Client Alert | Data, Privacy & Cybersecurity

The California Consumer Privacy Act Regulations Are Finally Here, But Wait There's More…

August 2020

Authors: F. Paul Pittman, Kyle Levenberg

On August 14, 2020, California's Office of Administrative Law ("OAL") approved the final version of the implementing regulations for the California Consumer Privacy Act ("Final Regulations"). The approval of these final regulations caps off a long period of uncertainty and establishes specific content and administrative compliance obligations for businesses subject to the California Consumer Privacy Act ("CCPA"). The regulations are effective immediately.

Although the Final Regulations have only just been approved, the California Attorney General ("California AG") has already begun initiating enforcement activity by sending initial notices of noncompliance with the CCPA to businesses in multiple industries on July 1, 2020. According to the California AG, the notices focused on online businesses that allegedly failed to comply with the obligation to provide a "Do Not Sell My Personal Information" link, and emanated from consumer complaints. While the California AG clarified that those notices were based on noncompliance with the CCPA statute and not the proposed final regulations, enforcement focus could soon shift to include compliance with the Final Regulations.

As such, businesses who have not yet implemented the unique disclosure and business process requirements set forth under the Final Regulations should take immediate steps to bring their programs into compliance. This is so, not only because of the increasing enforcement risk, but also because new and additional consumer privacy compliance obligations under the proposed California Privacy Rights Act ("CPRA") are lurking. We outline the immediate steps to achieve compliance with the Final Regulations below, taking into account prior efforts to comply with the CCPA statute that we outlined previously.

Steps to Comply with the CCPA Final Regulations

The Final Regulations establish specific procedures for businesses to implement the CCPA's statutory requirements that facilitate new consumer rights. The Final Regulations do not reflect a change in what is required under the CCPA statute, but rather elucidate the expectations of the regulator for businesses under the CCPA.

- **Update Privacy Policy Disclosures**. Amend existing privacy policies to disclose additional data privacy collection, use, disclosure and sale practices, and provide details on the business's verification and processing of requests, and financial incentives.
- **Provide Notice of Collection of Personal Information**. Provide timely notice of collection and use of personal information to employees and consumers online, in-store and via mobile apps,

and update that notice as collection practices change. Businesses should ensure that their data mapping exercise identifies all points of ingress of personal information, so that notice is provided at the appropriate time.

- **Adjust Methods for Accepting and Responding to Consumer Requests**. Implement or revise existing processes and mechanisms for accepting and responding to consumer requests that ensure consistency with CCPA requirements, including, for example, ensuring that sensitive personal information (*i.e.*, SSNs, account passwords, biometric information, etc.) is never disclosed, utilizing less restrictive methods for submitting requests that are consistent with the methods a business uses to primarily interact with consumers, and including required disclosures within its response to a consumer.

- **Apply Reasonable Security Controls to Responses to Consumer Request**. Specific security controls and measures are necessary to ensure that personal information provided to a consumer pursuant to a consumer request is subject to reasonable security procedures. This concept of reasonable security continues an emphasis in the CCPA on businesses having reasonable security with regard to personal information, with the original statute permitting private cause of action for data breaches that are determined to have resulted from a lack of reasonable security.

- **Adhere to Guidelines for Verifying Consumer Requests**. Incorporate criteria set forth under the Final Regulations for verifying consumer requests for general as well as specific information to varying degrees of certainty. An established and efficient verification process takes on even more importance since the Final Regulations clarify that the 45-day time period begins to run upon receipt of a request, regardless of the time required to verify a request.

- **Establish Recordkeeping**. Maintain records of CCPA consumer requests in a specific form for at least 24 months. Businesses that process the personal information of ten million or more consumers per calendar year are subject to additional obligations, and they are required to compile and disclose metrics relating to consumer requests in their privacy policy annually.

- **Enable Notice to Individuals with Disabilities**. Consider generally recognized industry standards to ensure that the required notices regarding the business's privacy practices is reasonably accessible to consumers with disabilities.

- **Confirm Receipt of Consumer Requests**. Businesses must respond to consumer requests within ten days of receipt, informing the consumer of the business's verification process and timing for response.

