

We propose instead that, in the event a business uses one or more service providers to collect data regarding consumers, that it be required to list the categories of such service providers in its notice at collection or privacy policy. In any event, the second sentence of 7012(g)(2) and the language after the semicolon in 7012(e)(6) should be deleted because it is permissive and confusingly suggests that providing the information to the first party is all that is required.

Section 7023(f)(3) (Requests to Correct)

7023(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:

~~(3) — Inform the consumer that, upon the consumer's request, it will note both internally and to any person with whom it discloses, shares, or sells the personal information that the accuracy of the personal information is contested by the consumer. The business does not have to provide this option for requests that are fraudulent or abusive.~~

We recommend deleting Section 7023(f)(3) in its entirety. The additional information, which is here required to be provided to recipients of the data, may have no basis. Requests could be denied because they are obviously incorrect or because the identity of the requester could not be verified. In such cases, it would be unduly burdensome and even harmful to require a business to make changes to the way that it discloses the data. A better approach is to hold businesses accountable to implement reasonable procedures for verifying the identity of requesters and the validity of their requests. Indeed, businesses are already required under Section 7023(b) to consider the totality of the circumstances relating to contested personal information when determining whether the information is more likely than not accurate. Including disclaimers within the data itself is potentially harmful, overly complex, and of little benefit to consumers.

Section 7023(i) (Requests to Correct)

~~7023(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 provide the consumer with the name of the source from which the business received the alleged inaccurate information.~~

We recommend deleting this provision in its entirety. Particularly where data is the result of research, it may be difficult or impossible to identify the source of an error in the information, and it would be unduly burdensome on businesses to trace down any inaccuracy to its ultimate source.

In addition, supplier relationships may be competitively sensitive, and this request could be used to uncover trade secrets and proprietary business processes or other sensitive information. This concern is reflected in Recital 63 of the GDPR, which acknowledges that the right of access to information (including the disclosure of the source(s) of information) "should

not adversely affect the rights or freedoms of others, including trade secrets or intellectual property.” This is evident in situations where the source of the information may need to remain anonymous, such as an individual reporting harassment in the workplace.

Consistent with other provisions of the CPRA and the Draft Regulations, we propose that businesses be required to provide the categories of sources of data and to assume the responsibility to make reasonable determinations as to the accuracy of data upon a consumer’s request. Alternatively, we recommend revising the provision to clarify that businesses are not required to provide the source of allegedly inaccurate information where it may be impossible or impractical to do so, or where the provision of such information would adversely affect the rights or freedoms of others, including trade secrets or intellectual property.

Section 7025(e) (Opt-Out Preference Signals)

[S]ection 1798.135[(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 **subsections (f) and (g) of** 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. **Notwithstanding the foregoing, businesses may take reasonable steps in order to honor such opt-out preference signals regardless of whether such steps constitute processing in a frictionless manner, such as by providing consumers with the option to provide additional information in order for the business to fully effectuate the consumer’s request. 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.**

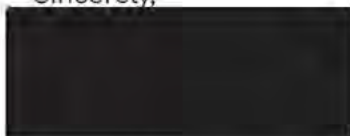
CPRA Section 1798.135(a) says a business must provide “Do Not Sell” links. Section 1798.135(b)(1) says “[a] business shall not be required to comply with subdivision (a) if the business allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal.” Section 1798.135(b)(3) further states “[a] business that complies with subdivision (a) is not required to comply with subdivision (b). *For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b).*” Section 1798.185(20) states that the regulations should be issued “to govern how a business that has *elected to comply* with subdivision (b) of Section 1798.135 responds to the opt-out preference signal.”

By implication, the Draft Regulations provide that a business only processes opt-out preference signals for purposes of 1798.135(a) and (b) if it does so in a “frictionless” manner. However, to be frictionless, a business may not display a pop up in connection with responding to the signal. See 7025(f)(3). Yet, in order to respond to the signal, the business may have a need to request additional information. See 7025(c)(2) (allowing a business to provide consumers with the option to provide additional information to facilitate an opt-out). And furthermore, Section 7025(g) indicates that the opt-out preference signal would need to opt the consumer out of all sale or sharing of their data, even though the business is not able to request additional information to match with existing data sources. Therefore, a business may implement all reasonable protocols to respond to an opt-out preference signal, but still be required to post opt out links, creating potential for duplicate processes and consumer confusion. We see no reason or justification for the Draft Regulations to apply such a limited interpretation of what constitutes honoring an opt-out preference signal.

Without additional verifications being permitted, consumers may believe that by activating an opt-out preference signal, they will be opted out of all of a particular business’s data selling, sharing, or sensitive data processing practices, when that is not the case. In other words, the regulations as currently drafted will force bifurcated processes instead of a consolidated experience for the consumer. In light of the above, we propose that the Draft Regulations be revised to require businesses to either (1) only provide the opt-out links required under the CPRA or (2) process opt-out preference signals and not provide such opt-out links, but to permit businesses to take reasonable steps to honor such signals, which may not meet the definition of “frictionless.”

Thank you for the opportunity to provide public feedback to these important regulations. We welcome additional discussion and appreciate your consideration. Please feel free to contact me if you have any questions.

Sincerely,



General Counsel
ZoomInfo



ZoomInfo (NASDAQ:ZI) is a Go-To-Market Intelligence Solution for more than 15,000 companies worldwide. The ZoomInfo platform empowers business-to-business sales, marketing, and recruiting professionals to hit their number by pairing best-in-class technology with unrivaled data coverage, accuracy, and depth of company and contact information. With integrations embedded into workflows and technology stacks, including the leading CRM, Sales Engagement, Marketing Automation, and Talent Management applications, ZoomInfo drives more predictable, accelerated, and sustainable growth for its customers. ZoomInfo emphasizes GDPR and CCPA compliance. In addition to creating the industry’s first proactive notice program, the company is a registered data broker with the states of California and Vermont. Read about ZoomInfo’s commitment to compliance, privacy, and security. For more information about our leading Go-To-Market Intelligence Solution, and how it helps sales, marketing, and recruiting professionals, please visit www.zoominfo.com.



From: **Cynthia Pantazis** [REDACTED]
To: **Regulations** <Regulations@coppa.ca.gov>
Subject: CPPA Public Comment
Date: 23.08.2022 19:04:15 (+02:00)
Attachments: Google Comments - CPPA proposed regulations implementing CPRA.pdf (21 pages)

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

Attached please find Google's comments on the California Privacy Protection Agency's proposed regulations implementing the California Privacy Rights Act.

Thank you.

