wiley

NEWSLETTER

Ten Things You Need to Know About the CCPA Draft Regulations

November 2019

Privacy in Focus®

On October 10, 2019, the California Attorney General released draft regulations to implement the California Consumer Privacy Act (CCPA). While the draft regulations clarify some obligations under the statute, they also potentially add to a business's compliance burden and create uncertainty in several areas. The regulations are not final and are open for comment until December 6, meaning that in all likelihood, we will not see the final regulations until well after the CCPA goes into effect on January 1, 2020.

Amid this uncertainty, we are helping clients manage compliance strategies for the CCPA, including the new compliance obligations proposed in the draft regulations. Informed by the draft regulations, here are 10 key points to consider when planning for CCPA compliance:

1. **Your Privacy Policy Will Need Significant Updates.** The statute and the draft regulations require a business to disclose very specific information in its privacy policy. This includes details about how personal information is collected; how personal information is sold or disclosed for a business purpose; what rights consumers have; how consumers may submit a request to exercise those rights; how a consumer may designate an authorized agent to submit requests; when the privacy policy was last updated; and how to contact the business. On top of this, some businesses that deal with a high volume of personal information, under the draft rules, would need to disclose specific metrics (discussed in more detail below).

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

At the same time, the privacy policy must be designed and presented to the consumer in a way that is "easy to read and understandable to an average consumer" – a difficult task given the volume of information that must be disclosed. It must also be accessible to consumers with disabilities. The statute and regulations do not specify how exactly this latter requirement should be met, so companies will need to look closely at standards and best practices.

2. **The Draft Regulations Contemplate Multiple Consumer Notices.** The draft regulations contemplate three separate notices, in addition to the privacy policy: a notice at the time of collection of personal information, a notice of the right to opt out of the sale of information, and a notice of financial incentives (or price or service difference) for collection. While the draft regulations would allow these notices to either be stand-alone documents or included as separate sections within the privacy policy, each would need to have a separate, conspicuous link. The draft rules call for these links (in all cases but the link to the notice of financial incentive) to be found on a website's "homepage." Unfortunately, the draft regulations do not clear up the ambiguity created by the statute as to what constitutes a website "homepage." Additionally, the draft regulations explicitly exempt businesses that do not "sell" personal information from posting a notice of right to opt out, but *include* a requirement that the business affirmatively state that it "will not" sell personal information in the future – an obligation not found in the statute.
3. **Offering Compliant Financial Incentives and Pricing Differences Is Complicated.** The draft regulations expand on (but complicate) the statute's guidance on how to offer compliant financial incentives and pricing differences. The CCPA prohibits discrimination against consumers based on the exercise of their CCPA rights, but permits financial incentives and price and service differences in limited circumstances. The CCPA requires that the price or service difference must be reasonably related to the value of the consumer's data. The draft regulations require a business to provide a detailed analysis of how the value is calculated and include an expansive list of factors to consider when estimating value, including the marginal or average value of the data to the business, revenue or profit generated by use of the data, or expenses related to collection or use of the data. Confusingly, the draft regulations define a "price or service difference" to include differences obtained through use of financial payments (that is, a "financial incentive"), and the notice and data valuation provisions suggest that businesses must also calculate data valuation for both financial incentives and price or service differences (though this requirement is not in the CCPA itself). Bottom line: Businesses will need to carefully think through any differential treatment of consumers based on collection, sale, or ability to delete their data.
4. **The Process to Verify a Consumer Request Is Elaborate, but Not Well-Defined.** Under the draft regulations, a business needs to establish a "reasonable method" for verifying the identity of an individual who submits a request to know or a request to delete (though notably, not a request to opt out of sale). A business should, where feasible, match the identifying information provided by the consumer to personal information the business already maintains, or use a third-party verification service to do the same, but should avoid collecting new information or certain sensitive information

(such as a Social Security Number) unless "necessary" for verification. The regulations also require that the verification process be tailored to the type of information requested and the risk of harm posed by unauthorized access or deletion of that information. In short, the regulations will require a careful balancing act of being responsive to a consumer request and protecting information from disclosure to unauthorized third parties.

