Articles + Publications | December 13, 2022

CCPA Enforcement: The Sephora Settlement Is Just the Start

Privacy & Cybersecurity Newsletter

WRITTEN BY

Lindsey E. Kress | Molly McGinnis Stine | Tara L. Trifon

Flexing considerable enforcement muscle, California Attorney General Rob Bonta ("AG") recently announced a $1.2 million settlement with beauty retailer Sephora, Inc. ("Sephora") under the landmark California Consumer Privacy Act ("CCPA").[1] The Sephora Settlement is the first public enforcement action under the CCPA and dramatically highlights several points:

- The AG promises more – and more aggressive – enforcement against non-compliance and partial compliance of all kinds;
- The CCPA's 30-day cure period to resolve statutory violations expires at January 1, 2023 when the California Privacy Rights Act ("CPRA") goes into effect;
- Broad construction of the statutes seems likely, as illustrated by the AG's finding that Sephora's exchange of information constituted a "sale"; and
- The AG is very interested in the Global Privacy Control ("GPC") being used appropriately.

Businesses interacting with California consumers should urgently review their CCPA/CPRA compliance policies and procedures.

The Sephora Settlement.

The AG's settlement with Sephora was announced on August 24, 2022 and resolved allegations concerning violations of the CCPA and the California Unfair Competition Law ("UCL").[2] The complaint alleges that Sephora failed to inform California consumers that their personal information was going to be "sold" when visiting its website and/or mobile application. For example, the AG claims that Sephora failed to inform consumers that they have the right to opt out of the sale of their personal information, failed to display a clear "Do Not Sell My Personal Information" link, failed to provide two or more methods for submitting opt-out requests, failed to treat Global Privacy Control signals as an out-out request, and continued to sell personal information to third parties despite receiving the GPC signal.[3] The complaint further claims that Sephora violated the UCL by "making false and misleading statements of facts concerning Defendants' sale of consumers' personal information and unfairly depriving consumers of the ability to opt-out of the sale."[4]

The Sephora Settlement is worth noting for several reasons. As it is the first public enforcement action involving the CCPA, it offers insight into how the AG interprets the provisions of the CCPA, including the term "sale." The AG specifically alleges that Sephora provided its third party business partners with access to customer data in

exchange for advertising or analytic services. The AG posits that these exchanges constitute a "sale" under the CCPA – *i.e.* the exchange of personal information for something of value.[5] While some exchanges with service providers can be exempt from the definition of "sale" under the CCPA, the AG alleges that Sephora did not have "valid service-provider contracts" in place with these third parties such to qualify for the exemption.[6] Instead, the AG found that "Sephora's arrangement with these companies constituted a sale of consumer information under the CCPA, and it triggered certain basic obligations, such as telling consumers that they are selling their information and allowing consumers to opt-out of the sale of their information. Sephora did neither."[7]

It is also worth noting that the Sephora Settlement did not involve a data breach. Rather, the settlement resulted from a broader enforcement sweep in June 2021 in which the AG investigated whether certain large retailers were complying with GPC directives. The GPC investigation led to the AG discovering additional alleged violations by Sephora. The AG claims that his office notified Sephora of the alleged violations on June 25, 2021, but that Sephora failed to cure the identified issues within 30 days.[8]

Aside from the payment of $1.2 million in penalties, the Sephora Settlement also require Sephora to comply with certain injunctive terms. Under the terms of the Sephora Settlement, must: "(1) clarify its online disclosures and privacy policy to include an affirmative representation that it sells data; (2) provide mechanisms for consumers to opt out of the sale of personal information, including via the Global Privacy Control; (3) conform its service provider agreements to the CCPA's requirements; and (4) provide reports to the Attorney General relating to its sale of personal information, the status of its service provider relationships, and its efforts to honor Global Privacy Control."[9]

The AG is Just Getting Started.

The AG has pointedly announced his Office's intent to ramp up enforcement of the CCPA – especially with regard to the obligation to identify and process GPC signals. In a statement posted on the AG website, Bosta states:

Technologies like the Global Privacy Control are a game changer for consumers looking to exercise their data privacy rights. But these rights are meaningless if businesses hide how they are using their customer's data and ignore requests to opt-out of its sale. I hope [the Sephora] 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.*** *It's been more than two years since the CCPA went into effect, and businesses' right to avoid liability by curing their CCPA violations after they are caught is expiring. There are no more excuses. Follow the law, do right by consumers, and process opt-out requests made via user-enabled global privacy controls.*[10]

The AG further confirmed that additional CCPA violation notices were recently sent out to businesses that are not properly processing opt-out requests made pursuant to GPC signals. As the AG explains, "a global privacy control allows consumers to opt out of all online sales in one fell swoop by broadcasting a 'do not sell' signal across every website they visit, without having to click on an opt-out link each time."[11] The AG has repeatedly touted the convenience of these universal opt-out options to consumers and has made it clear that companies that do not comply with these signals or otherwise place undue obstacles on consumers exercising their rights to opt-out of the sale of their personal information will be held liable by his Office.

