Updates
October 30, 2019

The Proposed CCPA Regulations Impose New Obligations

The California Attorney General's Office released for public comment the long-awaited proposed regulations for the California Consumer Privacy Act (CCPA) on October 10, 2019. The attorney general is expected to finalize the regulations in early 2020 and begin enforcement of the CCPA on July 1, 2020.

While the regulations clarify some aspects of the CCPA, they also go well beyond the statutory requirements and impose new obligations on businesses. Businesses should take a close look at their existing CCPA compliance plans, identify any compliance gaps, and begin addressing the new requirements imposed by the regulations. This update summarizes the more significant new obligations introduced by the regulations.

Article 2: Notice

Article 2 of the regulations focus on privacy notices and sets out requirements for four different types of notices to consumers: (1) notice at collection; (2) notice of the right to opt out of sales of personal information (PI); (3) notice of financial incentives; and (4) privacy policies. For each type of notice, the regulations require the notice to be:

- Easy to read and understandable to an average consumer
- Written in plain, straightforward language that avoids technical or legal jargon
- In a format that draws the consumer's attention and is readable even on smaller screens
- Available in languages that the business uses in its ordinary course
- Accessible to consumers with disabilities

The regulations also provide specific content requirements for each type of notice and instructions for how the business must present the notice to consumers.

Notice at Collection

Businesses are required to provide notice to consumers at or before the time PI is collected from the consumers. The notice at collection must include the following:

- A list of the categories of PI about consumers to be collected
- For each category of PI, the business or commercial purposes for which it will be used
- If the business sells PI, a link (or URL for offline notices) to the webpage where consumers can opt out of such sales
- A link (or URL for offline notices) to the business's privacy policy

Notice of Right to Opt Out of Sale

Businesses that "sell" PI, as that term is defined by the CCPA, are required to provide a notice of the right to stop sales. The regulations provide specific instructions for how this notice needs to be provided (in both an offline

and online context) and what type of disclosures it must contain. Specifically, the notice of the right to opt out must provide the following:

- A description of the consumer's right to opt out of the sale of PI
- The webform by which the consumer can submit a request to opt out online, or if the business does not have a website, the offline method for submitting the request
- Instructions for any other method for submitting the request to opt out
- Any proof required when a consumer uses an authorized agent to exercise his or her right to opt out or, for a printed form containing the notice, a webpage, online location, or URL where consumers can find information about authorized agents
- A link or the URL to the privacy policy or, for a printed notice, the URL of the webpage where consumers can access the privacy policy

Notice of Financial Incentive

The regulations require a business to provide a notice of financial incentives explaining each financial incentive or "price or service difference" that the business provides in exchange for consumer PI. "Price or service difference" is defined under the regulations as "(1) any difference in the price or rate charged for any goods or services to any consumer, 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, including denial of goods or services to the consumer." 11 CCR § 999.301(l). The notice of financial incentive must include the following information:

- A succinct summary of the financial incentive or price or service difference
- A description of the material terms (including the categories of PI that are implicated)
- How the consumer can opt into the financial incentive or price or service difference
- A notification of the consumer's right to withdraw from the financial incentive at any time and instructions for how to do so
- An explanation of why the financial incentive or price or service difference is permitted under the CCPA, including a good faith estimate of the value of the consumer's data and a description of the method the business used to calculate this value

The non-discrimination provisions set forth in Article 6 identify approved methods for calculating this value.

Privacy Policies

The regulations clarify that privacy policies must describe a business' *online* and *offline* practices regarding the collection, use, disclosure, and sale of PI. The regulations then provide an outline of required disclosures, many of which go beyond what the CCPA itself requires. For example, the regulations require a business to describe the process it will use to verify consumer requests, including any information that the consumer must provide. They also require a business to describe, for each category of PI collected, the categories of sources from which the PI was collected, the business or commercial purposes for which the PI was collected, and the categories of third parties with whom the PI is shared. A business is also required to provide links to an online request form or portal for making requests to know or requests to delete, if offered by the business. For a business that buys, receives, sells, or shares PI of 4 million or more consumers, the regulations require that it disclose metrics related to consumer requests (including the number of requests the business received, complied with in whole or in part, and denied, and the median number of days within which the business substantively responded to these requests)—either in its privacy policies or elsewhere on the website and accessible from a link within the privacy

policy.

Article 3: Business Practices for Handling Consumer Requests

Some of the most significant new requirements imposed by the regulations relate to how businesses must handle consumer requests to know and delete their PI and respond to sale opt-out requests. For example, the regulations provide new requirements related to the designated methods that businesses must make available for consumers to submit such requests (e.g., toll-free phone number, interactive webform, designated email address, and forms submitted in person or through the mail). Businesses must consider the methods by which they interact with consumers when determining which designated methods to provide, and at least one of the methods offered must reflect the manner in which such businesses primarily interact with consumers. For example, a business that primarily interacts with customers in person at a retail location must offer a form that can be submitted in person at the retail location, in addition to a toll-free number and interactive webform accessible through the business's website.