--
Cynthia Pantazis
Director, State Policy
Google LLC



August 23, 2022

BY EMAIL

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

Dear Mr. Soublet:

Please find below Google's comments on the California Privacy Protection Agency's ("Agency") proposed regulations implementing the California Privacy Rights Act ("CPRA"). We thank the Agency and the representatives of the California Attorney General's office for what was clearly a significant undertaking. We look forward to the opportunity to comment on these proposed regulations as well as future rulemaking efforts regarding areas not within the scope of the current Notice of Proposed Rulemaking.¹

1. Introduction and General Considerations

In our 2021 CPRA comments,² we offered three priorities for the Agency to consider: (1) focus on providing clarity to businesses around the new obligations established by the CPRA over introducing additional obligations at the start; (2) seek to align the CPRA's requirements with other privacy regimes to facilitate consumer understanding and promote privacy-preserving business practices; and (3) provide flexibility for businesses to respond to consumer requests in a manner that puts substance over form. We appreciate that the proposed regulations reflect these priorities in many areas, including helpful clarifications with respect to definitions, streamlining of prior regulations to avoid repetition, and further clarity regarding verification procedures with respect to consumer rights requests. There are, however, areas that could be further refined and improved. To that end, we offer the following recommendations for the

¹ The Notice of Proposed Rulemaking, dated July 8, 2022, clarifies that rules on cybersecurity audits, risk assessments, and automated decisionmaking technology will be the subject of a future rulemaking and are not within the scope of this Notice of Proposed Rulemaking. See *Notice of Proposed Rulemaking*, Cal. Priv. Prot. Agency, https://coppa.ca.gov/regulations/pdf/20220708_npr.pdf.

² Our prior comments were submitted with respect to the September 22, 2021, Invitation for Preliminary Comments on Proposed Rulemaking Under the CPRA, dated November 8, 2021.

Agency's consideration as it develops final regulations, with more specific comments on particular provisions below.

- *Prioritize preventing consumer harms and promoting privacy-protective business practices over establishing new, prescriptive obligations.*

The CPRA's stated purpose is to "strengthen consumer privacy, while giving attention to the impact on business and innovation."³ This objective is best achieved through standards that allow businesses to deliver on consumer rights, provide required notices, and build privacy and security programs in ways that are tailored to their data collection practices and business models.

In certain places, the proposed regulations instead adopt a prescriptive approach that prioritizes form over substance—an approach that could impede rather than foster consumer privacy. For example, while the "dark patterns" provisions of the CPRA would appropriately ban interfaces that subvert user choice and autonomy, the proposed regulations dictate a specific user interface design, irrespective of whether any consumer is actually confused, much less harmed, by non-conforming designs.⁴ Similarly, the proposed regulations add additional, specific disclosure requirements to include in privacy policies,⁵ notices at collection,⁶ and contracts with service providers,⁷ while providing that even immaterial failures to include these detailed disclosures could lead to substantial fines. For example, including longer, more boilerplate disclosures in privacy policies only increases the burden on users of understanding business practices, and rewards tick-the-box compliance over innovative approaches to communicating complex data practices. We urge the Agency to reconsider its highly prescriptive approach in favor of more flexible rules, or at minimum to make clear that only a *material* failure to abide by the regulations would be considered a violation of the law.

- *Wherever possible, seek to harmonize the CPRA with existing privacy regimes and other state privacy laws to facilitate consumer understanding and encourage development of privacy-protective business practices.*

The CPRA's Findings and Declarations acknowledge that "[t]o the extent it advances consumer privacy and business compliance, the law should be compatible with privacy laws in other jurisdictions."⁸ More can and should be done to harmonize the proposed regulations with existing privacy regimes and with other states' privacy laws, including new omnibus consumer privacy laws in other states that impose substantively identical (while superficially different)

³ CPRA § 3(C)(1).

⁴ Proposed Regulations § 7004(a) (providing numerous prescriptive methods for designing and implementing methods for submitting CCPA requests and obtaining consumer consent, while stating that any method not in compliance therewith may be considered a dark pattern).

⁵ See, e.g., *id.* § 7011.

⁶ See, e.g., *id.* § 7012(f).

⁷ See, e.g., *id.* § 7051.

⁸ CPRA § 3(C)(8).

rights and obligations. Adopting the proposed regulations in their current form would require companies to adopt California-specific notices, contracts, and user choices (while adopting different notices, contracts, and consumer choices to ensure compliance with other state laws). Substantial compliance costs aside, this could serve to confuse rather than assist consumers' understanding of their rights and companies' data practices. Given its unique expertise and institutional foundation, the Agency should be leading the effort across states to develop interoperable rights and obligations. Instead, certain aspects of the proposed rules go further down an incompatible and inefficient path.

- *Ensure that the audit and enforcement provisions help the Agency to punish violators, while also minimizing burden on law-abiding companies.*

The proposed regulations properly seek to ensure that the Agency is able to identify, investigate, and punish those that violate the law, but certain provisions fail to balance the Agency's interest in this regard with law-abiding businesses' need for certainty in running their businesses, and the need for time to build fully compliant programs for addressing the requirements of the law. Most pressing, the Agency should provide businesses with sufficient time to build meaningful compliance programs by clarifying that enforcement of the regulations will begin one year after all CPRA regulations become final.

2. Sec. 7002: Restrictions on the Collection and Use of Personal Information

The CPRA specifically permits processing that is “reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed” or “for another disclosed purpose that is compatible with the context in which the personal information was collected.”⁹ The proposed regulations appear to substantially deviate from this standard, permitting only processing that is “consistent with what an average consumer would expect when the personal information was collected,” or “compatible with what is reasonably expected by the average consumer.”¹⁰

This standard is vague and would be difficult for businesses to implement, as it requires determining the subjective understanding of a consumer. It appears to cast doubt on the legality of processing data for properly disclosed purposes, for example where it is subsequently alleged that the purpose was not expected by an average consumer. That standard is at odds with the text of the law, which clearly permits processing that is “*reasonably* necessary and proportionate” to the business's purpose for collecting the data, or otherwise disclosed and “compatible with the context” of collection. It is also inconsistent with the Fair Information Practice Principles, which for nearly 50 years have acknowledged the role of clear consumer disclosures in determining the scope of permissible information processing.¹¹ Read literally,

⁹ Cal. Civ. Code § 1798.100(c).

¹⁰ Proposed Regulations § 7002(a).

