First CCPA Enforcement Action by the California AG – Lessons Learned

September 8, 2022

The California Privacy Rights Act (CPRA) and other new state data privacy laws are set to take effect in 2023. If you needed an incentive to review your compliance obligations, the California Attorney General recently provided one in its $1.2 million settlement of an enforcement action under the California Consumer Privacy Act (CCPA), upon which the CPRA expands. Anyone with an e-commerce website should take heed.

Summary of the Enforcement Action. According to the California AG, Sephora, a French cosmetics brand, failed to disclose to consumers it was "selling" (a broadly defined term under the CCPA) their personal information; failed to honor user requests to opt out of sales via a user-enabled Global Privacy Control; and failed to cure these violations within the 30-day period allowed by the CCPA. In addition to the settlement amount, Sephora promised to report to the AG on its changes to its privacy regimen for a period of two years.

Sephora was sharing personal information of their customers with third-party advertising networks and analytics providers, as do most businesses conducting e-commerce. These providers, in turn, allowed Sephora to learn what kind of device customers were using, what was in their shopping carts, and their precise locations.

The California AG found a "sale" under the CCPA because Sephora gave these vendors access to its consumer data so it could receive free or discounted analytics and other advertising benefits, including "the valuable option to serve targeted advertisements to the same shopper on the analytics provider's advertising network."

The AG further determined that these "sales" triggered Sephora's obligations to inform consumers about the "selling" of their information and their opportunity to opt-out of the sales through a "Do Not Sell My Personal Information" button on the company's website.

California AG Office Release: https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement

Takeaways from the Enforcement Action. We now have a better idea of what the California AG considers "sale" of personal information under the CCPA, and what triggers a company's "do not sell" compliance obligations under the law. Here are our key takeaways from the Sephora settlement:

1. **Evaluate "Sharing" vs. "Selling" Personal Information.** Given that the AG considers "sales" to include the sharing of personal information with the Googles, Facebooks and other analytics companies of the world, you should look at who benefits from these arrangements. If the analytics company benefits from the exchange, then you may have a CCPA "sale" on your hands, in which case you need to reconsider your privacy policy and vendor agreements regarding consumer data.
2. **Review your Cookies.** Know what personal information you are collecting. Review your cookie policy and document the presence of any third-party cookie, pixel, or SDK on your website or mobile app.
3. **Update your Service Provider Agreements.** The California AG noted that the alleged "sale" of personal information by Sephora could have been cured by having "valid service-provider contracts in place with each third party." If you use vendors for analytics or ad targeting, make sure you have appropriate agreements restricting use of the consumer data and prohibiting uses that benefit the vendor or its other customers. Also, if you separately purchase the analytics services in exchange for money, independent of the sharing of data, it could arguably not be a "sale," although the California AG may not agree with that approach.
4. **Become Familiar with the Global Privacy Control.** The GPC acts as a global one-stop-shop mechanism to opt-out of data sales. The California AG has endorsed it, asserting that "[t]echnologies like the Global Privacy Control are a game changer for consumers looking to exercise their data privacy rights." The AG specifically noted Sephora's failure to recognize GPC as an opt-out request. If your website and cookies treat GPC requests as do-not-sell signals, you will be in accord with the AG's expectations. It is not a panacea, however, as it is unclear whether browsers can accept the GPC opt-out by default or if affirmative action by a consumer is needed to enable the signal.
5. **Do Not Ignore the California Attorney General.** The CCPA has a 30-day cure period. Sephora's failure to respond to the California AG's notice of non-compliance prompted the enforcement action. If you receive a notice of non-compliance, take timely steps to address the alleged problem.
6. **Operationalize Compliance**. Now is a great time to make sure you fully comply with the CCPA and CPRA. Re-evaluate your privacy policies and notices for accuracy. Confirm you have appropriate data rights request processes in place. Review your websites and mobile apps, especially those that contain third-party trackers or other adtech solutions, to make sure they are adequately configured to monitor for and honor user-enabled opt-out preference signals, such as the GPC.

We will continue to monitor all global, federal, and state data privacy laws and enforcement actions and keep you informed of any suggested compliance activities.