5. **A Consumer's Right to Know May Require a Personalized and Detailed Response.** The draft regulations provide detailed requirements for responding to requests to know, which in some cases goes beyond the statute. First, consider timing – per the statute, there is a 12-month "look back" on consumers' data, meaning that consumers can request information about the collection, use, disclosure, and sale of their personal information for the 12-month period prior to the request. Since the law takes effect January 1, 2020, that means businesses must be prepared to receive requests about personal information during all of 2019 (when the law was not in effect). Consumers have the ability under the statute and draft regulations to request detailed information that a business has collected about them. The CCPA contemplates that the response to the consumer would be customized, not a generic response. The consumer could ask for the categories of information that the business has collected about them or could request specific pieces of data collected about them during the past year. A business must be ready to respond to each type of request, and there are different requirements for doing so. For example, there are various security considerations and requirements around transmitting specific pieces of data. Additionally, the business must be prepared to disclose the purpose of the collection, categories of third parties to whom information was disclosed, and the business or commercial purpose for the disclosure.

6. **Responding to a Request for Deletion – Pay Attention to the Deadlines.** The draft regulations propose to require a business to confirm receipt of a consumer's request within 10 days and comply with the request within 45 days. These same deadlines apply to a request to know. The business can extend its deadline by an additional 45 days if it notifies the consumer. If the business denies the request for deletion, it must explain why. Depending on its reason for denying the request, a business may create additional obligations for itself. For example, if the denial is based on inability to verify the identity of the consumer, it must nevertheless treat it as a request to opt out of sale (which does not require verification).

7. **The Regulations Impose Specific Obligations for the Right to Opt Out.** The CCPA's right to opt out is perhaps its best-known consumer right. The draft regulations provide additional context, but also additional requirements for a business that sells information. The draft regulations confirm that a business must have a prominent hyperlink on its website declaring "Do Not Sell My Information" or "Do Not Sell My Info." The draft regulations contemplate that a consumer could use an authorized agent to exercise their rights, including the right to opt out. However, the regulations also encourage a business to verify that an authorized agent is acting on at the individual's request. The draft regulations require a shorter response time for requests to opt out than that proposed for the other rights. A business is required to act on a request to opt out "as soon as feasible possible" but no later than 15 days. Additionally, it must pass that request down the chain of third parties to which it has sold the consumer's information within the preceding 90 days.

8. **If Your Business Collects Information About Consumers Indirectly, It Has Obligations.** Some businesses may obtain personal information indirectly – either as "service providers" or because a business purchases or otherwise obtains personal information from another business. If the business is acting as a service provider, ensure there is a written contract in place with the required CCPA language that prohibits the business from using or disclosing the information for any purpose other than the contractual business purpose. If the business has otherwise obtained personal information about a consumer indirectly, then the draft regulations require that before **selling** that information, the business must contact the consumer directly to provide an opt-out notice (or, alternatively, contact the source from which your business received the personal information and obtain a signed attestation that the consumer received a notice at collection).
9. **For a Business That Deals with a High Volume of Personal Information, the Draft Regulations Propose Heightened Disclosure Requirements.** The draft regulations introduce wholesale new requirements for businesses that buy, receive, sell, or share for commercial purposes the personal information of 4 million or more consumers. These businesses would be required to provide very detailed disclosures in their privacy policies or on their websites of: (1) the number of requests to know/delete/opt out (including the number approved and denied), and (2) the median number of days it took the business to respond to those requests. Additionally, these businesses must implement a training program for their employees who handle consumer requests (which is a requirement under the CCPA for all businesses).
10. **Don't Forget the "Other" California Privacy Rules.** The CCPA and draft regulations notably do not reference the existing California laws that govern privacy policies and practices, including the California Online Privacy Protection Act (CalOPPA) and California's Shine the Light law. CalOPPA, for example, requires commercial websites and online services to post a privacy policy and requires disclosures regarding tracking of online visits. As you are updating your policies and practices to be compliant with the CCPA, it is important not to overlook these other laws.