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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

CALIFORNIA OFFICE OF THE ATTORNEY GENERAL

NOTICE OF PROPOSED RULEMAKING

THE CALIFORNIA CONSUMER PRIVACY ACT

February 25, 2020

The Electronic Privacy Information Center ("EPIC") submits these comments in response to the Notice of Modifications[1] on the California Consumer Privacy Act (CCPA). EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC has long supported the establishment of comprehensive federal privacy law and also argued that federal law should not preempt stronger state laws.[3] EPIC has also previously provided comments on the CCPA.[4]

The proposed regulations make clear that the OAG intends to establish strong data privacy protections in the CCPA for Californians. EPIC supports the efforts of the Attorney General. EPIC submits these comments to further safeguard the privacy of California consumers.

---

[1] California Dept. of Justice, Updated Notice of Modifications to Text of Proposed Regulations and Addition of Documents and Information to Rulemaking File, Title 11 (Feb. 10, 2020), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-mod-020720.pdf.

[2] *About EPIC,* EPIC (2020), https://epic.org/epic/about.html.

[3] EPIC, *Grading on a Curve: Privacy Legislation in the 116th Congress* (Dec. 2016) https://epic.org/GradingOnACurve; Testimony of EPIC Exec. Dir. Marc Rotenberg on *Privacy in the Commercia World*, before the House. Subcomm. on Comm. Trade, and Cons. Protection, Comm. on Energy and Comm., 107th Cong., 1st Sess. ___ (Mar. 1, 2001), https://epic.org/privacy/testimony_0301.html

[4] Comments of EPIC to the California Office of the Attorney General, Notice of Proposed Rulemaking, the California Consumer Privacy Act (Dec. 6, 2019), https://epic.org/apa/comments/EPIC-CCPA-Dec2019.pdf . *See also EPIC Backs Strong Implementation of California Privacy Law* (Dec. 6, 2019), https://epic.org/news/2019/default.html

Section § 999.301 Definitions

The draft proposes to add the following text to the definitions of "categories of sources" and "categories of third parties:"

> (d) "Categories of sources" means types or groupings of persons or of entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity. They may include ~~including but not limited to~~ the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers ~~from which public records are obtained, and consumer data resellers.~~
>
> (e) "Categories of third parties" means types or groupings of third parties with whom the business shares ~~of entities that do not collect~~ personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party. They may include ~~directly from consumers, including but not limited to~~ advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and ~~consumer~~ data brokers ~~resellers~~.

EPIC supports these changes. The clarifications will help consumers understand who is collecting, processing and receiving their personal information. However, actual transparency requires that consumers have specific knowledge of which third parties have access to their data and the reason for the access. EPIC encourages the OAG to consider future changes that will allow consumers to know precisely who has obtained their data and for what purpose.

The draft proposes adding the following language to the definition of "Price or Service Difference":

> (l) "Price or service difference" means (1) any difference in the price or rate charged for any goods or services to any consumer related to the disclosure, deletion, or sale of personal information, including through the use of discounts, financial payments, or other benefits or penalties; or (2) any difference in the level or quality of any goods or services offered to any consumer related to the disclosure, deletion, or sale of personal information, including the denial of goods or services to the consumer.

However, under the CCPA, a business is currently not allowed to charge a consumer for disclosing their personal information.[5] Therefore, EPIC recommends the following change deleting "disclosure" from this definition.

> (l) "Price or service difference" means (1) any difference in the price or rate charged for any goods or services to any consumer related to the ~~disclosure~~, deletion~~,~~ or sale of personal information, including through the use of discounts, financial payments, or other benefits or penalties; or (2) any difference in the level or quality of any goods or services offered to any consumer related to the ~~disclosure~~, deletion~~,~~ or sale of personal information, including the denial of goods or services to the consumer.

Section § 999.302. Guidance Regarding the Interpretation of CCPA Definitions

The draft proposes to add the following text:

> (a) Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household." For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be "personal information."

EPIC recommends revising the example in the guidance as IP addresses are explicitly referenced in the definition of personal information in the CCPA[6]. As currently drafted, the provision allows companies to collect and retain IP information about users that could in fact be

---

[5] 1798.100(d) states: *A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section.*

[6] *1798.140**(o)(1)** states (Emphasis added): "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:* ***(A)*** *Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier,* ***internet protocol address****, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.*

made personally identifiable. That is clearly not the intent of the provision and the example should be revised.

Therefore, EPIC favors this addition with the following clarification:

> (a) Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household." For example, even if a business that collects the IP addresses of visitors to its website and does not link the IP address to any particular consumer or household, ~~and any party not reasonably link the IP address with a particular consumer or household, then~~ the IP address would ~~not~~ still be "personal information." 1798.140(o)(1)(A).

