Small Updates from the California Attorney General Create Major CCPA Impacts

Article By
Heather A. Antoine
Jeremy Beutler

Stubbs Alderton & Markiles, LLP

Related Practices & Jurisdictions

- Administrative & Regulatory
- Communications, Media & Internet
- Corporate & Business Organizations
- Election Law / Legislative News
- California

Monday, July 26, 2021

In an effort to help consumers bring concerns of noncompliance with the California Consumer Privacy Act (CCPA) to covered businesses, the California Attorney General has created a tool to assist consumers with drafting notices of noncompliance that can be sent to businesses that may have violated the CCPA. The California Attorney General has stated that the submission of a notice of noncompliance created through the tool may trigger the 30-day cure period under the CCPA. That means that if a business does not address the alleged noncompliance in 30 days, the California Attorney General may bring suit and seek civil penalties or an injunction.

In addition, at the end of last month, the Office of the California Attorney General updated guidance that address a consumer’s right to opt-out of the sale of their personal information under the CCPA. The guidance now requires that companies
Consumer Privacy Interactive Tool

On July 17, 2021, the California Attorney General released a tool that is designed to help consumers draft noncompliance notices to send to businesses that may have violated the CCPA. The tool is currently limited to generating notices for violations that consist of failing to post easy-to-find “Do Not Sell My Personal Information” links. The California Attorney General intends to broaden the functionality of the tool to include other potential CCPA violations in the future. By answering a handful of questions, the tool generates a draft noncompliance notice that consumers can send to the allegedly non-compliant business.

Remarkably, the California Attorney General has stated that the consumer’s noncompliance letter “may satisfy” the notice requirement under the CCPA that triggers the 30-day period for businesses to cure violations of the law. If the business does not resolve the alleged noncompliance in that period, the California Attorney General may bring suit seeking penalties of up to $2,500 for each violation and up to $7,500 for intentional violations.

Before the California Attorney General’s statement that consumer notices may trigger the cure period, many commentators assumed that a notice triggering the 30-day cure period had to come from the California Attorney General, not consumers. This is because, outside of a relatively narrow exception to bring suit in the event of a data breach, there is no consumer private right of action under the CCPA. Instead, the California Attorney General is responsible for enforcing the law.

Under a section titled “Attorney General Enforcement,” the CCPA provides that a business is not technically in violation of the CCPA until “it fails to cure any alleged violation within 30-days after being notified of alleged noncompliance.” Although the quoted statement does not identify who must provide such notice, most presumed that the notice had to come from the California Attorney General. Not so, however, under the California Attorney General’s interpretation of the law. Based on the California Attorney General’s statement issued with the release of the Consumer Privacy Interactive Tool, it seems that notice triggering the 30-day cure period may be provided by consumers.

This, of course, poses significant concerns for businesses: the Consumer Privacy Interactive Tool may be used by persons untrained as attorneys to decide whether the law applies to a particular business and whether the business is in violation. Moreover, consumers may use the tool to generate and send voluminous or frivolous notices to businesses.

Regardless of these concerns, the California Attorney General’s statement should be taken seriously by businesses: a consumer notice of noncompliance should be investigated, resolved, and responded to as quickly as possible and, in any event,
within 30 days to ensure the business resolves the issue within the cure period.

Notably, the cure period appears to have allowed many businesses to address alleged violations and avoid penalties: in a recent press conference, the California Attorney General stated that 75% of companies that received a CCPA noncompliance notice (presumably from the Office of the California Attorney General) addressed the noncompliance within the cure period. The other 25% were either within the 30-day cure period or were under active investigation.

The GPC Guidance

When the CCPA came into effect on January 1, 2020, it provided California consumers with the right to opt-out of the sale of their personal information, including by requiring that businesses provide consumers with a link titled “Do Not Sell My Personal Information” that enabled consumers to submit such opt-out requests. Although the CCPA did not address tools such as the GPC, the California Attorney General later adopted implementing regulations that required businesses to treat “user-enabled global privacy controls” as a signal of the consumer’s choice to opt-out of the sale of their personal information. When those regulations were initially proposed, a global privacy opt-out mechanism did not exist. However, in response to the regulations, the set of organizations behind the GPC launched the GPC specification in October 2020 as a “user-enabled global privacy control.” Since then, the GPC has been adopted by millions of users, and a handful of publishers and consent management platforms now honor the GPC.

In late June, the California Attorney General updated its CCPA Frequently Asked Questions (FAQs) to address the GPC. The FAQs require that the GPC “be honored by covered businesses as a valid consumer request to stop the sale of personal information.” To the extent honoring the GPC was optional or dependent on development of a widely adopted global user privacy opt-out mechanism, the update to the California Attorney General’s guidance makes clear that it is now mandatory to recognize and treat the GPC as a consumer request to opt out of the sale of the consumer’s personal information.

Companies subject to the CCPA should start making updates now to recognize and honor the GPC. Under the updated FAQs and CCPA regulations, businesses must recognize the GPC as a valid opt-out request for the browser, device, or, if known, the consumer. For example, if a visitor to a company’s website is using the GPC—and even if the specific identity of the user is not known to the company—the website should treat the GPC as an indication that the consumer opts-out of the use of targeted advertising cookies and similar technologies that may involve the “sale” of personal information under the CCPA. To the extent a company is able to identify the user (such as if the user logs into an account through the website), the company should consider the feasibility of treating the GPC as a sale opt-out request just like it would a request submitted through the “Do Not Sell My Personal Information” link.