¹¹ See, e.g., *The Fair Information Practice Principles*, Dep't of Homeland Sec., <https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice->

Section 7002(a)'s standard could cast doubt on even core uses of data (i.e., for the purpose of providing and improving a service to a consumer), forcing companies to consider whether such processing would be expected by an "average" consumer (not even limited by the "reasonableness" standard inherent in California consumer protection law).¹² Coupled with the broad audit and investigative powers imposed by the proposed regulations, this language would empower the Agency to audit and/or investigate any uses of personal information it deems not expected by an average consumer—a standard that would presumably be within the Agency's sole purview to determine. And such a standard would risk diverging from other privacy laws in the U.S. and around the world, which focus—like the text of the CPRA—on limiting processing to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer.¹³

Data minimization and purpose limitation are important policy goals. The inquiry into whether processing is "reasonably necessary and proportionate" or "compatible with the context in which the personal information was collected" should be measured by the expectations of "reasonable" consumers, a well-understood notion inherent in California consumer protection law, along with other relevant criteria such as the nature and sensitivity of the data collected, responsible use of that data, disclosures about such uses, and efforts to minimize risk to consumers. For example, an "average" consumer may not understand how data is collected, used, and disclosed to protect them from fraud, identity theft, or phishing schemes. If businesses were limited to using data only for purposes they surmise average consumers would expect, these important consumer protections would effectively be prohibited. Relatedly, Section 7002(b) (and its examples) should emphasize the statutory standard of compatibility of processing purposes,¹⁴ rather than introducing entirely new concepts of "unrelated" or "unexpected" data use, which introduce unnecessary confusion.

At minimum, if the Agency prefers a standard based solely on consumer expectations rather than the criteria described above, the proposed regulations should (1) use well-understood notions of "reasonable" consumers rather than "average" ones, and (2) clarify the important role that consumer-facing notices have in shaping the expectations of reasonable consumers.

principles (last visited Aug. 23, 2022) (specifying that privacy policies should specifically articulate the purpose or purposes for which the personal information is intended to be used); *See also*, The White House, National Strategy for Trusted Identities in Cyberspace, Appendix A—Fair Information Practice Principles,

https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (clarifying that organizations should "specifically articulate the purpose or purposes for which the PII is intended to be used").

¹² For example, in determining whether an act or practice is likely to "mislead" consumers, courts evaluating claims under California's Unfair Competition Law have generally applied the standard of an ordinary consumer acting reasonably under the circumstances. *See, e.g., Lavie v. Procter & Gamble Co.*, 105 Cal. App. 4th 496, 512 & n.8 (2003); *see also, Consumer Advocs. v. Echostar Satellite Corp.*, 113 Cal. App. 4th 1351, 1360 (2003).

¹³ *See* GDPR Art. 5; VA. Code Ann. § 59.1-574.A; Colo. Rev. Stat. § 6-1-1308(3); Connecticut Data Privacy Act ("CTDPA"), S.B. 6, 2022 Gen. Assemb., Reg. Sess. (Conn. 2022) § 6(a).

¹⁴ Cal. Civ. Code § 1798.100(c).

Proposed Amendments:

Sec. 7002: “(a) A business’s collection, use, retention, and/or sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve the purpose(s) for which the personal information was collected or processed, ~~or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.~~ Whether a business’s collection, use, retention, and/or sharing is reasonably necessary and proportionate, or compatible with the context, depends on several factors, including: the expectations of a reasonable consumer when providing their personal information; the nature and sensitivity of the personal information collected; the business’s disclosure of the use, retention, or sharing of personal information at the time it collected the personal information from the consumer; and the business’s efforts to minimize risk to consumers. ~~To be reasonably necessary and proportionate, the business’s collection, use, retention, and/or sharing must be consistent with what an average consumer would expect when the personal information was collected. A business’s collection, use, retention, and/or sharing of a consumer’s personal information may also be for other disclosed purpose(s) if they are compatible with what is reasonably expected by the average consumer.~~ A business shall obtain the consumer’s explicit consent in accordance with section 7004 before collecting, using, retaining, and/or sharing the consumer’s personal information for any purpose that ~~was not disclosed when the personal information was collected or is otherwise unrelated or~~ incompatible with the purpose(s) for which the personal information ~~was~~ collected or processed.”

“(2) Business B provides cloud storage services for consumers. ~~A reasonable~~ ~~An average~~ consumer expects that the purpose for which the personal information is collected is to provide those cloud storage services ~~and other purposes disclosed to the consumer by Business B.~~ Business B may use the personal information uploaded by the consumer to improve the cloud storage services provided to and used by the consumer ~~as well as other disclosed purposes~~ because ~~it is such uses are~~ reasonably necessary and proportionate to achieve the purpose for which the personal information was collected. However, Business B should not use the personal information to research and develop ~~incompatible unrelated or unexpected~~ new products or services, such as a facial recognition service, without the consumer’s explicit consent because such a use is not reasonably necessary, proportionate, or compatible with the purpose of providing cloud storage services. In addition, if a consumer deletes their account with Business B, Business B should not retain files the consumer stored in Business B’s cloud storage service because such retention is not reasonably necessary and proportionate to achieve the purpose of providing cloud storage services.”

With respect to the other examples listed in Sec. 7002(b), replace all references to an “average consumer’s expectations” or a “consumer’s expectations” with a “reasonable consumer’s expectations”; deleting the phrase “unrelated to” or replacing it with “incompatible with,” where applicable; and adding discussion of additional criteria discussed above, i.e., the nature and

sensitivity of the data at issue, responsible use of that data, disclosures about such uses, and efforts to minimize risk to consumers.

3. Sec. 7011(e)(1): Contents of Privacy Policies

The proposed regulations set forth prescriptive requirements for privacy policy disclosures, adding to the already highly specific obligations in the existing CCPA regulations. Rather than introduce new, highly detailed requirements, the Agency should instead provide businesses with guidelines, and some level of discretion and flexibility to communicate with consumers in ways that make sense for them and that match their practices. Such an approach will help, rather than hinder, consumer understanding of privacy policies.

For example, the requirement that privacy policies include a “comprehensive description” of online and offline collection, use, sharing, and retention practices could be understood to contemplate a single privacy policy with exhaustive descriptions of every data point a business collects across its business (even for disparate business lines), how it is collected, exactly how it is shared, and how it is retained even for wholly unrelated services or processing.¹⁵ Similarly, the proposed regulations would require businesses to match every category of personal information they collect with corresponding categories of third parties, and would require companies that do not use or disclose sensitive information in ways that require offering consumers the ability to opt out of such uses to add confusing and potentially lengthy explanations about the ways that they do *not* use such information. These kinds of requirements are likely to hinder rather than aid businesses’ efforts to “specifically and clearly inform consumers” and provide consumers with a “meaningful understanding” of their data practices as required by the law.¹⁶ Instead, they provide incentives for companies to adopt “kitchen sink” approaches to compliance by adopting cookie-cutter and highly legalistic disclosures.

