epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

Nov 20, 2022

California Privacy Protection Agency
2101 Arena Blvd
info@cppa.ca.gov

Re: CPPA rulemaking

Dear Chairperson Urban and Board Members de la Torre, Le, Mactaggart, and Thompson,

The Electronic Privacy Information Center (EPIC) writes to submit recommendations to the California Privacy Protection Agency (CPPA) published regulations on November 3, 2022. EPIC is a public interest research center in Washington, D.C. EPIC 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. EPIC supports the establishment of strong privacy rules to protect consumers from invasive commercial surveillance practices. EPIC has previously provided comments on the CCPA[1] and published a detailed analysis of the California Privacy Rights Act (CPRA) before its approval by California voters.[2]

In Fall 2021, EPIC and three peer organizations urged the CPPA to implement strong, privacy-protective regulations under the state's new data protection law. Specifically EPIC, Consumer Action, the Consumer Federation of America, and New America's Open Technology Institute urged the agency "to continue 'protect[ing] consumers' rights' and 'strengthening consumer privacy' at every opportunity, consistent with the expressed will of California voters." Specifically, we encouraged the agency "to impose rigorous risk assessment obligations on businesses whose data processing activities could reasonably harm individuals' privacy or security; to maximize the transparency of automated decision-making systems and minimize the burdens on individuals who wish to opt out of such systems; and to prevent any exceptions to user-directed limits on the use and disclosure of sensitive personal information from swallowing the rule." In June 2022, EPIC and five peer organizations urged the agency to promulgate strong rules regarding the use of Universal Opt-Out Mechanisms.[3] In August 2022, EPIC, along with the California Public Interest Research Group Education Fund, Center for Digital Democracy, Consumer Action, the Consumer Federation of America, Ranking Digital Rights, and the U.S. Public Interest Research Group, sent comments to the

[1] Comments of EPIC to Cal. Office of the 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.
[2] EPIC, *California's Proposition 24* (2020), https://epic.org/californias-proposition-24/.
[3] EPIC, *Six Consumer Protection Groups to CPPA: Global Opt-Outs Are Essential to Protect Consumers and Mandatory for Businesses Under the CPRA* (June 8, 2022) https://epic.org/epic-coalition-commend-cppa-for-affirming-obligation-for-global-opt-out-signal/

agency regarding proposed regulations under the California Consumer Privacy Act.[4] We focused in particular on the need to strengthen the substantive restrictions on expansive and exploitative data collection in the online ecosystem. We stressed that "Californians' most urgent need is not for more notices about their rights; it is for substantive, meaningful limitations on the use and disclosure of their sensitive personal information."

In this letter, EPIC will provide further responses and recommendations to the proposed regulations in sections 7002, 7004, 7011, 7012, 7022, 7023, 7027, 7050, and 7052. Specifically, we believe that the agency should modify these proposed regulations to:

- Further clarify and strengthen the data minimization rules.
- Clarify that businesses providing services to nonbusiness are still subject to the regulations, and further specifying contractor obligations.
- Restore the deleted examples about symmetry of choice and manipulative choice architecture in the consumer consent section.
- Avoid ambiguity in methods for calculating the value of consumer data.
- Ensure that businesses disclose all purposes for using sensitive personal information.
- Require that Notice at Collection of personal information should include an initial, short-form notice.
- Make clear that consumer requests to delete or correct data will be passed through to and honored by third parties.
- Expressly restrict the collection and processing of sensitive data beyond strictly necessary and enumerated purposes.

Throughout this comment, EPIC provides suggested edits to revised proposed regulatory text in *italics* and ~~strikethrough~~.

EPIC recommends the agency further refine the data minimization rule in §7002 to avoid ambiguity and make clear that consent is not an adequate independent basis to collect and process data.

In our comments on the initial draft regulations, we urged the agency to prohibit businesses from processing personal information in ways that are incompatible with the reasonable expectations of consumers and with the context in which the data was collected. EPIC commends the CPPA for modifying the proposed rules in §7002 to strengthen these restrictions. However, we are concerned that certain provisions in the revised proposed regulations could be ambiguous or confusing. We are also concerned that under the proposed regulations consent would still act as an independent basis to collect and process data, rather than being one of many factors to consider.