Section § 999.304. Overview of Required Notices

The draft regulations propose adding the following language:

> a) Every business that must comply with the CCPA and these regulations shall provide a privacy policy in accordance with the CCPA and these regulations, including section 999.308.
>
> (b) A business that collects personal information from a consumer shall provide a notice at collection in accordance with the CCPA and these regulations, including section 999.305.
>
> (c) A business that sells personal information shall provide a notice of right to opt-out in in accordance with the CCPA and these regulations, including section 999.306.
>
> d) A business that offers a financial incentive or price or service difference shall provide a notice of financial incentive in accordance with the CCPA and these regulations, including section 999.307.

EPIC appreciates the "Overview of the Required Notices" and recommends that it is included in the final rules. The overview gives businesses clear guidance of what is required if they are a business as defined by the CCPA. However, we caution that while these notices provide effective mechanism for privacy enforcement, they typically place unfair unburdens on consumers. There is also a risk that privacy notices might operate as waivers or disclaimers, depriving consumers of rights to which they would otherwise be entitled,

Section § 999.305 Notice at Collection of Personal Information

The draft regulations propose adding the following changes:

> *(*3)(a) When a business collects consumers' personal information online, it may ~~conspicuously~~ post a conspicuous link to the notice on the introductory page of the business's ~~website homepage or the mobile application's download page, or~~ and on all webpages where personal information is collected.

EPIC appreciates the guidance for businesses about when they have to post a "conspicuous link." In fact, EPIC led a coalition of California consumer organizations in 2008 to enforce the conspicuous link provision of the California Online Privacy Protection Act of 2003 against Google when the company refused to make a link to its privacy policy accessible from its homepage.[7] We therefore recommend that the substitution of the word "must" for "may" so that the provision would read:

> *(*3)(a) When a business collects consumers' personal information online, it ~~may~~ must ~~conspicuously~~ post a conspicuous link to the notice on the introductory page of the business's ~~website homepage or the mobile application's download page, or~~ and on all webpages where personal information is collected.

We also recommend that the drafters clearly define the term "Conspicuous Link." EPIC suggests adding the following language:

> A Conspicuous Link is a hypertext link that is written in capital letters equal to or greater in size than the surrounding text; is displayed in a type, font or color that contrasts with the surrounding text of the same size; or is otherwise distinguishable from surrounding text on the homepage.[8]

---

[7] Letter from Privacy Organizations to Google CEO Eric Schmidt, June 3, 2008 ("We are writing to you on behalf of California consumers and Internet users around the world to urge Google to include a direct link to its privacy policy on its homepage."), https://epic.org/privacy/ftc/google/Google_Letter060308.pdf. *See also,* Jaikumar Vijayan, *Google Asked to Add Link to Privacy Policies,* Computerworld, June 3, 2008, https://archive.nytimes.com/www.nytimes.com/idg/IDG_852573C4006938800025745D006675FE.html ("Rotenberg called Google's stance 'very bizarre' and said it appears to put the company in violation of California's Online Privacy Protection Act of 2003. One of the provisions in the act calls for companies to incorporate a prominent link to their corporate privacy on their home pages.") Saul Hansell, *Is Google Violating a California Privacy Law?* N.Y. Times, May 30, 2008, https://bits.blogs.nytimes.com/2008/05/30/is-google-violating-a-california-privacy-law/. Eventually, we prevailed. EPIC, *Google Adds Link to Privacy Policy*, July 7, 2008.

[8] This definition of "conspicuously posts" borrows from current California Law, the California Online Privacy Protection Act of 2003 (CalOPPA). This is the definition in CalOPPA: (*b) The term "conspicuously post" with respect to a privacy policy shall include posting the privacy policy through any of the following:*

The draft regulations propose the addition of the following language:

> (*4) When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a just-in-time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection. For example, if the business offers a flashlight application and the application collects geolocation information, the business shall provide a just-in-time notice, such as through a pop-up window when the consumer opens the application, which contains the information required by this subsection.*

EPIC supports the new clarifications around special just-in-time notice requirements for businesses that collect personal information that consumers may not expect. The drafter's example of the flashlight app gained national attention[9] and it would be helpful for consumers to know if other apps are following similar practices.

Section § 999.306 Notice of Right to Opt-Out of Sale of Personal Information

The draft regulations propose adding the following language:

---

(1) A Web page on which the actual privacy policy is posted if the Web page is the homepage or first significant page after entering the Web site.
(2) An icon that hyperlinks to a Web page on which the actual privacy policy is posted, if the icon is located on the homepage or the first significant page after entering the Web site, and if the icon contains the word "privacy." The icon shall also use a color that contrasts with the background color of the Web page or is otherwise distinguishable.
(3) A text link that hyperlinks to a Web page on which the actual privacy policy is posted, if the text link is located on the homepage or first significant page after entering the Web site, and if the text link does one of the following: (A) Includes the word "privacy."
(B) Is written in capital letters equal to or greater in size than the surrounding text.
(C) Is written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size or set off from the surrounding text of the same size by symbols or other marks that call attention to the language.
(4) Any other functional hyperlink that is so displayed that a reasonable person would notice it.
(5) In the case of an online service, any other reasonably accessible means of making the privacy policy available for consumers of the online service.
https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.&lawCode=BPC

[9] Cecilia Kang, *Flashlight app kept users in the dark about sharing location data: FTC*, Wash. Post (Dec. 5, 2013), https://www.washingtonpost.com/business/technology/flashlight-app-kept-users-in-the-dark-about-sharing-location-data-ftc/2013/12/05/1be26fa6-5dc7-11e3-be07-006c776266ed_story.html

(e) A business shall not sell the personal information it collected during the time the business did not have a notice of right to opt-out notice posted unless it obtains the affirmative authorization of the consumer.

EPIC appreciates the clarification that if a business changes their privacy policy to state that they in fact do collect personal information, that business is prohibited from selling personal information it previously collected unless it subsequently obtains opt-in consent from the consumer.

Section § 999.312 Methods for Submitting Requests to Know and Requests to Delete

The draft regulations propose adding the following language:

(a) A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to know

EPIC recommends that all businesses that collect personal data about consumers must provide at least two methods of contact whether or not they have a direct relationship with consumers. Many businesses, including the major social media companies, collect personal information about consumers with whom they do not have a direct relationship. It is important that those consumers can also easily contact these businesses to access their personal information.

Therefore, EPIC recommends striking the following from §999.312(a):

~~A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to know.~~

Section § 999.313 Responding to Requests to Know and Requests to Delete

The draft regulations propose adding the following language:

(a) Upon receiving a request to know or a request to delete, a business shall confirm receipt of the request within 10 business days and provide information about how the business will process the request.

(b) Businesses shall respond to requests to know and requests to delete within 45 calendar days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request.

EPIC supports the clarification. It is an important that the right to know process does not take an excessive period of time. We recommend these changes should be codified in the final regulations.

The draft proposes the following additions:

(3) In responding to a request to know, a business is not required to search for personal information if all the following conditions are met:

(a) The business does not maintain the personal information in a searchable or reasonably accessible format;
(b) The business maintains the personal information solely for legal or compliance purposes;
(c) The business does not sell the personal information and does not use it for any commercial purpose; and
(d) The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.

EPIC opposes this proposed addition. While EPIC respects the effort of the drafters to narrow the exception and to create multiple requirements, this addition is problematic. For example, telephone companies are required by the FCC to retain call detail records on their customers.[10] That data is not searchable, it is maintained for compliance purposes, and is not sold to third parties. Even if telephone customers in California were told of this business practices, they would not have the right to obtain their personal data held by the telephone company. The provision should be removed.

The draft regulations propose adding the following language:

(4) A business shall not at any time disclose in response to a request to know a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics.

[10] https://www.fcc.gov/tags/record-retention

EPIC recognizes that if a business collects certain categories of sensitive personal information disclosure to a consumer of the actual information could create some privacy risks. However, whether or not it is possible to make the disclosure without risk, a consumer should still know that a business collects these types of information. Therefore, we advise that the regulations add the following language:

> A business that collects such information shall disclose to the consumer which particular types of information the business has collected. For example, if a business collects a social security number it shall disclose that fact to the consumer without disclosing the specific social security number.

The draft regulations propose adding the following language:

> (d)(1) If the business sells personal information and the consumer has not already made a request to opt out, the business shall ask the consumer if they would like to opt out of the sale of their personal information and shall include either the contents of, or a link to, the notice of right to opt-out in accordance with section 999.306.

EPIC supports the change eliminating the requirement that if a business cannot delete a consumer's personal information it should treat that deletion request as an opt-out. It is important to note that the right to opt-out of the sale of personal information is different from the right to delete personal information and some consumers may not want to opt-out of the sale of personal information especially if the business offers different financial incentives to consumers who do not opt-out of the sale of their personal information. EPIC supports this addition.

Section § 999.314 Service Providers

The draft regulations propose adding the following "permissible use":

> (3) For internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles, or cleaning or augmenting data acquired from another source;

EPIC is opposed to this addition and recommends striking this language. EPIC believes that this is a loophole for service providers to use personal information in ways other than to provide the service requested by the consumer. The CCPA is clear that if personal information is disclosed to service

providers to perform a business purpose, the service provider can only use that personal information for that purpose[11] and is contractually prohibited from using it for any other purpose.[12] This addition to the regulations goes beyond the scope of what is allowed in the CCPA. It may be possible to allow a service provider to use the information provided if that information is provably anonymized or deidentified.