The proposed regulations should instead permit businesses to inform consumers of their data practices through layered and context-appropriate notices. A layered approach to transparency often better facilitates consumer comprehension and control, and can be informed by user testing based on the particular context, rather than a purely legalistic approach. And it enables businesses to better achieve a balance between the provision of sufficient information to ensure transparency while not over-encumbering consumers with excessive detail. For example, Google provides consumers with a control panel¹⁷ that enables them to review the third parties with which they have decided to share data in their Google account, as well as revoke that access. Given that consumers typically direct these data transfers to third parties while using particular services, it would not be possible to provide disclosures about them in advance, in a business’s uniform privacy policy. However, a layered approach to providing this information in

¹⁵ Proposed Regulations § 7011(a).

¹⁶ See CPRA § 3(B)(1)); Proposed Regulations § 7012(e)(1).

¹⁷ *Manage third-party apps & services with access to your account*, Google Account Help, <https://support.google.com/accounts/answer/3466521>.

context can empower consumers with more meaningful and relevant information, and more control over their data.

Proposed Amendments:

Sec. 7011(e): “The privacy policy shall include ~~or facilitate readily available access to~~ the following information:

(1) A ~~comprehensive~~ description of the business’s online and offline practices regarding the collection, use, sale, sharing, and retention of personal information, which includes the following:

- (A) Identification of the categories of personal information the business has collected about consumers in the preceding 12 months. The categories shall be described using the specific terms set forth in Civil Code section 1798.140, subdivisions (v)(1)(A) to (K) and (ae)(1) to (9). To the extent that the business has discretion in its description, the business shall describe the category in a manner that provides consumers a meaningful understanding of the information being collected.
- (B) Identification of the categories of sources from which the personal information is collected.
- (C) Identification of the specific business or commercial purpose for collecting personal information from consumers. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is collected.
- (D) Identification of the categories of personal information, if any, that the business has sold or shared to third parties in the preceding 12 months. If the business has not sold or shared consumers’ personal information in the preceding 12 months, the business shall disclose that fact.
- (E) For each category of personal information identified in subsection (e)(1)(D), Identification of the categories of third parties to whom the information was sold or shared.
- (F) Identification of the specific business or commercial purpose for selling or sharing consumers’ personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is sold or shared.
- (G) A statement regarding whether the business has actual knowledge that it sells or shares the personal information of consumers under 16 years of age.
- (H) Identification of the categories of personal information, if any, that the business has disclosed for a business purpose to third parties in the preceding 12 months. If the business has not disclosed consumers’ personal information to third parties for a business purpose in the preceding 12 months, the business shall disclose that fact.
- ~~(I) For each category of personal information identified in subsection (e)(1)(H), the categories of third parties to whom the information was disclosed.~~

(J) Identification of the specific business or commercial purpose for disclosing the consumer's personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is disclosed.

~~(K) A statement regarding whether or not the business uses or discloses sensitive personal information for purposes other than those specified in section 7027, subsection (I)."~~

4. Sec. 7012(g): Third Party Notice at Collection

As drafted, the proposed regulations are ambiguous as to their expectations for third parties providing notices at collection. Section 7012(g)(1) states that "[b]oth 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."¹⁸ Section (g)(2), however, appears to allow the first party to provide notice of the practices of any third parties collecting personal information on the first party's website or application. The latter interpretation is reinforced in the example provided in Section 7012(g)(4)(A), which contemplates the first party (Business F) providing notice of a third party (Business G).¹⁹ The Agency should make clear that only first parties, not third parties, have an obligation to provide "notice at collection" on their properties, including with respect to the practices of third parties authorized to collect personal information on their properties.

In addition, a strict reading of these provisions could imply that notice from each third party must be pushed directly to users upon arriving on a given website or app. This could inadvertently lead to widespread usage of notice pop-ups and consent management tools like those prevalent in the EU, notwithstanding that there is no indication that either the CPRA or the Agency intends adoption of this aspect of the EU's approach to privacy. Instead, the proposed regulations should make clear that notice at collection can be satisfied by the first party business linking to the appropriate section of the first party's privacy policy that lists third parties,²⁰ rather than through the use of "cookie pop-ups" or similar tools by which third parties may provide notice directly.

Finally, the Agency should clarify that first parties must list or describe *third parties* that collect personal information on their sites or through their services, but need not list or describe *service providers* that collect such personal information. The example listed in Section 7012(g)(4)(A) of an "analytics business" introduces potential confusion in this regard because most analytics providers operate as service providers rather than "third parties" within the meaning of the CCPA. The CCPA, moreover, classifies analytic services as "business purposes" in which service providers (and not third parties) engage. To reduce confusion, we recommend striking the phrase "analytics business" from the example in Section 7012(g)(4)(A) and replacing it with a more typical example of a third party, such as an ad network.

¹⁸ Proposed Regulations § 7012(g)(1) (emphasis added).

¹⁹ *Id.* § 7012(g)(4)(A) (emphasis added).

²⁰ *Id.* § 7012(f).

Proposed Amendments:

Sec. 7012(g): “(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. ~~In that case, 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.”

Sec. 7012(g)(4)(A): “Business F allows Business G, an ~~analytics-business-ad network~~, to collect consumers’ personal information through Business F’s website. Business F may post a conspicuous link to its notice at collection, which ~~notice~~ 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.”

5. Sec. 7022(b)(3), Sec. 7026(f), and Sec. 7052(a): Third Party Pass On Obligations

The proposed regulations also appear to impose substantial obligations on third parties to delete personal information or change their data practices when a business that provided personal information to them informs them of a request that a consumer made to that particular business. For instance, Section 7052(a) would require third parties to comply with requests to delete that are forwarded to them by first parties “in the same manner” as if the request had been made directly to them by the consumer.²¹

These “pass on” obligations for third parties should be more closely aligned with the text of the CPRA, which treats “third parties” as independent businesses with their own compliance obligations, including independent reasons for processing personal information. As noted above, the proposed regulations appear to presume that a deletion request made to one company should result in the deletion of personal information held by wholly independent third parties with separate data practices. That kind of presumption contradicts the independent role of a third party business and ignores that such businesses may, for example, receive personal information from disparate sources and combine that information, often without a way to disambiguate the sources from which it was obtained. Moreover, the proposed regulations overlook the fact that third parties may justifiably rely on exemptions to deletion requests and have verification procedures that are not shared with the business that received the request. Rather than dictate how third parties respond to rights requests forwarded to them by first parties, the regulations should acknowledge that third parties operate as independent

²¹ *Id.* § 7052(a).

businesses and accordingly may act on such requests consistent with their obligations under the CCPA as such.

