Published on *The National Law Review* https://natlawreview.com

California Privacy Protection Agency Officially Commences CPRA Rulemaking Process

Article By:

Hunton Andrews Kurth’s Privacy and Cybersecurity

On July 8, 2022, the California Privacy Protection Agency Board (“CPPA Board”) began the formal rulemaking process to establish regulations promulgating the amendments made to the California Consumer Privacy Act (“CCPA”) by the California Privacy Rights Act (“CPRA”) (collectively, the “CCPA/CPRA”). The CPPA Board issued a formal Notice of Proposed Rulemaking and Initial Statement of Reasons, and released the proposed regulations. The 45-day public comment period has now begun.

The Notice of Proposed Rulemaking notes that the CPPA has taken into consideration privacy laws in other jurisdictions, and that the proposed regulations would allow businesses to implement compliance with the CCPA/CPRA “in such a way that would not contravene a business’s compliance with other privacy laws,” such as the GDPR, and the U.S. state privacy laws of Colorado, Connecticut, Utah and Virginia.

While the proposed regulations are voluminous – at 66 pages – they do not include all of the approximately two dozen topics required to be addressed under the CCPA/CPRA. Additional regulations covering topics including cybersecurity audits, risk assessments, and automated decision-making are expected to be released at a later date.

The proposed regulations seek to harmonize the existing CCPA regulations with the CPRA’s amendments, operationalize new concepts introduced under the CPRA, and reorganize the text to facilitate understanding.

Summary of Proposed Regulations

The proposed regulations, if adopted, would add certain significant new compliance obligations on businesses. Below are key examples of topics the proposed regulations address.

Data Minimization (Section 7002)

The proposed regulations expand upon the CCPA/CPRA’s data minimization principle, and specify that a business’s “collection, use, retention, and/or sharing [of personal information (“PI”)] must be consistent with what an average consumer would expect.” Businesses may collect, use, retain, or "share" (for cross-context behavioral advertising purposes) PI for other disclosed purposes, provided that they are compatible with the average consumer's reasonable expectations. Explicit consumer consent is required when a business uses PI for secondary purposes unrelated to, or incompatible with, the original purpose(s) at collection. Additionally, a business may only collect PI categories that are disclosed via notice at the time of collection.

The proposed regulations illustrate several examples of where explicit consumer consent would be required because a business's use of PI would not be consistent with the reasonable expectations of an average consumer, including:

- a mobile flashlight app would need to obtain consent to collect geolocation data because the average consumer would not reasonably expect the collection of such data for the provision of flashlight services; and

- an ISP may collect geolocation data to track service outages, but may not sell the information to data brokers without consumer consent.

The introduction of the "average consumer" concept to the CCPA/CPRA's data minimization principle could mean that a business may no longer be able to rely solely on the disclosures in its privacy policy for its use of PI, and instead may need to obtain consent to use PI in ways that would be incompatible with an average consumer's reasonable expectations. This could have significant compliance implications for businesses that seek to use PI for a variety of purposes that are unrelated to the initial purpose(s) for which the data was processed.

Requirements for Methods for Submitting Consumer Rights Requests and Obtaining Consumer Consent (Section 7004)

The proposed regulations outline a number of requirements with which businesses must comply when designing and implementing consumer rights request methods and obtaining consumer consent:

- Provide Symmetry in Choice: a business's opt-out of sale/sharing mechanism must be symmetrical to the business's opt-in process; a business must not require more steps for a consumer to opt out of the sale/sharing of PI, compared to the process to opt in to such sale/sharing (after having previously opted out). For instance, the choice between "Accept All" and "More Information" is asymmetrical, whereas the choice between "Accept All" and "Decline All" is considered symmetrical. Choices must be presented in similar sizes and colors. If the choice to opt in is selected by default, it will not be considered symmetrical to the choice not to participate.

- Avoid Confusing Language: a business must avoid using confusing language when obtaining consumer consent or providing consumer rights request methods, such as the use of double negatives (e.g., the choice of "Yes" or "No" next to "Do Not Sell My Personal Information"), or toggle options that state, "On" or "Off," without further clarifying language.

- Avoid Manipulative Language: a business must not use manipulative language or architecture that guilts a consumer into making a particular decision, such as choosing between the options of "Yes" and "No, I like paying full price."