Regulating a Modern Gold Rush

How Did We Get Here?

After the CCPA's enactment in June 2018, the California AG's office embarked upon a journey to provide guidance for compliance with the "historic, game-changing" CCPA. Accordingly, on October 11, 2019, California Attorney General Xavier Becerra introduced the first version of the proposed implementing regulations required under Section 1798.185 of the CCPA. These first proposed regulations aim to address five key components:

1. Explain how businesses are required to inform consumers of their rights under the CCPA
2. Address how businesses would handle consumer requests about their data
3. Clarify how businesses are to verify consumer's identities in response to consumer requests
4. Explain how businesses are to respond to requests concerning the data of minors under the age of 16
5. Explain how businesses can avoid discriminating against consumers who choose to exercise their rights under the CCPA

The proposed regulations kicked off a 45-day notice and comment period in which the California AG held seven public forums, and received more than 300 written comments from various interested parties, including industry representatives, activists and concerned California citizens. On February 10, 2020, the California AG released updated modified regulations, which triggered a 15-day Comment Period, attracting nearly 800 pages of feedback from interested parties.

The second set of modified regulations to the CCPA were released on March 11, 2020, subject to another 15-day Comment Period. The California AG submitted this version of the regulations along with a Statement of Reasons ("SOR") providing background and justification behind the regulatory requirements to the OAL on June 1, 2020, for approval. OAL reviewed the regulations, and made mostly non-substantive changes for accuracy, consistency and clarity, but did withdraw (for future consideration) several provisions relating to offline opt-out rights, methods for accepting opt-out requests, use of previously collected personal information inconsistent with a notice at collection, and verification of an authorized agent, before issuing its approval on August 14, 2020.

Where Are We Now?

The Final Regulations are split into six articles, each intended to guide compliance with the CCPA in certain specific ways.

1. Article 1 provides additional clarity to the terms of art used throughout the CCPA. In addition to clarifying meaning, some of these definitions go a long way in describing some of the obligations contemplated by the regulator.

2. Article 2 provides detailed information about the form, content and purpose of the notices contemplated by the CCPA.

3. Article 3 provides specific guidance concerning: (a) the mechanisms businesses should provide for consumers to submit requests to know, delete or opt-out, (b) how businesses should respond to those requests, (c) the obligations of service providers in responding to consumer requests, and (d) general information concerning the training and record-keeping requirements of the CCPA.

4. Article 4 provides general rules regarding verification of the identity of consumers, and specific methods to be used for accountholders, non-accountholders and authorized agents.

5. Article 5 sets out the special rules relating to minors under 16 years of age.

6. Article 6 provides details on when a financial incentive or a price or service difference may be considered discriminatory under the CCPA and examples of ways to calculate the value of a consumer's data to the business.

As described above, the Final Regulations underwent two revisions following comments from industry and practitioners. Consequently, certain provisions have evolved over time to reflect these identified issues and considerations. We highlight a few of these areas below.

Highlight: Evolution of Service Providers

The definition and permissible activities of a service provider have evolved throughout the CCPA rulemaking process. Under the CCPA statute, service providers provide protection for certain necessary, limited transfers of personal information by a business, allowing them to fall outside of the definition of "sale" and the related disclosure requirements. The Final Regulations expand on the entities and activities that fall under the service provider rubric, and identify five specific instances where a service provider may use, retain or disclose personal information obtained in the course of providing services. In contrast, the initial version of the CCPA regulations permitted a much broader use of personal information by the service provider. As such, businesses that previously took an expansive view of which vendors were service providers may have to reconsider their designations.

Highlight: The Opt-Out Button that Never Was

Under the CCPA, the California AG was required to establish rules and procedures for the development and use of a recognizable and uniform opt-out button to promote consumers' opportunity to opt-out of the sale of personal information. In the first set of modifications, the California AG did just that, proposing a design which many in the industry called unworkable. By the release of the Final Regulations, however, all mention of the opt-out button had been removed.

