Articles + Publications | August 30, 2022

Not So Pretty: Five Takeaways from New CCPA Settlement with Sephora and Other Enforcements

WRITTEN BY

James Koenig | Ronald Raether, Jr. | Kim Phan | Brent T. Hoard | Joel M. Lutz | Sadia Mirza | Edgar Vargas | Lissette Payne | Graham T. Dean | Robyn W. Lin

This article was republished in Law360 on September 13, 2022.

With the notice and cure set to expire on January 1, 2023, California Attorney General Rob Bonta (CA AG) provided a glimpse at what to expect with its first settlement of alleged violations of the California Consumer Privacy Act of 2018 (CCPA). That same day, the CA AG also updated its "CCPA Enforcement Case Examples," which provides illustrative examples of situations in which companies were sent a notice of alleged noncompliance and the steps taken by each company. These enforcement cases targeted companies in a variety of industries, including health care services, medical device manufacturers, financial technology, data brokers, clothing retailers, and online advertising. While businesses ramp up compliance with the California Privacy Rights Act (CPRA), which also takes effect January 1, 2023, there are several "lessons learned" that businesses should consider as they plan for compliance.

Background on CCPA. In 2018, California voters enacted the nation's first comprehensive data privacy law, the CCPA. In the midst of the pandemic, CCPA enforcement began on July 1, 2020. Two years later, CA AG Rob Bonta announced the first CCPA settlement with Sephora, resolving allegations that the beauty company violated the CCPA, and provided an updated list of CCPA enforcement case examples.

California v. Sephora, Inc. Beauty company Sephora, Inc. (Sephora) is well known as a one-stop shop for makeup, skin care, and hair care with many retail locations, an online store, and a mobile application. On June 25, 2021, the CA AG notified Sephora that it may be in violation of the CCPA and had 30 days to cure its privacy practices before facing legal liability. Specifically, the CA AG alleged that Sephora:

- Failed to disclose that it sells data;
- Engaged in the unlawful sale of personal information, including by exchanging data with third parties for analytics information;
- Failed to post a "Do Not Sell My Personal Information" link on its website and homepage; and
- Failed to respond to or process consumer opt-outs in accordance with global privacy controls (GPC).

After Sephora allegedly failed to cure its violations within 30 days, the CA AG entered into a tolling agreement on September 14, 2021. On August 24, 2021, the CA AG announced a settlement with Sephora, which included a $1.2 million penalty, two-year monitoring period, additional reporting requirements, and terms requiring Sephora to review its service provider contracts.

Other Enforcement Activity. On August 24, CA AG updated its list of CCPA enforcement case examples. These enforcement cases concerned allegations relating to the following:

- A loyalty program that offered financial incentives without a compliant Notice of Financial Incentive;
- Noncompliant opt-out processes, including an opt-out that required consumers to take additional steps by sending them to a third-party trade association's tool;
- Inadequate privacy policies, including one privacy policy whose hyperlinks did not direct consumers to the relevant section; and
- Failures to properly handle consumer requests.

After receiving notices of alleged noncompliance, the companies cured such noncompliance within 30 days. While the companies are not named, for each CCPA enforcement case example, the CA AG identified the industry of the company, the noncompliance issue, and a summary of the company's response.

Companies Beware: Attorney General No Longer Required to Offer 30-Day Cure Period. It's worth noting that the CPRA, which takes effect January 1, 2023, eliminates the 30-day cure period that currently applies to CCPA enforcement, and instead grants both the CA AG and the California Privacy Protection Agency (CPPA) discretion whether to offer a cure period. When announcing the settlement with Sephora, the CA AG sent a strong message to businesses, indicating that time is running out to comply with the law: "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. 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."[1]

Five Takeaway Lessons. Companies should: (1) consider how they interpret the definition of "sale" and review their service provider contracts; (2) pay attention to any financial incentive programs; (3) consider whether their websites are configured to detect or process any GPC signals; (4) review all CCPA/CPRA disclosures and methods to accept data subject requests to ensure the average consumer can understand them and that they are functioning properly, as well as review all notices, including privacy policies and notices of financial incentives; and (5) test or audit consumer request procedures to determine the adequacy of the company's response.

1. We've Said It Before, Consider the Definition of "Sale" and Review Your Service Provider Contracts. The CCPA's definition of "sale" includes any transfer of personal information to a third party for *monetary or valuable consideration*. In the Sephora complaint, the CA AG alleged that Sephora shared consumers' geolocation data and internet or other electronic network activity information with third parties, including advertising networks,

business partners, and data analytics providers. It was further alleged that Sephora made this data available by installing third-party trackers in the form of cookies pixels, software development kits, and other technologies that automatically sent data about consumers' online behavior to the third-party companies. The CA AG categorized this type of data processing activity "in exchange for services from those entities" as a sale of personal information because: (1) Sephora derived something "of value" from the third-party companies (*e.g.,* as a result of this processing activity, the CA AG alleged that Sephora could learn about a shopper's activities on its websites or in its app); and (2) Sephora did not have valid service-provider contracts in place with each third party, which is one exception to "sale" under the CCPA.

Implementation Tip: Remember when everyone was confused about what may constitute "valuable consideration" under the definition of "sale"? The Sephora complaint provides some insight.