- No Bundled Consent: a business cannot obtain bundled consent to incompatible processing activities, which would be manipulative because the consumer would be forced to consent to incompatible uses to obtain an expected product or service.

- Dark Patterns: any method that does not comply with the above requirements may constitute a "dark pattern," which the proposed regulations define as "a user interface that has the effect of substantially subverting or impairing user autonomy, decision-making, or choice, *regardless of a business's intent*." (Note that this definition adds the language in italics, thereby expanding the CCPA/CPRA's existing definition of the term.) The proposed regulations, like the CCPA/CPRA, specify that agreement obtained through use of dark patterns does not constitute valid consent.

- Notice of Third-Party Data Collection (Section 7012): The proposed regulations add an entirely new notice requirement that is not reflected in the text of the CCPA/CPRA. If a business allows third parties to control the collection of PI, the business must include in its notice of collection either (1) the names of all such third parties or (2) information about the third parties' business practices. While not explicitly mentioned in the proposed regulations, "third parties that control the collection of PI" arguably would include third-party cookie providers operating on a business's site. This is a significant addition, as the CCPA currently only requires businesses to disclose certain information about the *categories* of third parties to whom PI is disclosed, but not the actual *identity* of such third parties. It is not clear how a business would comply with the alternative option, to disclose information about the third parties' "business practices," which is not detailed in the proposed regulations.

- Notice of Right to Opt-Out of Sale/Sharing (Section 7013): The proposed regulations specify that the "Do Not Sell or Share My Personal Information" link must either immediately effectuate the consumer's choice, or redirect the consumer to a webpage where the consumer can "learn about and make that choice." The proposed regulations also for the first time specify that this link must be included on the header or footer of the business's Internet "homepage" (which is broadly defined to mean any page that collects PI). The proposed regulations also allow for a business to forego posting the "Do Not Sell or Share" link if it provides an alternative opt-out link (see below) or processes global opt-out preference signals in a frictionless manner (also see below). Notably, the proposed regulations also state that a business that sells or shares PI it collects through a connected device (e.g., smart TV) or via virtual reality must ensure consumers encounter the notice via the same medium.

- Right to Limit the Use/Disclosure of Sensitive PI (Section 7014): The proposed regulations set forth a list of purposes for which a business may process sensitive PI without offering the right to limit the use or disclosure of such information (e.g., to perform the goods or services requested, to detect security incidents, to prevent fraud). A business that uses or discloses sensitive PI for purposes other than those listed in the proposed regulations must provide notice of the right to limit the use or disclosure of sensitive PI that complies with the proposed regulations' requirements. The notice must be disclosed to a consumer in the same manner in which the consumer's sensitive PI is collected (e.g., if a business collects sensitive PI by phone, the notice must be provided orally during the call). In addition to the notice, a business that collects sensitive PI online must allow consumers to submit requests to limit through an interactive form accessible via a link titled, "Limit the Use of My Sensitive Personal Information" that is displayed on the header or footer of the business's homepage, which either has the immediate effect of limiting the use and disclosure of the consumer's sensitive PI or leads the consumer to a webpage where the consumer can learn about and make that choice. The proposed regulations also allow businesses to combine the right to opt out of sale/sharing with the right to limit, in the form of an alternative opt-out link (see below).

Notably, unlike the CCPA/CPRA, the proposed regulations do not specify that the right to limit the use or disclosure of sensitive PI must be provided only where a business uses sensitive PI to *infer characteristics about consumers* (*see* Cal. Civ. Code Sect. 1798.121(d)). Therefore, businesses that process sensitive PI for purposes other than those listed in the proposed regulations, but do not use the data to infer characteristics about consumers, may nonetheless may be required to offer the right to limit the use or disclosure of sensitive PI under the proposed regulations; this inconsistency creates some confusion.

Similar to opt-out requests, the proposed regulations specify that requests to limit do not need to be verifiable. The proposed regulations require businesses to instruct their service providers/contractors and third parties to whom a consumer's sensitive PI has been disclosed to comply with the consumer's request to limit.

Processing Consumer Requests

The proposed regulations would make the following changes to the process for handling consumer rights requests:

- Deletion Requests (Section 7022): Upon receipt of a deletion request, a business must flow down such request to any third party to whom the business has sold, or with whom the business has shared, PI, unless doing so is "impossible or would involve disproportionate effort." This requirement is in addition to the existing requirement under the CCPA to flow down deletion requests to a business's service providers and contractors. Further, a business that denies a consumer's request to delete, in whole or in part, must nonetheless instruct its service providers and contractors to delete the consumer's PI that is not subject to the relevant legal exception, and not use the consumer's PI for any purpose other than the purpose provided by that exception.