That said, the AG's interest and focus in enforcing the CCPA expands beyond compliance with

GPC signals. Examples of other notices of violation announced by the AG include: failure to post Notice of Financial Incentives with regard to loyalty programs that offered financial invectives in exchange for collection of consumer's personal information; failure to post required notices concerning CCPA consumer rights; failure to disclose whether the company has sold personal information; failure to displace a clear "Do Not Sell My Personal Information" link; erroneous treatment of requests to know; non-compliant privacy policies; non-compliant opt-out processes; non-compliant service provider contracts; untimely responses to CCPA requests; charging consumers to respond to a request under the CCPA; defective methods to submit requests; and more.

The scope of these violation notices demonstrate that the AG will not accept partial-compliance with the statute. Businesses must ensure they are clearly notifying consumers of their intent to sell personal information under the statute and must provide easy and efficient mechanisms to opt-out of any such sale.

Enforcement Actions Are Expected to Increase With Implementation of CPRA

The 30-day notice and opportunity to cure provided by the CCPA expires when the CPRA takes effect on January 1, 2023. Significantly, the CPRA does not provide for a notice and cure period and instead permits the enforcing entity to order substantial administrative fines (from $2,500 to $7,500 per violation) at the time a cease and desist letter is used, though the "good faith cooperation of the business" can be considered in determining the amount of any administrative fine. Further, the CPRA has a "look back" provision to January 2022 for enforcement purposes. The CPRA also amends and expands the enforcement mechanism of the CCPA through the creation ?of "the Agency," a newly formed California state government agency whose sole purpose is the ?regulation of consumer data privacy.[12] The Agency obtained rulemaking authority of the CCPA effective July 1, 2021, and will oversee ?enforcement of the CPRA effective July 1, 2023. ?

The AG made clear during an August press conference that the "kid gloves are coming off" when the CCPA notice and cure provision expires at the end of year and that his office "will not hesitate to protect consumers."[13] Business should not expect to receive any courtesy notices once the CPRA takes effect. It is therefore imperative that companies review their CCPA/CPRA compliance procedures now and take steps to remedy any issues as soon as possible.

Conclusion

The Sephora Settlement is just the beginning of the AG's aggressive push to protect consumer privacy rights in California. Companies interacting with California consumers should not assume that the CCPA/CPRA does not apply to their business, especially considering the broad interpretation of the "sale of personal information" under the CCPA and the upcoming expiration of the "personnel" and "B2B" exemptions.[14] The Sephora Settlement demonstrates that the AG will interpret statutory privacy protections broadly.

Further, given the AG's intense scrutiny of consumer data privacy compliance, businesses must not only make sure that their policies and procedures comply with the CCPA/CPRA– but also that the policies and procedures are being implemented correctly. This means, for example, routinely monitoring and reviewing opt-out technology to ensure that consumer opt-out requests are promptly (and correctly) processed – including GPC signals. Further, businesses should endeavor to make the opt-out process as streamlined and efficient as possible for consumers.

Given the breadth of the protections provided by the CCPA/CPRA, businesses are best served by adopting an over-compliance approach and assuming that all requirements (and exemptions) will be interpreted in the most consumer-friendly way possible.

***

[1] Cal. Civ. Code § 1798.100 *et seq.*

[2] Cal. Bus. & Prof. Code §§17200 *et seq*.

[3] Complaint filed in *People of the State of California v. Sephora USA, Inc*., San Francisco Superior Court Case No. CGC-22-601380 ("Compl."), ¶¶ 19, 21.

[4] *Id*. ¶ 24.

[5] ?Cal. Civ. Code § 1798.140(t).

[6] Compl. ¶ 13.

[7] https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-?enforcement.

[8] Compl.¶ 16.

[9] https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-?enforcement.

[10] *Id*. (emphasis added).

[11] *Id.*

[12] ? Cal. Civ. Code § 1798.199.10 *et seq.?*

[13] https://www.youtube.com/watch?v=mT8jT8LW8XE.

[14] https://www.lockelord.com/newsandevents/publications/2022/09/californias-looming-privacy-deadline.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber