DAVIS GILBERT

Privacy + Data Security

First CCPA Enforcement Action's $1.2 Million Fine to Sephora is a Wakeup Call for the Ad Tech Industry

The Bottom Line

- The first substantial CCPA enforcement action should be a wakeup call for the advertising industry.
- California is aggressively policing the industry and looking closely at the third-party tracking mechanisms used on sites.
- With the CPRA just around the corner, more enforcement actions are likely.

The California Attorney General announced that a $1.2 million settlement was reached in the first-ever California Consumer Privacy Act (CCPA) public enforcement action, brought against prominent retailer Sephora.

The Attorney General alleged that Sephora failed to provide its customers with sufficient notice of the sale of personal information; failed to provide a "Do Not Sell My Personal Information" link, as required by the CCPA; failed to provide two or more methods to opt-out of such sale; and, significantly, failed to process requests to opt-out via user-enabled Global Privacy Controls (GPC). The settlement, which included the significant fine, was announced Aug. 24.

Third Party Trackers – Sale of Personal Information

The enforcement action focused largely on Sephora's use of third-party tracking pixels on its website. When a website allows other parties to collect personal information, such as data generated via cookies, the data transfer from the website (a "Business" under the CCPA) to such other parties is either

1. a transfer of data to a "Service Provider" under the CCPA, which must be evidenced by a contract that documents the service provider relationship or
2. a sale of personal information to a "Third Party" under the CCPA, which requires the business to notify consumers

> of such sales and provide them with an opportunity to opt-out through a "Do Not Sell My Personal Information" link on the homepage and two or more methods for submitting such opt-out requests.

Sephora failed to meet either standard. The company's privacy policy stated that it did not sell personal information, but it did not have service provider agreements in place. Therefore, the data transfers must be considered sales of personal information, and the CCPA obligations when selling personal information were not put in place.

Global Privacy Controls Signals

The Sephora settlement is particularly notable given its emphasis on the treatment of GPC signals. The CCPA does not mention GPC or user-preference signals in the law itself. The Attorney General first introduced the issue in the regulations disseminated as required by the CCPA, stating:

> "If a business collects personal information from consumers online, the business shall 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 choice to opt-out of the sale of their personal information."

While advertising industry members have lacked clarity about compliance obligations due to an absence of standards and confusion over what it means to be "user-enabled," the Attorney General clearly takes a fairly aggressive approach and believes there is no ambiguity.

The California Privacy Rights Act (CPRA/aka "CCPA 2.0"), which takes effect Jan.1, specifically mentions "opt-out preference signals." While the law implies that honoring such signals is an option for compliance with opt-out requests, the draft version of the CPRA regulations released on May 27 clearly states that "[a] business shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing." The Sephora settlement sends a clear message: Entities subject to the CCPA and CPRA need to process GPC signals as opt-out requests *now*.

Sensitive Data

Adding gasoline to the fire, the Attorney General was further motivated to act because Sephora's website, while allowing such tracking without complying with the CCPA, also allowed consumers to browse and purchase products such as prenatal and menopause support vitamins. Regulators and lawmakers have heightened their focus on the collection of sensitive personal information online.

Conclusion

The Attorney General's complaint uses inflammatory language, such as "surveillance," when describing online tracking – clearly indicating that regulators do not have a favorable view of third-party data collection through websites. The CCPA has a 30-day cure period during which a company may address alleged violations of the law; however, that cure period did not resolve this matter. The CPRA does away with that cure period.

The settlement sends a strong message to retailers and entities subject to the CCPA: Comply now or risk substantial fines. In the settlement, Sephora agreed to notify its customers that it sells their data, provide its customers with the right to opt-out of that sale and honor GPC signals going forward.

For More Information

Please contact the attorneys listed below or the Davis+Gilbert attorney with whom you have regular contact.

Gary Kibel

Partner
212 468 4918
gkibel@dglaw.com

Emily Catron

Associate
212 468 4857
ecatron@dglaw.com