Published on *The National Law Review* https://natlawreview.com

California Attorney General Announces First CCPA Enforcement Action

Article By:

Steven M. Millendorf

Eileen R. Ridley

On August 24, 2022, California Attorney General Rob Bonta announced a settlement with Sephora, Inc. that included a fine of $1.2 million for alleged violations of the California Consumer Privacy Act (CCPA). The settlement is likely the first of many enforcement actions stemming from the Attorney General's enforcement sweep against online retailers and other businesses for potential violations of the CCPA, which began in June 2021. While other investigations have focused on the failure to disclose financial incentives for loyalty programs, privacy disclosures that are not understandable to the average consumer and do not include required information, and "Do Not Sell My Personal Information" links that only worked on some internet browsers, the enforcement action against Sephora is especially important to many website operators because it hinged on the allegation that Sephora failed to disclose the sale of personal information or provide a "Do Not Sell My Personal Information" link as a result of the use of analytics and advertising cookies on its website.

The Complaint

The Attorney General's complaint alleges that Sephora's website collects personal information (as defined in the CCPA) such as the products that consumers view and purchase, geolocation data, cookies and other unique identifiers, and information about the consumers' operating systems and browsing types. It further alleges that Sephora makes this personal information available to third parties to receive advertising and analytics services through the installation or use of trackers such as cookies, clear-gifs, and other technologies which automatically transmit the personal information.

The complaint states that while Sephora's privacy notice accurately disclosed the fact that it shared geolocation and other electronic network information with third parties such as advertising networks, business partners, and data analytics providers, such a disclosure in exchange for services from those entities constituted a "sale" under the CCPA. The CCPA defines a "sale" of personal information to include a disclosure for monetary or other valuable consideration. The complaint alleges that Sephora's use and transmittal of the personal information was a "sale" under the CCPA because the disclosure was made in exchange for free, discounted, or higher quality advertising or analytics services from its third-party vendors.

Having concluded that Sephora did engage in a "sale" of personal information as defined in the CCPA, the complaint further alleges that Sephora failed to disclose this sale in its privacy notice and instead claimed that it did not sell personal information. Furthermore, the complaint alleges that Sephora failed to offer a "Do Not Sell My Personal Information" link or comply with an opt-out browser signal (in particular the Global Privacy Signal or GPC). While the complaint claims that the Attorney General notified Sephora on June 25, 2021 of the potential violations, Sephora failed to cure the deficiencies on the website in the 30-day cure period required under the CCPA. As a result of Sephora's alleged failure to cure the deficiencies, the Attorney General's complaint alleged violations of not only the CCPA but also California's unfair and deceptive practices statute, California Business and Professions Code § 17200, *et seq.,* for allegedly unfairly depriving consumers of their right to opt-out of the sale of personal information.

The Settlement

Under the settlement, Sephora is required to pay (to the Consumer Privacy Fund) a fine of $1.2 million. In addition, Sephora must:

- Update its privacy notice to clearly state that it sells personal information and that consumers have the right to opt-out of these sales. Sephora must also update its privacy notice to comply with the California Privacy Rights Act (CPRA) with respect to "sale" or "sharing" when it becomes effective.

- Process requests to opt-out of the sale of personal information, including through the use of the GPC.

- Implement and maintain a program to assess, test, monitor, and report to the Attorney General on its activities relating to the sale of personal information, disclosures to service providers and other third parties, and compliance with the GPC. These must generally be implemented within 180 days of the effective date of the settlement and must continue for 2 years.

- Ensure its disclosure to "service providers" are pursuant to agreements that meet the contractual requirements described in the CCPA and implement any "restricted data processing" configurations that may be necessary to adopt such contractual requirements with some third parties (such as Google and Facebook).

Impact to Businesses

The settlement is important because it makes clear that the use of analytics, advertising cookies, and other automatic data collection technologies are a "sale" under the CCPA and will be considered a "sale" or "sharing" under the upcoming CPRA. The settlement also makes it clear that, although the GPC is not widely adopted and there may be other signals sent by browsers in the future, the Attorney General considers it mandatory to comply with the GPC if it is sent.