We believe that §7002 of the regulations could be clarified and strengthened in the following ways:

[4] Comments of EPIC et. Al to Cal. Priv. Protec. Agency (Aug. 23, 2020) available at https://epic.org/documents/epic-comments-cppa-aug2022/

- Revise the second subparagraph of §7002(c) to simplify the clause and make the meaning clear. The purpose of the subparagraph appears to be that the other disclosed purpose should be compared with the list of business purposes in §1798.140(e) and that being within that scope of one of those enumerated purposes weighs in favor of compatibility.
- Delete the third subparagraph in §7002(c) and move the example up to the second paragraph. It is not clear what the agency means by the "strength of the link between subsection(c)(1) and subsection (c)(2)." The preamble in subsection (c) already states that the standard is whether the other disclosed purpose is "compatible with the context" based on the two factors in (c)(1) and (c)(2), so the current third subsection is not necessary. And the example should illustrate how the
- Move §7002(e) into a new subparagraph (3) of §7002(c). The consent provision in E should not be an independent basis for which to collect or process data, but it should be considered as a factor in evaluating the compatibility of another disclosed purpose. The act of obtaining the consumer's consent under section 7004 will necessarily involve disclosing the new purpose, and consent can therefore be factored into the compatibility analysis under §7002(c).
- Revise §7002(d) to simplify the preamble and make it clear that the subparagraphs are factors that businesses should evaluate to determine whether their purposes are necessary and proportionate. As currently written the preamble and subparagraphs are difficult to parse and do not provide a sufficiently clear instruction of how to evaluate the factors.

EPIC recommends that §7002 be revised as follows:

> § 7002. Restrictions on the Collection and Use of Personal Information
>
> * * *
>
> (c) Whether another disclosed purpose is compatible with the context in which the personal information was collected shall be based on the following:
>
> (1) At the time of collection of the personal information, the reasonable expectations of the consumer(s) whose personal information is collected or processed concerning the purpose for which their personal information will be collected or processed, based on the factors set forth in subsection (b) *For example, when a consumer uses a map app, the app may collect and use her personal information, including her location data, to optimize the best route to her destination and may retain that information for the limited purpose of suggesting that destination to the consumer again. These purposes are sufficiently within consumer expectation for the original purpose of the data collection and the secondary uses.*
>
> (2) The other disclosed purpose for which the business seeks to further collect or process the consumer's personal information, including whether it is a Business Purpose listed in Civil Code section 1798.140, subdivisions (e)(1) through (e)(8). *For example, when a consumer expects that their personal information is used to provide them with a requested service at the time of collection, the later use of that information to repair errors that impair the intended functionality of that requested service would be*

compatible. By contrast, for example, a consumer whose personal information is provided to a requested cloud storage service at the time of collection may not expect that their personal information will later be used to research and develop a facial recognition service.

(3) ~~The strength of the link between subsection (c)(1) and subsection (c)(2)~~. *Whether a business has obtained the consumer's consent in accordance with section 7004 before collecting or processing personal information for any purpose that does not meet the requirements set forth in subsection (a).*

~~For example, a strong link exists between the consumer's expectations that the personal information will be *provided to a company for* with a requested service at the time of collection, and the use of the information to repair errors that impair the intended functionality of that requested service are sufficiently related to a consumer's reasonable expectation when. This would weigh in favor of compatibility. By contrast, for example, a weak link exists between the c onsumer's reasonable expectations that the personal information will be collected to provide a requested cloud storage service at the time of collection, and the use of the information to research and develop an unrelated facial recognition service.~~

(d) ~~For each purpose identified in subsection (a)(1) or (a)(2), the collection, use, retention,~~
~~and/or sharing of a consumer's personal information to achieve that purpose shall be reasonably necessary and proportionate. The business's collection, use, retention, and/or sharing of a consumer's personal information shall also be reasonably necessary and proportionate to achieve any purpose for which the business obtains the consumer's consent~~
~~in compliance with subsection (e).~~ Whether a business's collection, use, retention, and/or sharing of a consumer's personal information is reasonably necessary and proportionate to
achieve the purpose identified in subsection (a)(1) or (a)(2~~), or any purpose for which the business obtains consent,~~ shall be based on the following:

(1) The minimum personal information that is necessary to achieve the purpose identified in subsection (a)(1) or (a)(2)~~, or any purpose for which the business obtains consent~~. For example, to complete an online purchase and send an email confirmation of the purchase to the consumer, an online retailer may need the consumer's order information, payment and shipping information, and email address.

