California Attorney General Wastes No Time Beginning CCPA Enforcement

July 28, 2020

Earlier this year, a coalition of over 60 different businesses and trade groups joined forces in an effort to delay enforcement of the California Consumer Privacy Act (CCPA). That effort failed, and the California Attorney General's power to take enforcement action took effect on July 1, 2020.

What Exactly Can The Attorney General Enforce?

The CCPA, which has been in effect since January 1, 2020, gives the Attorney General full authority to bring enforcement actions against companies for any violations that have occurred since the act's effective date. This means the Attorney General can file a civil lawsuit against any company that commits an uncured, or incurable, violation of the Act, and a court may impose civil penalties of up to $7,500 per violation. Examples of violations the Attorney General may pursue include, but are not limited to:

- failure to provide adequate notice to consumers at or before the point their personal information is collected regarding categories collected and how they will be used;
- failure to post a comprehensive privacy policy that makes CCPA-specific disclosures regarding online and offline data collection, use and sharing and consumer rights;
- failure to post a "Do Not Sell My Personal Information" button on the business's website that links to a web form consumers can use to direct the business not to sell their personal information (if the business is sharing personal information in a manner that meets the CCPA's extraordinarily broad definition of "sale");
- incorrectly declaring in the privacy policy that the business does not sell personal information (if the business is sharing personal information in a manner that meets the CCPA's extraordinarily broad definition of "sale");
- failure to process consumer requests (i) to know what personal information the business has about them and how it is used and shared, (ii) to delete their personal information, or (iii) to opt-out of sales of their personal information;
- selling the personal information of children under the age of 16 without first getting opt-in consent from the child, or from a parent or legal guardian in the case of children under the age of 13; and
- theft or unauthorized disclosure of sensitive categories of personal information that results from the business's failure to use reasonable security procedures and practices.

Complicating this picture is the fact that the Attorney General's proposed implementing regulations—which in many respects define compliance obligations in more detail than the language of the act itself—have undergone several changes since the first draft was released in October 2019. In fact, this continued "evolution" of the CCPA's requirements served as one the main reasons companies sought to postpone its enforcement date. Many were concerned that there would be insufficient time to implement the regulations before they become enforceable.

They were half right. The Attorney General submitted the final version of the proposed regulations to the California Office of Administrative Law (OAL) on June 1, 2020, just one month before the enforcement date, with a request that the review be expedited to ensure the regulations became effective on July 1. Normally, after the Attorney General submits proposed regulations, the OAL has thirty days to review and approve them. The regulations are not enforceable until after the OAL approves and they have been filed with the Secretary of State.

However, in light of the COVID-19 pandemic, Governor Gavin Newsom gave the OAL an additional sixty days to review the regulations, and so far the OAL has not issued a decision. While this means the proposed regulations may not become enforceable until as late as October 1, 2020, companies are not off the hook entirely. The Attorney General has made it clear that his office will not wait for an OAL decision to begin enforcing the "four corners" of the Act itself.

What Has Happened Since July 1, 2020?

Keeping to his promise to begin enforcement without any delays, the Attorney General has already issued an initial round of notice letters to companies suspected of being in violation of the CCPA. The notices give these companies 30 days to cure the violation and come into compliance to avoid further enforcement action.

Given that these notices were sent to companies across all sectors, it does not appear that the Attorney General is targeting any specific industry. Rather, in determining which companies would receive a notice, the Attorney General has been looking in part at social media sites and other publically-available information for companies that have already been the subject of consumer complaints relating to the difficulty in exercising privacy rights under the CCPA.

In addition to sending out notices, the Attorney General has also published a set of Frequently Asked Questions on its website. The FAQs provide general consumer information about the CCPA divided into seven main categories: (1) general information, (2) the right to opt-out of sale, (3) the right to know, (4) required notices, (5) the right to delete, (6) the right to non-discrimination, and (7) data brokers.

While the FAQs are geared toward consumers, they also summarize key obligations businesses have under the CCPA and California's related data broker law:

- **Businesses Subject To The CCPA:** The CCPA applies to for-profit businesses that do business in California and either (i) have a gross annual revenue of over $25 million, (ii) buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices, or (iii) derive 50% or more of their annual revenue from selling California residents' personal information.
- **Right To Opt-Out Of Sale:** If a consumer requests that a business stop selling his or her personal information ("opt-out"), the business must stop and wait at least 12 months before asking the consumer to opt back in to the sale. Furthermore, businesses can only sell a child's personal information if they get affirmative authorization from the child, unless the child is under 13, in which case, the authorization must come from the child's parent or guardian.
- **Right To Know and Right To Delete:** Businesses must respond within 45 calendar days to a consumer's request to know what personal information has been collected, used, shared, or sold about him or her and why, as well as a consumer's request to delete such information. Businesses can extend that deadline by another 45 days if they provide notice to the consumer.
- **Required Notices:** Businesses must provide a notice of collection to consumers that (i) lists the categories of personal information they collect about consumers and the purposes for which they were used, and (ii) contains a link to their privacy policy. If the business sells a consumer's personal information, the notice of

collection must include a Do Not Sell button.

- **Right To Non-Discrimination:** Businesses cannot deny goods or services, charge a different price, or provide a different level of quality of goods or services just because a consumer has exercised his or her rights under the CCPA.
- **Data Brokers:** Data brokers are CCPA-covered businesses that collect and sell consumers' personal information to a third party but do not have a direct relationship with consumers. Data brokers must register on the Attorney General's public data broker registry by January 31 following each year in which the business meets the definition of a data broker.

What Should Companies Be Doing?

Regardless of when the implementing regulations take effect, covered businesses should ensure that public-facing steps towards compliance—including notices at collection, privacy policies, and the "Do Not Sell My Personal Information" (DNS) button (where applicable)—are posted, accurate and up to date. While the Attorney General has not officially addressed whether the companies that have received notices were targeted because of violations relating to the DNS button, the Deputy Attorney General has made clear that the DNS button is an important part of the CCPA and companies should be sure to include it on their websites immediately if they sell personal information of California residents. Determining whether any of the company's data sharing rises to the level of a "sale" of personal information is one of many compliance items that requires advice from an experienced legal advisor given the CCPA's expansive definition of that term and related regulatory risks.

Authors:

Travis P. Brennan
949.725.4271
tbrennan@sycr.com

Mayant Luk
949.725.4057
mluk@sycr.com