Patterson Belknap

Privacy & Data Security Alert

October 2019

Count Down to the California Consumer Protection Act: Charting a Course to CCPA-Readiness

The California Consumer Privacy Act ("CCPA") becomes operative on January 1, 2020. *See* Cal Civ. Code § 1798.100 *et al*. To date, the CCPA is the most sweeping consumer privacy law in the United States, covering most for-profit entities that do business in California and collect the personal information of California residents. The law assigns enforcement of its provisions to the California Attorney General, but it also provides a private right of action for data breaches along with statutory damages. In this primer, the Patterson Belknap Webb & Tyler Privacy and Data Security team provides an overview of what businesses need to know about the CCPA, steps they can take now to prepare, and open questions under the CCPA that will bear on CCPA risk mitigation going forward.

The CCPA was enacted in 2018 and has been amended once already on September 23, 2018. More recently, on September 13, 2019, the California legislature sent five additional bills amending the law to the governor's desk. The California Attorney General is also expected to publish regulations this fall that may bring welcome clarity to the scope and implementation of the law. With the operative date fast approaching, however, companies covered by the law ("Businesses") should begin taking steps toward compliance. To that end, we are providing the following guidance to companies faced with ensuring readiness for a law unlike any other in the U.S. and steeped in uncertainty. Here, we break down the CCPA with ***five*** major responsibilities for Businesses under the law; ***four*** action items for Businesses to tackle right away on the road to compliance; and ***three*** open questions about the law.

Five Obligations Under The CCPA

The CCPA imposes five core requirements on Businesses: Notice; Disclosure; Deletion; Opt-Out; and Non-discrimination.

1. **Notice (§§ 1798.100; 1798.130)**: Businesses that collect personal information from California consumers ("Consumers") must provide notice to those Consumers at or before the moment the Business obtains or otherwise receives that information. The notice must inform Consumers of the categories of information that will be collected and the purpose for collecting the information. Businesses must also update their privacy policies to include a description of Consumers' rights to disclosure, opt-out of sale, and non-discrimination, as well as the categories of personal information they collect.
2. **Disclosure (§§ 1798.100; 1798.110; 1798.115; 1798.30)**: Businesses must provide Consumers with two methods for submitting requests for information under the CCPA. For most Businesses, this will be a toll-free number and a web page. Upon receipt of a Consumer's verifiable request for information, a Business must disclose the following information about the requesting Consumer that the Business collected, sold, or disclosed over the preceding 12 months:

a. Categories of personal information it has collected, sold, or disclosed for a business purpose about the Consumer;

b. Specific pieces of personal information that the Business has collected about the Consumer;

c. Categories of sources from which the personal information was collected;

d. The purpose for the collection; and

e. The categories of third parties with which the Business shared or to which it sold the personal information.

3. **Deletion (§ 1798.105)**: After receiving a Consumer's request for deletion of their personal information, Businesses must delete the personal information from their records and direct their service providers to do the same. There are, however, several exceptions to this deletion requirement. Businesses are not obligated to delete Consumer personal information if maintaining the information is necessary to:

    a. Complete the transaction for which the personal information was collected, provide a reasonably anticipated good or service, or otherwise perform a contract between the Business and the Consumer;

    b. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity;

    c. Identify and repair errors that impair existing intended functionality;

    d. Exercise free speech, ensure the right of another Consumer to exercise free speech rights, or exercise another right provided by law;

    e. Comply with the California Electronic Communications Privacy Act;

    f. Engage in scientific, historical, or statistical research in the public interest, if the Consumer has provided informed consent;

    g. Enable solely internal uses that are reasonably aligned with the Consumer's expectations based on the Consumer's relationship with the Business;

    h. Comply with a legal obligation; or

    i. Use the Consumer's personal information, internally, in a lawful manner that is compatible with the context in which the Consumer provided the information.

4. **Opt-Out (§§ 1798.120; 1798.135):** Businesses that sell Consumers' personal information to third parties must provide notice to the Consumers that their information may be sold and a clear and conspicuous link enabling the Consumers to opt-out of the sale. If Consumers are younger than 16 years old, Businesses may not sell their information without the Consumers' affirmative opt-in or, if under 13 years old, the opt-in of their parents or guardians.

5. **Non-Discrimination (§ 1798.125):** Businesses cannot discriminate against Consumers who choose to exercise their rights under the CCPA unless the difference in the services provided is reasonably related to the value of that Consumer's data. Businesses may, however, offer financial incentives for the collection and sale of personal information.

Four Steps Toward Compliance That Businesses Can Take Now

Complying with the CCPA will be a substantial undertaking. Here are four steps that Businesses can take now to jumpstart their compliance efforts. Businesses will be well-advised to consult closely with counsel in all aspects of their compliance efforts, especially in light of the potential for enforcement by the California Attorney General and litigation pursuant to the private right of action, coupled with the potential for statutory damages.

1. **Determine whether you are covered by the CCPA:** The CCPA covers any for-profit entity that satisfies four central criteria: (i) it collects personal information of Consumers or has such information collected on its behalf; (ii) it "determines the purposes and means of the processing of consumers' personal information"; (iii) it does business in California; ***and*** (iv) it satisfies at least one of the following three criteria:

    a. The Business has annual gross revenues in excess of $25 million; ***or***

    b. The Business annually buys, receives for commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more Consumers, households, or devices; ***or***

    c. The Business derives 50% or more of its annual revenue from selling Consumers' personal information.

    If a Business that meets this definition controls or is controlled by another entity and shares common branding with that entity, then that entity is also a "Business" under the CCPA. Notably, this control and common branding provision, on its face, raises the possibility that a related entity could be covered even if it is not a for-profit company, does not do business in California, or would not otherwise be covered by the CCPA.

2. **Take stock of the data you have and the data you expect to collect:** Businesses should determine what data from Consumers they hold or will collect in the future. In taking this inventory, it is critical to keep in mind the expansive scope of the CCPA's definition of "personal information." Businesses should also determine where relevant data is stored and the best way to search it if and when a Consumer requests it or requests its deletion. Two of the recent amendments to the CCPA are noteworthy here:

    a. **Employment Information:** If signed into law, one amendment will delay for one year, until January 1, 2021, all CCPA requirements, except for the notice requirement, with regard to personal information of a Business' employees, owners, directors, contractors, and job applicants collected and used by Businesses in the context of the person's employment.

    b. **Business Communications:** Another amendment would delay for one year, until January 1, 2021, all CCPA requirements, with the exception of the opt-out and non-discrimination requirements, regarding business-to-business communications. Business email in particular may contain personal information (for example, email addresses, physical addresses, and phone numbers), so this deferral will potentially provide Businesses with additional time to address the many compliance issues posed by business-to-business email.

3. **Create a notice and update your privacy policy:** Businesses will be required to notify Consumers, at or before the point of collection, of the categories of personal information being collected and the purposes for which that information will be used. Businesses are also required to update their online privacy policies to include a description of Consumers' rights to disclosure, opt-out of sale, and non-discrimination, as well as list the categories of personal information collected and personal information sold or disclosed for a business purpose. For Businesses that sell Consumers' personal information, the privacy policy must also include a link entitled, "Do Not Sell My Personal Information," that takes Consumers to an opt-out page.

4. **Set up designated methods for Consumers to submit requests:** The CCPA requires that Businesses create two methods for Consumers to submit information requests; one of those methods must be a toll-free telephone number. If the Business has a website, it must also provide a website address for submitting requests. Businesses that sell Consumers' personal information, moreover, must go one step further, creating a clear and conspicuous link on their homepages entitled, "Do Not Sell My Personal Information." This link should easily enable Consumers to opt-out of the sale of their personal information.

   Businesses also need to be mindful that the law requires all individuals responsible for handling Consumer data requests to be informed of the CCPA's disclosure, opt-out of sale, and non-discrimination requirements, and able to inform Consumers of how to exercise their rights to disclosure, opt-out, and non-discrimination.

<u>Three Open Questions</u>

Businesses covered by the CCPA can begin taking steps now to ensure readiness on January 1, 2020. But the CCPA leaves a number of important questions unanswered. Three of the most pressing questions are outlined below, some of which may be resolved—or at least addressed—by the forthcoming regulations from the California Attorney General:

1. ***How does the CCPA apply to companies that receive personal information from Businesses who collect that information?*** The CCPA refers to these data recipients as "third-parties," but says little to delineate the contours of their obligations. And for companies that fall into this category, the CCPA's ambiguity can raise critical questions: how can a third party provide meaningful notice or opt-out rights to Consumers with whom it has no direct contact? Are third parties required to accept requests for disclosure or deletion and respond to those requests?

2. ***What is a "verifiable consumer request" and how can a Business verify that it is disclosing information to the actual Consumer and not an imposter?*** This question implicates the heart of day-to-day compliance under the CCPA because the answer will guide Businesses in distinguishing between actionable requests, and those of a more spurious variety.

3. ***How can a Business "cure" a CCPA violation?*** The CCPA provides a grace period for Businesses found to be out of compliance with the statute. Before the California Attorney General may bring a civil action against a Business for violating the CCPA, that Business has 30 days from notice of the alleged violation to cure it. But the statute is silent on the standard to be applied in determining the sufficiency of a "cure." Shaping this concept into practical guidance will be critical to ensuring Businesses are not only on notice of their obligations under the CCPA, but also understand what they can do to mitigate the effects of a violation and reduce the risk of an enforcement action by the Attorney General.

We will continue to monitor developments related to the CCPA and will post updates on our blog, https://www.pbwt.com/data-security-law-blog/, as additional amendments and guidance are released.

Please contact us with any questions.

Michael F. Buchanan	212.336.2350	mfbuchanan@pbwt.com
Alejandro H. Cruz	212.336.7613	acruz@pbwt.com
Peter A. Nelson	212.336.2406	pnelson@pbwt.com
Julia R. Livingston	212.336.2579	jlivingston@pbwt.com
Jonathan Schenker	212.336.2075	jschenker@pbwt.com
Jeffrey C. Skinner	212.336.2686	jskinner@pbwt.com

This alert is for general informational purposes only and should not be construed as specific legal advice. If you would like more information about this alert, please contact one of the following attorneys or call your regular Patterson contact.