The draft regulations propose adding the following language:

> (d) A service provider shall not sell data on behalf of a business when a consumer has opted-out of the sale of their personal information with the business.

EPIC recommends adding the following language to clarify that it is the business' obligation to notify any service providers who sell personal information that a consumer has opted-out of the sale of their personal information:

> A business must notify all service providers that sell data on their behalf when a consumer has opted-out of the sale of their personal information and that service provider shall be prohibited from further selling that consumer's personal information.

Section § 999.315. Requests to Opt-Out

The draft regulations add the following language:

> (c) A business's methods for submitting requests to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-

[11] 1798.140 **(C)** The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:
(i) The business has provided notice of that information being used or shared in its terms and conditions consistent with Section 1798.135.
(ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

[12] 1798.140 **(v)** "Service provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

> out. A business shall not utilize a method that is designed with the purpose or substantial effect of subverting or impairing a consumer's decision to opt-out.

EPIC supports this clarification that opt-out should be easy for consumers, while addressing the current trend of businesses making it very difficult for consumers to opt-out of the sale of their personal information.[13] EPIC also recommends adding the following language to shift the burden onto businesses once a consumer has exercised their right to opt-out of the sale of their personal information:

> If a consumer opts-out of the sale of their personal information, the business shall notify any third parties who collect personal information about that consumer on that businesses platform, service or physical location, that the consumer has opted out of the sale of their personal information and those third parties are prohibited from collecting personal information about those consumers.

Section § 999.323 General Rules Regarding Verification

The draft regulations propose adding the following language:

> (d) A business shall not require the consumer to pay a fee for the verification of their request to know or request to delete. For example, a business may not require a consumer to provide a notarized affidavit to verify their identity unless the business compensates the consumer for the cost of notarization.

EPIC supports this addition. The CCPA is clear that a business may not charge consumers who exercise their right to know the information a business collects. The authors considered requiring consumers to submit a notarized affidavit when drafting the CCPA but rejected this requirement because it places an undue burden on consumers to exercise their rights.

---

[13] Geoffrey A. Fowler, *Don't' Sell my data! We finally have a law for that,* Wash. Post (Feb. 2, 2020), https://www.washingtonpost.com/technology/2020/02/06/ccpa-faq/ ("They're not incentivized to make it easy: Amazon hid critical links in legal gobbledygook. Marketing data company LiveRamp asked me to submit a selfie holding my own ID, kidnap-victim style. Walmart asked for my astrological sign to confirm my identity. (Really.) And one business left me a voice mail, but the message included no return number … or even the name of the company. (Please call back!)… Some companies will try to shift work onto you. Airbnb and PayPal, among others, make you email them requests, rather than using web forms. Instead of a simple "do not sell" switch, companies including Mastercard make you manage a series of privacy "preferences" (as if anyone's preference would be to have their data sold). To opt out, Best Buy says you have to change your web browser to block all cookies (breaking some sites) and dig into your phone settings to turn off some advertising tracking.")

Section § 999.336. Discriminatory Practices

The draft regulations propose adding the following language:

> *~~(b) Notwithstanding subsection (a) of this section, a~~ A business may offer a financial incentive or price or service difference if it is reasonably related to the value of the consumer's ~~data as that term is defined in section 999.337~~. If a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the financial incentive or price or service difference.*

EPIC supports this change. The proposed text will clarify the non-discrimination provision and will shift the burden to business to justify financial incentives it offers consumers.

Conclusion

In EPIC's previous comments to the Attorney General on the CCPA, we noted that much could be done to make the CCPA stronger for consumers.[14] EPIC recent report, *Grading on a Curve: Privacy Legislation in the 116th Congress*, sets out the key elements of a comprehensive federal privacy law: (1) strong definition of personal information; (2) establishment of an independent data protection agency; (3) individual rights; (4) strong data controller obligations; (5) algorithmic transparency; (6) data minimization and privacy innovation; (7) prohibits take-it-or-leave it and pay-for-privacy terms; (8) private right of action; (9) limits government access to personal data; and (10) does not preempt stronger state laws. [15] Many of those provisions could be integrated into a strong state law, and many are missing from the CCPA including stronger enforcement, strong obligations on data controllers such as data minimization, algorithmic transparency, and prohibitions on "pay for privacy" and "take it or leave it" terms. The California Legislature should consider strengthening the CCPA with these provisions.

[14] *See supra* note 4.
[15] *See supra* note 3.

EPIC supports the Attorney General's leadership on privacy issues and work on the proposed regulations.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Mary Stone Ross*
Mary Stone Ross
EPIC Associate Director

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director