  The proposed regulations also for the first time impose direct obligations on service providers and contractors with respect to deletion requests, requiring such entities to (1) comply with requests to delete, (2) notify their own service providers/contractors of such requests, and (3) notify any other service providers, contractors, or third parties that may have *accessed* PI from or through the service provider or contractor of such requests, unless the information was accessed at the direction of the business (unless doing so is "impossible or would involve disproportionate effort").

- Correction Requests (Section 7023): The proposed regulations specify that, in response to a correction request, a business may consider the totality of the circumstances regarding contested PI when determining whether the PI is accurate. To do so, a business may consider the nature of the PI, how it was obtained, and documentation related to the accuracy of the PI. Notably, the proposed regulations state that if the business is not the source if the PI and has no documentation to support the accuracy of the information, the consumer's assertion of inaccuracy "may be sufficient" to establish that the PI is inaccurate. The proposed regulations also require businesses to instruct their service providers and contractors to make the necessary corrections to the PI in their respective systems, and service providers/contractors must comply with such requests. The proposed regulations permit businesses to delete PI in response to a correction request if doing so would not negatively impact the consumer, or the consumer consents to the deletion.

If a business denies a request to correct, it must, among other requirements, (1) explain its rationale to the consumer (including any applicable legal exceptions) and (2) inform the consumer that upon the consumer's request, the business will note, internally and to any person to whom it discloses the PI, that the PI is contested. In addition, the proposed regulations specify that a consumer's request to confirm that a business has corrected inaccurate information shall not be considered an access request, or count toward the CCPA/CPRA's limitation of two access requests made within a 12-month period.

Access Requests (Section 7024)

The proposed regulations specify that a business must provide all the PI it has collected/maintained about the consumer on or after January 1, 2022, *including beyond the 12-month period* preceding the request, unless doing so proves "impossible or would involve disproportionate effort." Notably, the proposed regulations explicitly require businesses to include in response to an access request any PI that the business's service providers or contractors obtained as a result of providing services to the business.

Opt-Out Preference Signals (Section 7025)

The proposed regulations indicate that businesses must be able to comply with universal opt-out of sale/sharing preference signals, provided the signal (1) is in a commonly used and recognizable format and (2) clearly states its purpose to consumers. If a business processes opt-out preference signals in a frictionless manner, in accordance with Sections 7025(f) and (g) of the proposed regulations, it need not (but may) display the "Do Not Sell or Share My Personal Information" link, or alternative opt-out link, on its homepage.

Alternative Opt-Out Link (Section 7015)

The proposed regulations specify that a business may provide consumers with a single, clearly-labeled link that allows consumers to easily exercise *both* the right to opt-out of sale/sharing *and* the right to limit the use and disclosure of sensitive PI, instead of posting separate links for each right. The link must direct the consumer to a webpage that informs the consumer of both their right to opt-out of sale/sharing and the right to limit, and provide the opportunity to exercise both rights. The webpage must include an interactive form or mechanism by which the consumer can submit their request that is easy to execute, requires minimal steps, and complies with the requirements set forth in Section 7004 of the proposed regulations. The alternative link must (1) be conspicuous and comply with the proposed regulations' requirements for disclosures and communications to consumers (as set forth in Section 7003 of the proposed regulations); (2) be titled "Your Privacy Choices" or "Your California Choices"; and (3) include the following opt-out icon to the left or right of the link title:

Service Providers/Contractors (Section 7050)

- Application to Non-Profits: The proposed regulations notably indicate that a service provider/contractor rendering services to a non-profit nonetheless would be subject to the CCPA/CPRA, even though the entity provides services to a non-"business" under the CCPA/CPRA, which exempts non-profits from application.

- No Cross-Context Behavioral Ads: The proposed regulations make clear that a service provider or contractor cannot contract with a business to provide cross-context behavioral ads; any entity providing such services would constitute a "third party" under the CCPA/CPRA.