Proposed Amendments:

Sec. 7052(a): “A third party shall comply with a consumer’s request to delete or request to opt-out of sale/sharing forwarded to them from a business that provided, made available, or authorized the collection of the consumer’s personal information. ~~The third party shall comply with the request~~ in the same way ~~a the business would be is~~ required to comply with the request ~~if made directly by a consumer~~ under sections 7022, subsection (b), and 7026, subsection (f). ~~With respect to requests to opt out of sale/sharing, the~~ third party shall no longer retain, use, or disclose the personal information unless the third party becomes a service provider or contractor that complies with the CCPA and these regulations.”

6. Sec. 7025(b): Technical Specifications for Opt-Out Preference Signals

Section 1798.185(a)(19) of the CCPA mandates that the Agency “issue regulations to define the requirements and technical specifications for an opt-out preference signal sent by a platform, technology, or mechanism, to indicate a consumer’s intent to opt-out of the sale or sharing of the consumer’s personal information and to limit the use or disclosure of the consumer’s sensitive personal information.” The CCPA further specifies topics that these regulations must address, such as how the choice must be presented, including to ensure that the platform that sends such signals does not unfairly disadvantage another business, that the opt-out preference signal is consumer-friendly, clearly represents a consumer’s intent, and does not conflict with other settings.²² This makes sense: to make these opt-out signals actually work for consumers, businesses must have clear direction from the Agency on what signals they must look for and how to process them.

However, the proposed regulations do not address these statutorily-mandated elements, instead deferring to companies to honor any opt-out preference signal that “is in a format commonly used and recognized by businesses” such as “an HTTP header field,”²³ but without any guidance on what is “commonly used,” which businesses must use a format for it to be valid, or how standardization can or should occur. For those that build such signals, the proposed regulations do not address the statute’s requirements, but only specify that the “platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer, whether in its configuration or in disclosures to the public, that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information.”²⁴

²² See Cal. Civ. Code § 1798.185(a)(19).

²³ Proposed Regulations § 7025(b)(1).

²⁴ See *id.*

Without clarity on what signals are valid under the law and how companies are to respond to them at a technical level, the goals of the CPRA with respect to universal opt out choices will not be met. Before requiring businesses to honor opt out preference signals, the Agency should ideally tell businesses *which particular* signals, formats, or tools are valid, by reviewing nominated tools and determining which ones qualify. At minimum, the Agency should state with precision the criteria that make a signal, format, or tool qualify under the law (based on the requirements outlined in the CPRA, including presentation of the choice, disadvantages to businesses, and reflection of consumer intent). Without that certainty, businesses' potential liability for violations of the law will depend on guesswork regarding what signals they should honor, how to look for such signals, and how to honor them. That guesswork, in turn, is certain to frustrate user choice and to create chaos when signals conflict or are incompatible. The approach of the proposed regulations, moreover, is likely to result in the Agency expending substantial resources in fleshing out what signals must be honored and how through post hoc enforcement actions. The better approach, and the approach that is prescribed by the law, is for the Agency to provide that certainty upfront.

The Agency's invocation of HTTP header fields, moreover, is not itself a useful or standard format, and instead demonstrates why opt out signals need standardization to be meaningful. Do Not Track (DNT) was also introduced as an HTTP header field over a decade ago, and similarly aimed at offering users a browser-based mechanism to opt out of some cross-site tracking. But without a common technical and policy framework for honoring such signals, those efforts at first led to a confusing patchwork of responses and later to a complete breakdown of the system intended to offer easier choices to consumers. The Agency is uniquely able to provide what was lacking in the DNT context: the authority to approve a consistent technical and policy framework that all affected businesses can understand and apply.

Proposed Amendments:

Strike Section 7025 of the proposed regulations in its entirety, as well as the associated notice requirements in Section 7011(3)(F) and (G), until the Agency defines the requirements and technical specifications for opt-out preference signals. In the alternative, add a new subsection (h) to Section 7025 that provides:

“(h) The Agency will not enforce this section 7025, nor any provisions of these regulations or the CCPA relating to opt-out preference signals until six months after the Agency has issued final regulations addressing requirements and technical specifications for opt-out preference signals pursuant to section 1798.185(19), Civil Code.”

Sec. 7011(e): “The privacy policy shall include or facilitate readily available access to the following information...

(3) An explanation of how consumers can exercise their CCPA rights and consumers can expect from that process, which includes the following: ...

~~(F) Explanation of how an opt-out preference signal will be processed for the consumer (i.e., whether the signal applies to the device, browser, consumer account, and/or offline sales, and in what circumstances) and how the consumer can use an opt-out preference signal;~~

~~(G) If the business processes opt out preference signals in a frictionless manner, information on how consumers can implement opt out preference signals for the business to process in a frictionless manner;"~~

7. Sec. 7052(c): Third Parties Honoring Technical Opt-Out Signals

Section 7052(c) of the proposed regulations requires third parties that collect personal information from consumers online to honor opt-out preference signals received as a valid request to opt-out of sales.²⁵ These provisions exceed the legal requirements of the CPRA. Under the law, the only obligation to cease selling or sharing personal information in response to an opt-out preference signal lies with the first party business. Section 1798.120 of the CPRA provides that a consumer shall have the right, at any time, “to direct a business *that sells or shares personal information* about the consumer to third parties not to sell or share the consumer’s personal information,” places notice obligations on a “business *that sells consumers’ personal information to, or shares it with, third parties,*” and speaks to the obligations of a business that has received direction from a consumer not to sell or share the consumer’s personal information to cease selling or sharing the consumer’s personal information after its receipt of the consumer’s direction.²⁶

The approach of the proposed regulations, moreover, presents substantial technical and practical implementation challenges that are likely to hinder rather than assist the Agency’s goal of ensuring that opt out preference signals are honored in a clear and consistent manner, particularly because it would require third parties to honor these signals *even if they do not themselves sell or share data*. For instance, signals may conflict, such as where the first party has consent to overcome the signal, but the third party would nevertheless be required to honor it. Similarly, given the Agency’s failure to adopt consistent technical protocols governing opt out preference signals, technical protocols received by the first party and different third parties may not match, resulting in lost signals, duplicate signals, and other confusion. Further, third parties that do not themselves sell or share data would receive opt out signals and have some responsibility under the proposed regulations to act on those signals, but have no means to do so because they do not sell or share data. Finally, the proposed regulations would create an incentive to have data sent to third parties indirectly rather than collected directly from the website or app, in order to avoid the risk of being held liable for failure to honor these signals, undermining consumer transparency generally without any obvious policy advantage.

