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_FTCDataMinimization_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_FTCDataMinimization_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 CPPA 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 consen~~t 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 businesss'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 op-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 (l). ~~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 (l).~~ 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 (l). 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.