The Sephora Enforcement Action

Following the first California Consumer Privacy Act (CCPA) enforcement action, California-based companies and those targeting California consumers might find themselves scrambling to comply. In this infographic, we'll break down Sephora's role in violating the CCPA and the penalties it incurred so you can better understand things to come.

The violations

SEPHORA FAILED TO:

Treat its transfer of consumer data as a "sale."

Sephora used data tracking technologies on its website that sent consumers' data to external ad tech and analytics companies. But the way Sephora collected and disseminated the information would be considered a sale under the CCPA. That means Sephora was supposed to alert consumers to the sale and give them a choice to opt-out.

Even if it didn't give consumers a chance to opt-out, Sephora also could have been in compliance with the correct contractual provisions in place. Ad tech and analytics vendors would have been considered service providers under the CCPA. Thus, with the right agreements, data transferred to them would not have been considered a sale.

The CCPA was a little unclear regarding its definition of the word "sale." It defined a sale as:

selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means a consumer's personal information for monetary or other valuable consideration.

With this enforcement, the definition becomes clearer. Also, the California Privacy Rights Act (CPRA) now includes "sharing data" in its requirements to provide an opt-out. And it explicitly discusses targeted advertising, or "cross-context behavioral advertising," noting that businesses can only engage in these activities if they have consumer consent and the proper safeguards.

SEPHORA FAILED TO:

Process consumers' opt-outs of that sale as indicated by a universal opt-out signal

While Sephora didn't offer consumers a way to opt-out of the sale of their information via its website, consumers could still opt-out via Global Privacy Control (GPC). This browser extension lets users indicate their privacy preferences once and then applies those preferences to each site they visit.

When users opted out of the sale of their data via GPC, Sephora didn't act on it.

Neither the CCPA nor the CPRA calls out that businesses must honor the GPC — only that companies must honor opt-out requests in general. However, the California Attorney General's office has clarified that this includes universal opt-out signals like the GPC.

According to the California AG 's office, "Opting out of the sale of personal information should be easy for consumers, and the GPC is one option for consumers who want to submit requests to opt-out of the sale of personal information via a user-enabled global privacy control."

SEPHORA FAILED TO:

Address these violations within 30 days

Businesses are often given a cure period (like a grace period) to adapt to newer regulations after enforcement begins. In this case, the CCPA provides a cure period of 30 days after the AG informs a business that it's in violation of the law. Sephora didn't address the issues within the cure period.

The CCPA's right to cure is disappearing as of January 1, 2023, when the CPRA goes into effect (which does not feature a cure period).

The California AG has said that other companies have been found in violation and given the 30-day cure period. Other businesses have addressed their violations in those 30 days. Sephora is the first to not do so.

Sephora's next steps

In addition to paying $1.2 million, the settlement also requires Sephora to take specific actions, including:

- Clarifying that it sells personal information in its online disclosures and privacy policy
- Enable consumers to opt-out of the sale of their personal information, including through universal opt-out signals
- Update its contracts to meet CCPA standards
- Report to the California AG about its efforts to meet the above requirements

Except for the reporting, these actions were all already required by the CCPA.

Becoming compliant with the CCPA

Following the announcement of the settlement, California AG Rob Bonta released this as part of his statement, "I hope today's settlement sends a strong message to businesses that are still failing to comply with California's consumer privacy law. My office is watching, and we will hold you accountable."

If this statement makes you anxious about your business's ability to comply with the CCPA and upcoming CPRA, we can help. Our privacy platform can notify customers about the sale or share of their personal information and honor their consent preferences (including via GPC). What's more, you can feel secure in your compliance knowing that our platform is backed by our No Fines, No Penalties pledge.

Worried about your business's compliance status?
Quickly become compliant with Osano.

Schedule a Demo