Highlight: Guidance Regarding the Interpretation of CCPA Definitions

One of the notable exclusions from the Final Regulations was the deletion of a provision clarifying when information maintained by a business constituted "personal information" as defined by the CCPA. The addition of the guidance in the first modified regulations was applauded by interested parties in affected industries and by privacy activists alike as greatly clarifying the intention of the CCPA and providing nuance to the question of whether certain pieces of information, such as IP addresses, fell under the protections of the CCPA. The clarifying provision, however, was short lived and was stricken from the regulations in the March, 2020, updates, possibly because it was viewed by commentators as overly limiting or exceeding the Attorney General's rulemaking authority.

Highlight: Global Privacy Controls

Although modified in some respects, the California AG has consistently included a requirement to treat "user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism," as a valid request to opt-out of the sale of personal information. Early on, advertising industry groups were requesting the removal of this requirement from the regulations, arguing that the opt-out undermined the ability for that consumer to make discrete choices about their data-sharing practices. The California AG did not relent, however, and the Final Regulations have maintained this requirement, while requiring that any global privacy controls clearly indicate that a consumer intends to opt-out. In addition, the regulations permit a business to notify a consumer that its global privacy control conflicts with their existing business-specific setting or participation in a financial incentive program.

For California, the CCPA is Not Enough

The California Privacy Rights Act of 2020

Just as businesses are wrapping up their consumer privacy compliance implementation efforts in California, new obligations may be on the horizon. To address perceived inadequacies or gaps in the CCPA, the advocacy group that originally sponsored the CCPA—Californians for Consumer Privacy—recently succeeded in gathering the required roughly 600,000 signatures to place an even more stringent privacy bill, the California Privacy Rights Act ("CPRA") on the 2020 ballot. Should this initiative be approved by California voters in November, Californian citizens will see their rights under the CCPA expanded, which in turn will create additional obligations with which businesses will have to comply.

Among the biggest changes in the CPRA is the creation of the California Privacy Protection Agency, which would be given power to enforce the CCPA. In addition to the creation of this agency, we note the following key provisions of the CPRA:

1. Creates a "sensitive personal information" subcategory of personal information, the collection of which vests additional rights in consumers and imposes further obligations on businesses relating to its processing

2. Creates additional consumer rights for California residents, including the (a) right to correct inaccurate personal information, (b) the right to opt-out of advertisers using precise geolocation, (c) the right to know the length of data retention, and (d) the right to restrict usage of sensitive personal information

3. Expands the private right of action for data breaches to include account credentials where the business fails to maintain reasonable security

4. Significantly impacts the online advertising ecosystem by requiring businesses to extend the right to opt-out of the sharing of their personal information for use in behavioral advertising, and excludes use of personal information in behavioral advertising as a business purpose

5. Strengthens opt-in requirements and enhances the penalties regarding the sharing or sale of children's data

6. Removes a 30-day cure period for businesses to rectify CCPA violations

7. Introduces necessity-based data retention limitations

8. Requests that the California AG issue additional regulations requiring, among other things, privacy and cybersecurity audits and risk assessments, addressing consumer-profiling

If passed, most provisions of the CPRA would become effective on January 1, 2023, with enforcement beginning on July 1, 2023.

Conclusion

For most businesses continuing to adjust to the impact of the ongoing COVID-19 pandemic—or fighting to stay afloat—the approval of the Final Regulations may cause an unwanted diversion of resources and attention to ensure compliance. The California AG has not been helpful in this regard, never wavering in its intention to proceed with enforcement activity, even in the face of the pandemic. Businesses that have already taken steps to comply with the CCPA—or even the GDPR—will have a much lower compliance burden than those who haven't, but as we outline above certain achievable compliance efforts remain. Further, despite the regulations being finalized areas of uncertainty remain regarding how the Final Regulations will be interpreted, enforced and what practices will be deemed compliant. As such, businesses will be left to determine a reasonable approach to compliance until further guidance through enforcement or rulemaking provide clarity. In light of this, and the proposed CPRA, White & Case will continue to monitor and report on new developments which can be found on our California Consumer Privacy Act website.

White & Case LLP
701 Thirteenth Street, NY
Washington, District of Columbia 20005-3807

T +1 202 626 3600