Proskauer

Message Sent! California Attorney General Announces $1.2 Million CCPA Settlement with Retailer and Its Focus on the Sale of Customer Information

Proskauer on Privacy Blog on **August 25, 2022**

On August 24, 2022, California Attorney General (AG) Rob Bonta announced a settlement with beauty products retailer, Sephora USA, Inc. ("Sephora"), resolving claims that Sephora violated the California Consumer Privacy Act (CCPA) for, among other things, failing to disclose to consumers that it was selling their personal information (including precise location data) and failing to honor opt-out requests via global privacy controls (GPC) broadcasted from users' web browsers. The proposed settlement has been submitted to a California state court for approval.

This settlement is noteworthy in that it is the AG's first CCPA enforcement action. After releasing the final proposed CCPA regulations in June 2020, businesses were given notice that enforcement would begin on or after July 1, 2020 (even as regulations were still being finalized, with additional amendments released in March 2021; rulemaking authority has since been assumed the California Privacy Protection Agency, which was established by the California Privacy Rights Act of 2020). Since that time, the AG has released a host of CCPA enforcement case examples that offered basic information about various situations where the AG had sent a notice of CCPA noncompliance to a covered entity, which then remedied the purported violation within the 30-day cure period currently allowed under the statute. The Sephora settlement is the first enforcement and monetary settlement involving the AG over alleged CCPA violations.

According to the AG's complaint, Sephora allegedly installed third-party tracking technology on its website and mobile app that monitored and profiled user activity (including precise location data) to assist Sephora with ad targeting. The complaint alleges that the consumer data was packaged and sold by the third-party data company to other businesses. The AG stated, "if companies make consumer personal information available to third parties and receive a benefit from the arrangement—such as in the form of ads targeting specific consumers—they are deemed to be "selling" consumer personal information under the law" and are required to give notice to the customers.

The complaint alleged that Sephora did not provide consumers with a clear and conspicuous "Do Not Sell My Personal Information" link (or two or more designated methods for submitting opt-out requests). The complaint also asserted that Sephora allegedly failed to process GPCs or "user-enabled global privacy controls" that gives consumers the option to universally opt-out of all online sales with just an adjustment to their web browsers. After being informed of these alleged violations, the AG claimed that Sephora failed to cure within 30 days, prompting the AG investigation that led to this settlement.

Under the proposed settlement, Sephora agreed to pay $1.2 million in penalties and comply with various injunctive relief, agreeing to:

- Provide notice to consumers that it sells personal information and that consumers have a right to opt-out;
- Provide consumer opt-out requests made via GPC;
- Conform its service provider agreements to the CCPA's requirements; and
- Implement a compliance program surrounding CCPA opt-out requests and provide an annual report to the CAG for a period of two years relating its compliance regarding its sale of personal information and compliance with CCPA opt-out requests, the status of its service provider relationships, and its efforts to honor GPC.

Messages the AG Hopes Businesses Receive

First, the AG is focused on the use of data tracking and what it calls "commercial surveillance" (including the sale of precise location data) that generally occurs without the full understanding of consumers. The language used by the AG echoes terms used by the Federal Trade Commission (FTC) in its recent Advance Notice of Proposed Rulemaking regarding potential trade regulations limiting commercial surveillance practices, among other things. While comprehensive, bipartisan federal data privacy legislation (e.g., the so-called ADPPA) remains in the U.S. Senate, data privacy enforcement continues to be a priority for the states (and the FTC).

Second, the enforcement and additional announcement that the AG has sent out additional notices to businesses alleging various failures to process consumer opt-out requests made via GPC privacy controls underscores that this particular violation is on the AG's radar.

Third, the illustrative examples of prior CCPA investigations and notices show that the AG is receptive to working with businesses to remedy violations under the 30-day cure period currently allowed under the CCPA. Still, looking ahead, it should be noted that the CCPA's notice and cure provision, which mandates that businesses receive notice of a violation and an opportunity to cure before the CAG can bring an action, will expire on January 1, 2023. Thus, with this grace period soon ending, businesses should reexamine their CCPA compliance to get ready to be operating within the CCPA's requirements on a tightrope of sorts, without a safety net.

View Original