(2) The possible negative impacts on consumers posed by the business's collection or processing of the personal information. For example, a possible negative impact of collecting precise geolocation information is that it may reveal other sensitive personal information about the consumer, such as health information based on visits to

healthcare providers.

(3) The existence of additional safeguards for the personal information to specifically address the possible negative impacts on consumers considered by the business in subsection (d)(2). For example, a business may ~~consider~~ *use* encryption or automatic deletion of personal information within a specific window of time as potential safeguards

~~(c) A business shall obtain the consumer's consent in accordance with section 7004 before collecting or processing personal information for any purpose that does not meet the requirement set forth in subsection (a).~~

***

EPIC recommends the agency to restore the examples in §7004 that clarify specific categories of harmful choice architecture.

The agency in its revisions to the proposed regulations has removed several examples that provide helpful guidance on harmful choice architecture. For example, the illustrative in 7004(a)(4)(A) that described user interface phrasing designed to shame a consumer into making a choice that benefits the company and discourages exercise of consumer rights had provided useful clarification.[5] Similarly, the two examples related to "symmetry in choice" in subsections 7004(a)(2)(E) and (F) were useful examples of improperly manipulative presentation of choices that would encourage consumers to click yes or pass through without making a meaningful choice. EPIC urges the CPPA to keep these original examples.

EPIC recommends the agency not permit too much variation in business' calculation of the value of consumer data in §7081.

EPIC is concerned about how the revised draft regulations permit businesses to use indeterminate and untested methods to calculate the value of consumer data in the good-faith provision. The use of this provision is likely to lead to businesses' significantly undervaluing consumer data or valuing some consumers' data more than others. We would recommend deleting clause (8) from § 7081(a), and the CPPA adjust it to reflect the following:

§ 7081. Calculating the Value of Consumer Data

(a) A business offering a financial incentive or price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer's data. The business shall consider one or more of the following:

[5] "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.

(1) The marginal value to the business of the sale, collection, or deletion of a consumer's data.
(2) The average value to the business of the sale, collection, or deletion of a consumer's data.
(3) The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers.
(4) Revenue generated by the business from sale, collection, or retention of consumers' personal information.
(5) Expenses related to the sale, collection, or retention of consumers' personal information.
(6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference.
(7) Profit generated by the business from sale, collection, or retention of consumers' personal information.
~~*(8) Any other practical and reasonably reliable method of calculation used in good faith.*~~

EPIC recommends the agency explicitly require in §7011 that businesses disclose all purposes for using sensitive personal information.

The proposed regulations rely in many cases on the representations of businesses regarding the purpose and means of their collection of personal information. The contents of the privacy policies posted by businesses are an important mechanism by which to evaluate the businesses claims about their data practices and to ensure that consumers are adequately protected. The agency should add specific provisions to the "Information Practices" section of the privacy policy requirements to ensure that the sensitive personal information protections are operationalizable and to ensure that consumers do not lose out when businesses make material changes to their policies. We recommend that the following two subparagraphs be added to subsection 7011(e)(1):

§7011. Privacy Policy.

***

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

(1) A comprehensive description of the business's online and offline Information Practices, 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 description shall be sufficient for a reasonably individual to understand the material effect of each material change.

EPIC recommends that notice at collection of personal information should include an initial, short-form notice in §7012.

While EPIC commends the agency for its work to refine the guidance for initial collection notices, we recommends that the agency include a requirement for short-form notice in certain circumstances. Consumers interact with so many businesses every day that they cannot meaningfully review even clear terms included in longer form notices. The most effective way to communicate an overview of individual rights and disclosures required for Notice and Collection at the initial stage is, in many cases, through a short-form notice. We recommend that the agency add a new subsection on short-form notice at the end of section 7012 as follows:

§7012 Notice at Collection of Personal Information

***

(j) 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.

EPIC recommends the agency make clear in §§7022-7023 that consumer requests to delete or correct data will be passed through to and honored by third parties.