²⁵ *Id.* § 7052(c).

²⁶ See Cal. Civ. Code § 1798.120(a), (b), (d).

To be clear: third parties will still need to honor user opt outs, as required by their contracts with the websites and apps that sell or share data. But rather than introduce a complex web of compliance challenges, the Agency should honor the CPRA's approach to having the first party (the party that is "selling" or "sharing" data) responsible for passing on the signal based on its own obligations.

Proposed Amendment:

Strike Section 7052(c) in its entirety.

8. Sec. 7051(a)(5): Service Providers' and Contractors' Ability to Combine Personal Information

Section 7051(a)(5) of the proposed regulations appears to prohibit a service provider or contractor from combining personal information received from, or on behalf of, one business with that received from, or on behalf of, another business "unless expressly permitted by the CCPA or these regulations."²⁷ However, neither the CCPA nor the proposed regulations expressly speak to the circumstances under which a service provider or contractor may combine data received from different businesses. As a result, the language of Section 7051(a)(5) casts doubt on service providers' and contractors' ability to combine personal information collected across customers for *any* purpose, including wholly non-controversial purposes such as detecting and preventing fraud. The Agency should strike this reference to combining data, or else modify Section 7051(a)(5) to make clear that that a service provider or contractor may combine or update personal information received from, or on behalf of, the business for the same business purposes for which they may use personal information. Alternatively, the Agency should revise Section 7051(a)(5) to align with the CCPA's definitions of "service provider" and "contractor," clarifying that service providers and contractors may combine data received from, or on behalf of, different clients for "business purposes" as defined by the CCPA, provided that where they are providing advertising and marketing services, they do not do so for cross-context behavioral advertising purposes, nor combine the personal information of opted-out users with other personal information.

Proposed Amendment:

Revise Section 7051(a)(5) to clarify the circumstances under which a service provider or contractor's combination of personal information is permissible, as follows: "The contract required by the CCPA for service providers and contractors shall: [...] Prohibit the service provider or contractor from retaining, using, or disclosing the personal information received from, or on behalf of, the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider or contractor shall be prohibited from combining or

²⁷ Proposed Regulations § 7051(a)(5) (emphasis added).

updating personal information received from, or on behalf of, the business with personal information that it received from another source, ~~provided however that the service provider or contractor may combine personal information to perform any business purpose as defined in Civil Code section 1798.140(e), except, as provided in paragraph (6) thereof, providing advertising and marketing services shall not include cross-context behavioral advertising, and when providing such services, the service provider or contractor shall not combine the personal information of opted-out consumers 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 persons or collects from its own interaction with consumers unless expressly permitted by the CCPA or these regulations.~~

9. Sec. 7051 and 7053: Requirements for Agreements with Third Parties and Service Providers

The proposed regulations would impose numerous substantive requirements for contracts with service providers and third parties. Failure to fully address each of the ten requirements for service provider contracts and six requirements for third party contracts would be deemed material noncompliance, subjecting businesses to substantial penalties even for trivial non-compliance. For example, under Section 7051(c), a business could arguably be deemed to have “sold” personal information to another business without the corresponding notice and opt out even when the disclosure is made pursuant to a contract that provides that the recipient is a service provider to the disclosing business, simply because the contract does not meet every one of the ten elements mandated by subsection (a) of the same section. Similarly, under Section 7053(c), third parties would be prohibited from processing personal information received from a business unless they have a contract with the business that fully meets each of the six requirements set forth in Section 7053(a).²⁸

Such detailed requirements, coupled with draconian consequences for immaterial non-compliance, would needlessly interfere with companies’ practices with little if any corresponding benefit to consumers. For instance, in the case of “selling” or “sharing” personal information to third parties, it makes little sense to require companies to document the precise purposes of such disclosures or permitted uses, as the recipient company typically has the right to use the information it receives in any manner consistent with the law. The obligations for contracts with third parties in particular also go well beyond the requirements for such agreements under other privacy regimes. Even the GDPR, for instance, does not mandate controller-controller agreements, much less the terms of such agreements. Even with that void, companies have executed meaningful controller-controller DPAs suited to their practices. There is no evidence that the GDPR approach is failing in this regard that would justify such a drastic departure. If the Agency nevertheless retains its prescriptive requirements, it should qualify the consequences of non-compliance with a materiality standard to ensure that companies are not punished for trivial violations of such requirements. Finally, the Agency should reconsider its

²⁸ *Id.* § 7053(c).

position that third parties are responsible for implementing contracts with first parties, as the CPRA places the obligations on first parties to ensure that the personal information they provide to third parties is appropriately protected.

Proposed Amendment:

Strike Sections 7051 and 7053 in their entirety, or alternatively edit Sections 7051(c) and 7053(c) as follows:

7051(c): “A person who does not have a contract that complies **in material respects** 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 **in material respects** 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.”

7053(c): “A ~~third-party first party shall not sell or share personal information with a third party unless it has that does not have~~ a contract ~~with the third party~~ that complies **in material respects** with subsection (a) ~~shall not collect, use, process, retain, sell, or share the personal information received from the business.~~”

10. Sec. 7004: Dark Patterns

Google strongly supports the CPRA’s goal of providing consumers with clear, meaningful privacy choices and information, and avoiding user interfaces that subvert or impair consumer autonomy. Based on our experience testing and implementing different modes of communication with consumers across a range of services, as well complying with similar requirements under other legal regimes, we recommend the Agency adopt a less prescriptive approach to “dark patterns” to avoid undermining these sound policy goals and the CPRA’s intent. As proposed, the rules are likely to result in formulaic notices that diminish consumer understanding and lead to notice blindness and information “fatigue.”

In particular, the proposed regulations include more than two-and-a-half pages of detailed and highly specific requirements, leaving little flexibility for businesses to choose how to communicate critical privacy information to their consumers. Rather than mandating another layer of highly detailed rules for communicating with consumers, the Agency should clarify that the examples in the regulations are illustrative and remain subject to the statutory standard, providing businesses with some flexibility to communicate with consumers, so long as they are not misleading and do not subvert user autonomy or choice. A more flexible approach to regulating dark patterns would also be consistent with other legal regimes that govern dark patterns without specifying rigid wording and interface requirements as law.²⁹

²⁹ For example, even the GDPR does not directly legislate dark patterns but rather provides a principled-based approach to determining, for instance, whether consent is valid. The European Data Protection Board has published draft guidance on dark patterns to help guide companies on how to

For example, while the CPRA defines “dark patterns” as a user interface designed to have “the substantial effect of subverting or impairing user autonomy, decision-making, or choice,”³⁰ the proposed regulations provide that any user interface that fails to meet the highly detailed requirements of the proposed regulations “may be considered a dark pattern,”³¹ irrespective of whether the user interface actually has a “substantial effect” of subverting or impairing consumer decision-making. The Agency should make clear that a user interface constitutes a dark pattern only when it has the “substantial effect” required by the law.

Proposed Amendments:

Sec. 7004(b): “A method that does not comply with subsection (a) ~~may~~**shall** be considered a dark pattern **if the method has the substantial effect of subverting or impairing user autonomy, decision-making, or choice**. Any agreement obtained through the use of dark patterns shall not constitute consumer consent. For example, a business that uses dark patterns to obtain consent from a consumer to sell their personal information shall be in the position of never having obtained the consumer’s consent to do so.”

11. Sec. 7304: Agency Audits

The Agency plays a critical role in ensuring compliance with the CCPA, and its authority to conduct audits will assist with that responsibility. As drafted, however, the proposed regulations would compel businesses to undergo announced or unannounced audits without providing sufficient procedures, processes, or other guidance regarding the scope or nature of these audits. For example, the proposed regulations do not define foundational terms like “audit” or explain how “audits” differ from the law enforcement investigations the Agency is also empowered to conduct.

The proposed regulations should provide additional guidance on the scope of the Agency’s “audit” authority and how these audits will be conducted. And in developing this guidance, the Agency’s oversight role should be exercised in a manner that reflects other important policy considerations, including legitimate businesses’ ability to run their operations and receive adequate notice of an audit. Unannounced audits threaten to be non-productive and a poor use of limited Agency resources, because the business will not have time to review requests for material in advance, prepare the requested materials, and identify relevant personnel with information requested. Unlike, for example, an audit of the health conditions of a food

comply with the GDPR in this regard. See *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them*, European Data Prot. Bd., https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en. The Agency, too, should avoid the temptation to regulate user interfaces through inflexible regulations and instead provide more flexible guidance through informal guidance.

³⁰ Cal. Civ. Code § 1798.140(l).

³¹ Proposed Regulations § 7004(b).

manufacturer's factory lines, data protection compliance cannot readily be examined by unannounced visits to a data center. The business will instead need time and preparation to ensure the appropriate records are located and made available. Unannounced audits also unduly threaten confidential, privileged, and private information.

To support the Agency's role in conducting audits to ensure compliance with the law, and to provide businesses with additional guidance and certainty, the regulations should provide reasonable limitations on the circumstances under which the Agency may conduct audits and the processes by which it does so. For example, the Agency should be permitted to conduct audits where the Chief Privacy Auditor finds a reasonable suspicion of an ongoing CCPA violation. Moreover, to distinguish them from law enforcement investigations, audits should be limited to Agency review of existing books, papers, or records, and they should also be limited in time. The proposed regulations should also require the provision of at least 30 days' written notice prior to an audit, unless the Agency has reasonable belief that such notice would lead to the destruction of evidence. And the scope of the audit should be limited to the reasonably suspected CCPA violation described in the notice. These kinds of safeguards would better harmonize the Agency's audit authority with other existing audit regimes.³² They also serve important due process interests by creating reasonable limitations to ensure audits do not exceed the scope of the Agency's powers under the CPRA,³³ and facilitate more efficient audits, thereby helping to conserve Agency resources.

Additionally, to ensure that businesses receive audit notices and have the necessary time to prepare, the proposed regulations should identify the provision of the CCPA that serves as the basis for the audit, and clarify the manner by which these notices must be delivered and to whom they must be addressed. Finally, consistent with CPRA Section 1798.185(a)(18), the proposed regulations should clarify that consumers' personal information shall not be disclosed to an auditor in the absence of a court order, warrant, or subpoena, as well as provide additional protections for business records from disclosure to others outside the audit.

Proposed Amendments:

Sec. 7001: We respectfully request that the Agency add a definition of "Audit" that explains how audits differ from law enforcement investigations that may be conducted by the Agency pursuant to Cal. Civ. Code § 1798.199.45.

³² For example, the Consumer Financial Protection Bureau's ("CFPB") supervisory authority to ensure "covered persons'" compliance with Federal consumer financial law includes safeguards for audits of various "covered persons," such as providing a "Notice of Reasonable Cause" with a description of the basis for asserting such reasonable cause and a summary of the documents, records, or other items relied upon to issue such Notice. See 12 U.S.C. §§ 5514-16 (outlining the procedures and safeguards relating to the CFPB's supervision of "nondepository covered persons," "very large banks, saving associations, and credit unions," and "other banks, savings associations, and credit unions," respectively).

³³ See, e.g., *Fid. & Guar. Life Ins. Co. v. Chiang*, No. 14-CV-01837, 2014 WL 6090559, at *6-7 (E.D. Cal. Nov. 13, 2014) (temporally and geographically unlimited government audits violate due process).

Sec. 7304: “(a) Scope. The Agency may audit a business’s existing books, papers, or records; ~~service provider, contractor, or person~~ to ensure compliance with any provision of the CCPA. The scope of the audit shall be limited to the CCPA provision that the Agency reasonably suspects is being violated, and shall be limited to a time frame reasonably necessary to audit the suspected violation, not to exceed 180 days from the audit’s start date unless otherwise agreed to by the parties.

(b) Criteria for Selection. The Agency may conduct an audit ~~to investigate possible violations of~~ if the Chief Privacy Auditor finds a reasonable suspicion that a business is violating the CCPA. ~~Alternatively, the Agency may conduct an audit if the subject’s collection or processing of personal information presents significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA or any other privacy protection law.~~

(c) Audits must be announced ~~to the business or unannounced as determined~~ by the Agency in writing with thirty days’ notice, unless the Chief Privacy Auditor finds a reasonable belief that such notice would cause the business to destroy the books, papers, or records at issue. Such notice shall identify the provision of the CCPA that serves as the basis for the audit; describe the suspected violation; identify the books, papers, or records the Agency intends to review; and provide the date and time of the audit. Notice shall be delivered by service of process or registered mail with return receipt requested, and shall be deemed made on the date of service; the date the registered mail receipt is signed; or if the registered mail receipt is not signed, the date returned by the post office. The persons to whom such notice shall be addressed shall be the same as the persons upon whom summons may be served under Cal. Civ. Pro. sections 416.10-416.90.

(d) Failure to Cooperate. ~~A subject’s failure to cooperate during the Agency’s audit may result in the Agency issuing a subpoena for the books, papers, or records at issue, seeking a warrant, or otherwise exercising its powers to ensure compliance with the CCPA.~~ The Agency should identify the specific rights the Agency has to ensure cooperation with audits under CPRA and the process by which it will exercise those rights.

(e) Protection of Personal Information / Return or Destruction of Materials at Conclusion of Audit. Consistent with the CPRA, consumers’ personal information shall not be disclosed to an auditor in the absence of a court order, warrant, or subpoena. Consumer personal information disclosed to the Agency during an audit pursuant to a court order, warrant, or subpoena, shall be maintained in compliance with the Information Practices Act of 1977, Civil Code section 1798, et seq. Audits shall be confidential and the Agency shall not disclose materials provided by an audited party without notice to such party. At the conclusion of the audit, the audited party may request the destruction or return of any materials provided by the audited party.”

12. Sec. 7301 - 7303: Enforcement

A. Sec. 7301: Agency-Initiated Investigations

The proposed regulations should also provide additional guidance and limitations on Agency-initiated investigations. While the Agency's expertise, resources, and priorities will be critical in determining when to initiate investigations, the proposed regulations should provide additional certainty for businesses by clarifying that an investigation can be initiated where the Board, by a majority vote, finds reasonable suspicion that a business has violated the CCPA. This will benefit businesses by ensuring that investigations will not be initiated where there is not a reasonable suspicion that a violation occurred. It will also benefit the Agency by conserving resources to focus on instances where a reasonable suspicion of a violation exists, and reducing the potential for claims that investigations are unfounded or an abuse of authority.

Proposed Amendment:

Sec. 7301: "All matters that do not result from a sworn complaint, including Agency-initiated investigations, referrals from government agencies or private organizations, and nonsworn or anonymous complaints, may be opened on the Agency's initiative **where the Board, by a majority vote, finds a reasonable suspicion that a business has violated the CCPA.**"

B. Sec. 7302: Probable Cause Proceedings

The CPRA allows the Agency to initiate probable cause hearings for alleged violations where the alleged violator is served with a notice that provides a summary of the evidence and the alleged violator is informed of their right to be present.³⁴ In order to ensure due process, the Agency should require that the notice contain a clear statement of the claims to be addressed at the probable cause hearing, a summary of the evidence in support of each such claim, and the documents and other evidence on which the Enforcement Division Staff will rely at the proceeding.

Section 7302 also states that probable cause proceedings "may be conducted in whole or in part by telephone or videoconference," where the proceeding is "not open to the public."³⁵ While convenience for the parties and cost minimization are worthy goals, the CPRA explicitly grants alleged violators the "right to be present in person" at probable cause proceedings.³⁶ Thus, the Agency should revise the proposed regulations to clarify that businesses have the right to a live proceeding upon request, even in the case of private proceedings. The Agency should also confirm that unless the alleged violator requests otherwise, information or arguments presented at the probable cause hearing shall not be shared with the public, as is the case for the notice and probable cause determinations.

Additionally, to ensure that businesses receive any probable cause determination made as a result of the proceeding, the proposed regulations should clarify the manner by which probable

³⁴ Cal. Civ. Code § 1798.199.50.

³⁵ Proposed Regulations § 7302(c)(1).

³⁶ Cal. Civ. Code § 1798.199.50.

cause determinations must be delivered and to whom they must be addressed. They should also clarify that the Agency's probable cause determination is only "final" for the purpose of determining that the Agency may hold an administrative hearing to determine whether there has been a violation of the CCPA.

Proposed Amendments:

Sec. 7302: "(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. ~~The persons to whom such notice shall be addressed shall be the same as the persons upon whom summons may be served under Cal. Civ. Pro. sections 416.10-416.90. Such notice shall contain a clear statement of each claim against the alleged violator and a summary of the evidence in support of each such claim as well as the documents and other evidence on which the Enforcement Division Staff will rely at the proceeding.~~

(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, ~~at the election of the alleged violator,~~ may be conducted in whole or in part by telephone or videoconference. . . .

(d) Probable Cause Determination. Agency staff shall issue a written decision with their probable cause determination and serve it on the alleged violator, ~~or their counsel if the alleged violator is represented by counsel, by service of process or registered mail with return receipt requested. electronically or by mail.~~ Notice to the alleged violator shall be deemed made on the date of service; the date the registered mail receipt is signed; or if the registered mail receipt is not signed, the date returned by the post office. The Agency's probable cause determination is final for the purpose of determining that the Agency may hold an administrative hearing to determine whether there has been a violation of the CCPA under Cal. Civ. Code § 1798.199.55 and not subject to appeal. If probable cause is not found, the Agency shall, at the alleged violator's request, destroy or return any materials provided by the alleged violator.

(e) ~~Unless the probable cause proceeding is open to the public at the request of the alleged violator, notices of probable cause, information or arguments presented at the probable cause proceeding by the parties, and probable cause determinations shall not be shared with open to the public. Under no circumstances will such materials be not~~admissible in evidence in any action or special proceeding other than one enforcing the CCPA."

C. Enforcement Date

Particularly if the Agency retains the substantial new obligations in the proposed regulations, enforcement of these rules should provide businesses with sufficient time to build meaningful compliance programs. As drafted, the CPRA contemplates a year between the date the

regulations are finalized and the date enforcement begins.³⁷ Requiring compliance in a more compressed timeline could lead to confusion and inconsistency amongst businesses building these new tools, as well as for consumers faced with potentially shifting notices and privacy choices. In turn, this could undermine the certainty and consistency around privacy practices that the CPRA and regulations are designed to promote. We therefore urge the Agency to start enforcement of the regulations one year after all CPRA regulations become final.

Proposed Amendment:

[New] Section 7305: “Notwithstanding any other law, civil and administrative enforcement of the provisions of law added or amended by these regulations shall not commence until one year after all CPRA regulations become final, and shall only apply to violations occurring on or after the commencement date.”

* * * * *

We appreciate the opportunity to provide comments on the proposed regulations.

Sincerely,



Cynthia Pantazis
Director, State Policy

³⁷ See Cal. Civ. Code § 1798.185(d) (stating “the timeline for adopting final regulations required by the Act adding this subdivision shall be July 1, 2022” and “civil and administrative enforcement of the provisions of law added or amended by this Act shall not commence until July 1, 2023, and shall only apply to violations occurring on or after that date”).