The regulations also introduce detailed new requirements for responding to requests. For instance, businesses may honor consumers' online requests to delete and requests to opt in to the sale of their PI after having opted out only after consumers reconfirm their requests. In addition, if a consumer request is not made through a designated method or is deficient, businesses must either treat the request as properly submitted or give the consumer specific directions on how to correct the deficiency or submit the request. The regulations also describe certain circumstances in which a business shall not provide a consumer with specific pieces of PI, such as when the disclosure creates a substantial, articulable, and unreasonable risk to the security of the PI, the consumer's account with the business, or the security of the business's systems or networks. Additionally, businesses shall not disclose a consumer's Social Security number, a driver's license number or other government-issued identification number, a financial account number, any health insurance or medical identification number, an account password, or security questions and answers.

With respect to sales opt-out requirements, the regulations incorporate do-not-track principles and require businesses that collect PI online to treat user-enabled privacy controls (such as browser plugins or other privacy settings) that communicate or signal the consumer's choice to opt out of the sale of his or her PI as a valid opt-out request for that browser or device or, if known, for the consumer. The regulations also impose a 15-day deadline for businesses to act upon an opt-out request and require that businesses notify all third parties to whom they have sold the PI in the 90 days prior to receiving the request of the consumer's decision to opt out and instruct such third parties not to further sell the PI.

The regulations also impose training and record-keeping requirements on businesses. All individuals responsible for handling consumer inquiries about a business' privacy practices or its CCPA compliance must be trained on all the requirements of the CCPA and the regulations and on how to direct consumers to exercise their CCPA rights. Businesses that buy, receive, sell, or share PI of 4 million or more consumers are further required to establish, document, and comply with a written training policy.

Article 4: Verification of Requests

The regulations require businesses to establish, document, and comply with a reasonable method for verifying identities before complying with consumer requests to know or delete PI. The regulations provide a list of factors that businesses should consider when developing their verification procedures, including but not limited to the type, sensitivity, and value of the PI; the risk of harm to the consumer posed by any unauthorized access or deletion; and the likelihood that the PI would be targeted by fraudulent or malicious actors. The regulations then

go into great detail about how to verify password-protected accounts and the identities of non-accountholders. Generally speaking, a business must avoid requesting information from the consumer that the business does not already have, and it must implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of PI. Article 4 also imposes new requirements for requests submitted by an authorized agent on behalf of the consumer.

Article 5: Special Rules Regarding Minors

The regulations impose specific obligations for opt-in and opt-out requests related to the sale of PI involving minors under 16. For minors under 13, businesses must establish, document, and comply with a "reasonable method" to determine that the person authorizing the sale of a child's PI is the parent or guardian. Examples of reasonable methods include providing a consent form to be signed and returned under the penalty of perjury by the parent or guardian or having the parent or guardian call a toll-free number staffed by trained personnel. For minors between 13 and 16, businesses must establish, document, and comply with a reasonable process for allowing such minors to opt in to the sale of their PI. A business must reconfirm a request from a minor to opt in. When a business receives an opt-in request for sale of minor PI, the business must inform the parent or guardian (if under 13) or minor (between 13 and 16) of the right to opt out at a later date and the process for doing so.

Article 6: Non-Discrimination

Article 6 attempts to provide more clarity around discriminatory practices and provides some illustrative examples of financial incentives that do *not* violate the CCPA. For instance, it is discriminatory if a music streaming business offers both a free service and a paid service but allows only the paying customers to opt out of sales of PI, *unless* the payment is reasonably related to the value of the consumer's data to the business. This example underscores the significance of the proper valuation of a consumer's data. While it is still unclear how businesses will calculate this value in practice, the regulations provide a list of suggested methods.

If adopted in their current form, the regulations will impose significant compliance obligations on businesses that process PI from California residents. And while the regulations are not yet final, they reflect the AG's enforcement outlook. There is still time for companies to create or adapt their privacy programs as well as influence the final outcome of the regulations. The AG is currently accepting comments to the regulations, which can be submitted at public hearings to be held in early December or by writing to PrivacyRegulations@doj.ca.gov before December 6.

Companies looking to incorporate these regulations into their compliance programs should consult with their legal counsel

Authors

Miriam Farhi

Partner
MFarhi@perkinscoie.com 206.359.8195

Natasha Amlani

Associate
NAmlani@perkinscoie.com 310.788.3347

Explore more in

Privacy & Security

Related insights

Update

Ninth Circuit Rejects Mass-Arbitration Rules, Backs California Class Actions

Update

CFPB Finalizes Proposed Open Banking Rule on Personal Financial Data Rights