- Service Provider/Contractor Agreements: A business's agreement with a service provider/contractor must identify the specific (not generic) business purpose(s) and service(s) for which the service provider/contractor processes PI on behalf of the business, and specify that the business is disclosing the PI to the service provider/contractor only for the limited and specified business purpose(s) set forth within the contract. The proposed regulations indicate that the description of the business purpose or service cannot merely reference the entire contract generally, but must instead be specific. A business's agreement with a service provider/contractor must also require, without limitation, that the service provider/contractor:

    - Comply with consumer rights requests and flow down certain requests to its own service providers/contractors or third parties that may have accessed the consumer's PI;

    - Provide documentation to verify that PI is no longer retained after a request to delete; and

    - Notify the business within five business days if it can no longer meet its obligations under the CCPA/CPRA.

If a business does not include the required content in its agreements with service providers/contractors, the entity to whom the business discloses PI would constitute a "third party," to which the business may be deemed to "sell" PI.

Third Parties (Section 7052)

- Affirmative Compliance Obligations: The proposed regulations for the first time impose affirmative obligations on third parties, including but not limited to the requirement to:

    - Comply with a consumer's request to delete PI, opt out of the sale/sharing of PI, or limit the use/disclosure of PI that is forwarded to the third party by a business (and no longer retain, use, or disclose the consumer's PI unless the third party becomes a service provider/contractor under the law); and

    - Recognize and comply with opt-out preference signals as valid requests to opt out of the sale/sharing of the consumer's PI.

- Third Party Agreements:
    - The proposed regulations specify that contracts with third parties must, among other requirements:
        - Identify the limited and specified purposes(s) (not a generic description) for which the PI is sold or disclosed to the third party (note that, unlike service provider/contractor agreements, contracts with third parties do not need to specify the “business purpose(s)” (as defined under the CCPA/CPRA) for which the PI is disclosed to the third party);
        - If the business authorizes a third party to collect PI through its website (either on behalf of the business *or* for the third party’s own purposes), require the third party to check for and comply with a consumer’s opt-out preference signal (unless informed by the business that the consumer has consented to the sale/sharing of their PI); and
        - Require that the third party notify the business within five business days if the third party can no longer meet its obligations under the CCPA/CPRA.

Due Diligence (Sections 7051, 7053)

The CCPA/CPRA provides businesses with an affirmative defense to alleged CCPA/CPRA violations committed by service providers, contractors and third parties to whom the business has disclosed PI, if the business “does not have actual knowledge, or reason to believe,” that the entity intends to commit such violation. The proposed regulations introduce a new due diligence concept, specifying that a business’s due diligence of a service provider, contractor, or third party *will factor into* whether the business reasonably can rely on this affirmative defense. For example, the proposed regulations state that a business that never enforces the terms of its contract with a service provider, contractor or third party to whom it discloses PI, nor exercises its rights to audit or test the entity’s systems, *may not* be able to rely on the defense that it did not have reason to believe that the entity intended to use the PI in violation of the CCPA/CPRA at the time the business disclosed the PI to the entity. While the proposed regulations do not impose an affirmative due diligence obligation on businesses, this language encourages businesses to engage in such due diligence with respect to entities to which it discloses PI.

CPPA Audits (Section 7304)

The proposed regulations state that the CPPA may audit possible violations of the CCPA/CPRA, and provides criteria for when such audits may occur. For instance, the proposed regulations specify that the CPPA may conduct an audit if a business’s, service provider’s, contractor’s, or other person’s collection or processing of PI presents significant risk to consumer privacy or security, or if the entity has a history of noncompliance with the CCPA/CPRA or any other privacy protection law.

Next Steps

Any interested person or their authorized representative may submit written comments regarding the proposed regulations. The written comment period closes on **August 23, 2022, at 5:00 PM**. Only written comments received by that time will be considered.

Comments may be submitted by the following means:

Electronic:

Comments may be submitted electronically to **regulations@cppa.ca.gov.**

Please include “CPPA Public Comment” in the subject line.

Mail:

California Privacy Protection Agency

Attn: Brian Soublet

2101 Arena Blvd., Sacramento, CA 95834

(279) 895-6083

Written and oral comments, attachments, and associated contact information (e.g., address, phone, email, etc.) become part of the public record and can be released to the public upon request.

National Law Review, Volume XII, Number 189

Source URL:https://natlawreview.com/article/california-privacy-protection-agency-officially-commences-cpra-rulemaking-process