SEPHORA'S PAST PRIVACY PRACTICES PRECIPITATE $1.2 MILLION PAYMENT

Ben Barnes

Eliza Davis

On August 24, 2022, California Attorney General Rob Bonta announced that his office had reached a settlement with Sephora to resolve claims that Sephora's use of third-party tracking violated the California Consumer Privacy Act (CCPA). This is the first ever privacy enforcement action by California for violations of the CCPA. This settlement serves as an example of how California will pursue enforcement actions for violations of the CCPA and California Privacy Rights Act (CPRA) in the future and a wake-up call for companies to review their practices to ensure compliance.

Background:

The Office of the Attorney General (OAG) alleged in its complaint that Sephora allowed third party companies to install trackers on its website and mobile apps. These trackers enabled the third parties to track the activity of Sephora customers. The third party providers would then match the user activity collected from Sephora's website and apps with data they collected from other sources to assist Sephora with identifying potential customers and sending targeted advertisements to them.

The OAG claimed that because Sephora received data about their shoppers in exchange for providing customer data to the analytics providers, this transaction constituted a "sale" under the CCPA. In addition, the OAG also alleged that Sephora violated the CCPA because its website did not disclose this exchange of information. In fact, the OAG alleged that Sephora's site did the opposite and told Californians that "we do not sell personal information."

The OAG argued in its complaint that allowing third parties to collect personal information via cookies constituted a sale of personal information and this sale triggered obligations for Sephora to provide consumers the choice to opt-out of the sale and to post a "Do Not Sell My Personal Information" link on its website, home page, and mobile apps. In addition, Sephora was required to detect and process opt-out signals sent by browsers where consumers had enabled the Global Privacy Control (GPC). Sephora did not take any of these required steps.

Without admitting any liability, Sephora settled and agreed to pay a $1.2 million fine. In addition, Sephora must:

- Clarify its online disclosures and privacy policy to include an affirmative representation that it sells data;
- Provide mechanisms for consumers to opt out of the sale of personal information, including via the GPC;

- Confirm its service provider agreements adhere to the CCPA's requirements;
- Conduct assessments of its processing of consumer requests to opt out of the sale of their information; and

Provide reports to the OAG related to sale of personal information, status of service provider relationships, and its efforts to honor GPC.

Key Implications:

- **Take advantage of "cure"**: Sephora was notified of the alleged violations and given 30 days to cure. They failed to cure any of the alleged violations.
- **Review compliance with user-enabled global privacy controls**: Sephora's website was not configured to detect or process any global privacy control signals like the GPC. Organizations should also review the privacy controls on mobile applications as well.
- **Strong statement to businesses:** Comply with the CCPA or pay a hefty price.
- **Review statements, disclosures, and policies:** Companies should periodically review statements, disclosures, and policies to ensure compliance with changing privacy regulations. The OAG alleged that Sephora's policy stated, "we do not sell personal information" and yet shared personal information with third parties.

Review analytics: Sephora implemented a widely-used analytics and advertising software package. Despite Sephora not getting paid for this information, the use of analytics constituted a "sale" under the CCPA as Sephora received value for providing information about their customers.

Looking Ahead:

The Sephora settlement demonstrates what CCPA settlements might look like in the future. Notably, Sephora was given the opportunity to cure, which it failed to do. That opportunity to cure disappears when the CPRA goes into effect on January 1, 2023. This first privacy enforcement action and settlement is a shot across the bow for companies to get things in line. It is critical that covered companies take the time now to ensure compliance with the CCPA and CPRA. Simply reviewing statements, disclosures, policies, and vendor agreements could prevent companies from facing hefty fines.

For assistance with or additional information on this topic, please contact Martin Tully at mtully@redgravellp.com or Eliza Davis at edavis@redgravellp.com.