**Privacy Alert**
July 2021

# Updates From California: Enforcement of Global Privacy Control Begins, New Consumer-Led Enforcement Tool Launches, Investigations Are Underway

California's Attorney General is taking affirmative steps to make it clear that businesses that collect personal information from consumers must honor "do not sell my personal information" requests made through user-enabled global privacy controls, both through updates issued within the past week to its guidance on the California Consumer Privacy Act (CCPA), and through enforcement letters reportedly sent directly to businesses. At the one-year mark for enforcement, Attorney General Rob Bonta also reported on his office's enforcement efforts and announced the launch of a new online Consumer Privacy Tool that allows consumers to directly notify businesses when they are in violation of the CCPA.

## Key Takeaways:

- California continues to move the goal posts on privacy; companies should be prepared for updates and initiatives that require additional implementation.
- Although the text of the California Privacy Rights Act (CPRA) suggests that responding to the Global Privacy Control (GPC) will be optional in 2023, the California Attorney General will require companies to respond to GPC signals now.
- California's new Consumer Privacy Tool will allow consumers to send cure notices directly to companies.
- Enforcement examples confirm that the California Attorney General is looking for clear and conspicuous "Do Not Sell My Personal Information" links (attempts to get consent to data sharing in lieu of that link will not suffice).

## Global Privacy Controls

The CCPA gives consumers more control over the personal information that businesses collect, including the right to opt out of having their personal information sold. Businesses must offer at least two ways for consumers to submit requests to opt out of the sale of their personal information—one of which is a "Do Not Sell My Personal Information" link. In updated Frequently Asked Questions (FAQs), the California Office of the Attorney General notes that one acceptable method for consumers to opt out is through a user-enabled global privacy control like the aptly named GPC.

While the CCPA does not specifically reference methods for global opt-outs or global privacy controls, the statute directs the Attorney General to adopt regulations that would "facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information." Section 999.315(c) of the CCPA regulations requires businesses that collect personal information to "treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's

*Attorney Advertising*

choice to opt-out of the sale of their personal information as a valid request ... for browser or device, or, if known, for the consumer." The CPRA, which goes into effect in January 2023, suggests that responding to the GPC will be optional, however.

From the consumer perspective, the GPC, which the FAQs describe as a "stop selling my data switch," is a feature consumers can enable on a number of internet browsers, including Mozilla Firefox, DuckDuckGo and Brave, or download as a browser extension.

From a technology perspective, the GPC is a proposed technical standard, still in development, that is designed to be a one-step mechanism to communicate opt-out requests across websites, browsers and devices. Different forms of the mechanism are likely to be developed as the loose coalition of developers from organizations including technology and media companies, publishers, foundations and at least one university works with the technical standard.

The Attorney General's Office is also reiterating its position, as stated in the FAQs, that the GPC is "a valid consumer request to stop the sale of personal information" that businesses covered by the CCPA must accept, by reportedly sending letters to at least 10 and as many as 20 companies calling on them to honor GPC opt-outs. There is little information at the moment as to what prompted the letters and which companies received them.

## New Consumer Privacy Tool

The new online Consumer Privacy Tool, launched July, allows consumers to directly notify businesses when they are in violation of the CCPA, asking guided questions to walk consumers through the basic elements of the CCPA before generating a notification that the user can then email to the business. According to the Attorney General, the email may trigger the 30-day period for the business to cure its violation of the law, which is a prerequisite to the Attorney General's bringing an enforcement action.

## Updates on Enforcement

Enforcement of the CCPA began one year ago. Bonta recently reported that 75% of businesses that have received notices have come into compliance within the 30-day statutory cure period. Of the remaining 25% of businesses that have received notices of alleged violation, most are within the 30-day cure period; a handful are under active investigation.

The Attorney General gave the following examples of notices to cure:

- A grocery chain required consumers to provide personal information in exchange for participation in its company loyalty programs. The company did not provide a Notice of Financial Incentive to participating consumers. After being notified of alleged noncompliance, the company amended its privacy policy to include a Notice of Financial Incentive.
- A social media app was not timely in responding to CCPA requests, and users publicly complained that they were not receiving notice that their CCPA requests had been received or effectuated. The business explained its response processes and submitted detailed plans showing that it updated its CCPA consumer response procedures to include timely receipt confirmations and responses to future requests.
- An online dating platform that collected and sold personal information did not have a "Do Not Sell My Personal Information" link on its homepage and disclosed that a user's clicking an "accept sharing" button when creating a new account was sufficient to establish blanket consent to sell personal information. After being notified of alleged noncompliance, the business added a clear and conspicuous "Do Not Sell My Personal Information" link and updated its privacy policy with compliant sales disclosures.

## Related Professional

Jessica B. Lee . . . . . jblee@loeb.com



6701 REV1 07-21-2021