The regulations governing consumer requests to delete or correct their data need to make clear that businesses are obliged to pass such requests through to third parties as appropriate and that such third parties are required to comply. We believe that the following modifications to sections 7022 and 7023 are necessary to ensure that these notifications and obligations flow to third parties.

§7022. Requests to Delete.

***

(c) A *business*, service provider, contractor, *or third party* shall, with respect to personal information that they collected pursuant to their written contract with the business and upon notification by the business, cooperate with the business in responding to a request to delete by:

(d) If a business, service provider, contractor, *or third party* stores any personal information on archived or backup systems, it may delay com 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, *contractors, or 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. The business shall also instruct all service providers and contractors that maintain the personal information at issue pursuant to their written contract with the business to make 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 corrections. If a business, service provider, or contractor stores any personal information that is the subject of the request to correct on archived or backup systems, it may delay compliance with the consumer's request to collect, with respect to data stored in 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. *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. For example, if Business N has sold or shared personal information to a third party and Business N later receives a request to correct from a consumer. Business N complies and corrects the personal information in its system and notifies the third party of the correction.*

EPIC recommends the agency add an explicit and affirmative limitation of disclosure of sensitive data in §7027.

Excessive data collection and retention can be particularly harmful when it includes sensitive personal information. As EPIC explained in its comments on the initial draft regulations, "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."[6] Therefore, the right to limit should not be the only rule specifically restricting the collection, processing, and sale of sensitive personal information. The rules for handling sensitive personal information should be more restrictive than those for non-sensitive information, and the structure of the CPPA as amended supports this construction. We recommend that the Agency promulgate rules that substantively restrict the permissible purposes for using sensitive data to read as follows:

> §7027 ~~Requests to Limit~~ *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 (m).* The purpose of the *prohibition against the use and disclosure of sensitive personal information is to protect how consumers'* ~~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*s* 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 (m). *The consumer should 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 (m).* Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to ~~requests to limit~~ *the prohibition*.
>
> ***
>
> (m) *The exceptions for which a business may use or disclose sensitive personal information are as follows.* The purposes identified in Civil Code section 1798.121, subdivision (a), 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, provided that the use or disclosure *is necessary to perform the services or provide the goods reasonably expected by an average consumers who requests those goods or services,* reasonably necessary and proportionate to

[6] Comments of EPIC et. Al to Cal. Priv. Protec. Agency (Aug. 23, 2020) available at https://epic.org/documents/epic-comments-cppa-aug2022/

for those purposes, is not required to post a Notice of Right to Limit or provide a method for submitting a request to limit.

(1) To perform the services or provide the goods reasonably expected by an average consumer who requests those good or services *to the consumer 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.

***

(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~~ *locate the victim of an* alleged kidnapping *to prevent death or serious physical injury*.

***

(7) To verify or maintain the quality or safety of a product, 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 for the purpose of testing *insofar as it is reasonably necessary to test* that its internal text recognition software accurately captures license information in car rental transactions.

EPIC supports the clarification in §7050 that businesses providing services to nonbusiness are still subject to the regulations, and recommends further specifying contractor obligations in §7052.

EPIC commends and supports the CPPA clarifying that businesses providing services to nonbusinesses are *not* exempt from requirements under the regulations, as articulated in the revised proposed text of subsection 7050(g).

We recommend that section 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. EPIC recommends the regulation be adjusted to the following:

§ 7052 Third Parties

***

(b) A third party shall comply with the terms of the contract required by the CCPA and these regulations, which include treating the personal information that the business made available to it in a manner consistent with the business's obligations under the CCPA and these regulations, *including deletion and opt-out request from consumers*.

Conclusion

The agency's proposed regulations would establish important protections for Californians and EPIC supports their promulgation. Our recommendations above are intended to ensure that the agency's regulations establish clear and strong rules that can help to limit the spread of invasive commercial surveillance practices in California.

x *Alan Butler*
Alan Butler
EPIC Executive Director

x *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Deputy Director

x *John Davisson*
John Davisson
EPIC Litigation Director

x *Ben Winters*
Ben Winters
EPIC Counsel

X *Sara Geoghegan*
Sara Geoghegan
EPIC Counsel

x *Suzanne Bernstein*
Suzanne Bernstein
EPIC Law Fellow