The enforcement action and settlement should also put to rest any belief that the Attorney General would be less than robust in its enforcement of the CCPA, and instead indicates that the Attorney General has been and continues to actively enforce the CCPA. The inclusion of claims that Sephora violated California Business and Professions Code § 17200, *et seq.,* also suggests that the Attorney General is willing to allege all potential causes of action above and beyond the CCPA itself in order to

enforce compliance.

While the Sephora settlement focusses on the use of cookies, the Attorney General's press release and prior statements on enforcement suggest that the Attorney General is willing to bring enforcement actions on other activities that it believes violates the CCPA, including unclear and incomplete privacy notices, technological issues that may deprive consumers of their ability to exercise their privacy rights, and disclosures to third-parties without appropriate contractual limitations for that third-party to be considered a service provider.

In light of this settlement and other enforcement actions disclosed by the Attorney General, businesses that are subject to the CCPA (and the upcoming CPRA) should immediately review their CCPA compliance to minimize being a potential target of further enforcement actions, including:

- Review the use of any cookies or other similar technologies for analytics, advertising, and other similar services that may be a "sale" under the CCPA.
- Ensure that privacy notices properly disclose any potential "sale" of personal information and the method that consumers may use to opt-out of such sales – particularly including disclosure of the use of personal information for advertising analytics, etc.
- Ensure that privacy notices properly disclose any activities (including loyalty programs) that may be considered a "financial incentive" and provide all required information about the financial incentive, including how the value of personal information is determined and how someone can opt-in or opt-out of the financial incentive program.
- Review agreements with third parties to ensure that all required CCPA terms and conditions are included and consider any such disclosure to be a "sale" of personal information subject to the right to opt-out of such sales.
- Implement a "Do Not Sell My Personal Information" link if any disclosures of personal information to third parties may be considered a "sale" under the CCPA.
- Ensure that the website recognizes and properly processes any GPC signal or other similar privacy control signal sent by a browser.
- Review privacy notices to ensure that they are clear and understandable to the average consumer. Businesses may wish to avoid "one size fits all" privacy notices for products and services that may be confusing to consumers in favor of tailored privacy notices for each product and services. Businesses should also be diligent regarding reviewing any claims that information is not sold.

Businesses should also be on the lookout for notices from the California Attorney General alleging violations of the CCPA. The Attorney General's announcement stated that he sent out notices to other businesses alleging non-compliance with opt-out requests made by global privacy controls. Under the CCPA, businesses have 30 days to cure such violations. The Sephora settlement suggests businesses that receive such notices should take immediate action to cure any alleged deficiencies and that the Attorney General is willing to bring enforcement actions against businesses who fail to take action to comply.

Businesses should also be aware of changes to their processing of personal information required under the California Privacy Rights Act, which goes into effect January 1, 2023. This may include complying with requests by consumers to exercise their additional privacy rights, such as the right to limit the use of sensitive personal information or the right to correct their personal information. Businesses should also be reminded that the employment information and business-to-business information exceptions will expire on January 1, 2023 unless one of the several pending bills are passed by August 31, 2022 – which appears unlikely. If those provisions expire, the full scope of the CPRA will be applicable to both employer and business-to-business information. For more information about additional requirements under CPRA, please see our discussion of this upcoming law at California Voters Pass the California Privacy Rights Act.

Finally, with greater enforcement by the Attorney General and the coming implementation of CPRA in January 2023, there is a greater risk of civil litigation being filed against businesses if they fail to comply with both the CCPA and CPRA. Thus, a diligent review of business practices regarding privacy notices, privacy policies, and the use of consumer information is critical to limit any potential exposure under the CCPA, CPRA, or the Business and Professions Code 17200, *et seq.*

National Law Review, Volume XII, Number 238