As a result of the allegations against Sephora, businesses would be wise to review their current data practices for any exchange of personal information with a third party that results in a benefit to the company, even if the benefit is not monetary. This review should consider whether the business could defensibly categorize the third party as a service provider — a well-recognized exception to a "sale" — or leverage any other exemption. Where businesses have determined that a third party meets the definition of a "service provider," businesses must take steps to update the vendor contract to align with the CCPA's requirements.

This tip is especially important for businesses that use innovative technology, or if their business model depends on the right to use their client's data for AI or other independent purposes beyond the contract. This often comes up in ad tech, analytics, location services, and the use of other innovative technology.

2. Pay Attention to Financial Incentives. Under the CCPA, financial incentives include any payments, different prices, rates levels, or quality of goods or services for the collection of consumers' personal information. In an "enforcement sweep," the CA AG alleged that multiple businesses operated loyalty programs that offered financial incentives (including product discounts and service differences) for the collection of consumers' personal information without posting a compliant Notice of Financial Incentive. In response, these businesses were required to review the design of their programs (*e.g.,* opt-in and opt-out methods) and the content and placement of their Notice of Financial Incentives.

Notably missing from the CA AG's enforcement example was any discussion about the CCPA's requirement that businesses describe how they "calculate the value of consumer data" — a statutory requirement with which many businesses continue to struggle.

Implementation Tip: Use the CA AG's enforcement case example as a means to audit your own financial incentive programs. The example identifies the "low hanging fruit" for the AG when it comes to financial programs, so businesses should act accordingly. We've made it easy for you with the below checklist:

- Does the organization’s website include links that take consumers directly to the Notice of Financial Incentive, as opposed to the business’s general homepage?

- Is the program designed to capture express opt-in consent?

- Does the program allow consumers to opt out of the program at any time and provide consumers with information on how to do so?

- Does the Notice of Financial Incentive describe how the business uses the personal information it collects as part of the program, such as for the purpose of sale, consumer profiling, or to personalize offers and other marketing?

Financial Incentives Program Audit Checklist

- Has the organization posted a Notice of Financial Incentive in an area where consumers will see it before voluntarily joining the program? Both on-site and online premises account.

3. Implement Procedures and/or Technology to Honor Global Privacy Controls. Global privacy control signals are plug-ins that allow the user to automatically broadcast their cookie preferences to every website they visit. While there was some uncertainty about whether CCPA required recognition of GPC, both the CPRA draft regulations and the Sephora settlement make it clear that California is requiring businesses to recognize these opt-out mechanisms.

Implementation Tip: Businesses should educate themselves on the different platforms, technologies, and mechanisms being developed to send opt-out preference signals. Businesses should also review the draft CPRA rules to understand how to process opt-out signals in a frictionless or non-frictionless manner. Stay tuned for CPPA regulations on the technical specifications for compliance.

4. Thought the CCPA Was Confusing? The CA AG Thinks the Same About Your Privacy Notices, so Revise and Clarify Your Privacy Notices and Test Your Opt-Out Mechanisms. In one enforcement example, the CA AG noted that an online classified advertisements company and an online advertising firm had privacy disclosures that were not easy to read or understandable to the average consumer, and the business’s method to opt out of the sale of information was also confusing and contained dysfunctional links. After being notified of the alleged noncompliance, the business revised its privacy policy to fix the identified violations and hired a user interface designer to improve their opt-out of sale method.

In another example, a wireless network provider received notification that its CCPA portal was not functional and was not accepting consumers’ requests to know what personal information was being collected and to delete that information. In response, the business explained the steps it had taken to ensure that its online CCPA portal was functional.

Implementation Tip: This example demonstrates that businesses are not only being judged on what information they provide to consumers, but also how such information is relayed. Notices should be written, so they can be

understood by the average consumer, and links to notices or data subject request portals should be periodically audited to ensure they work.

Businesses should also minimize the number of steps consumers must take to submit requests. Indeed, any process that requires consumers to jump through hoops to exercise their rights (*e.g.,* requiring consumers to create accounts to submit a request) will likely draw scrutiny from the CA AG.

5. Tabletop Exercises Aren't Just for Security Incidents: Test Your Data Subject Rights Request Procedures. The CCPA provides consumers (and as of January 1, 2023, employees and business-to-business contacts) with several rights that businesses must honor. To do so, a business must have adequate procedures that allow consumers to make their request and that ensures the business effectuates them. Several of the enforcement actions concerned inadequate request procedures, including against a clothing retailer, an online people search company, a fitness center chain, a financial technology services mobile app operator, and a medical devices manufacturer. The CA AG alleged all of them had insufficient procedures, whether it was a failure to post a "Do Not Sell My Personal Information" link on a homepage or a failure to train employees to respond to consumer requests appropriately.

While tabletop exercises were started to test incident response programs, given the complexity to coordinate data access, deletion, and other requests internally, companies are developing and conducting a new form of tabletop designed for the privacy, legal, compliance, and business teams to choreograph a data subject rights request response. This helps prevent delays, practice authenticating a request, review exceptions as to whether a request must be honored, and helps the IT and business to find and act upon the data subject to the request. While California and Europe provide for 30 and 45 days to honor data subject requests, Brazil provides for 15 days. This type of tabletop exercise is becoming increasingly important for global companies to make sure they can maintain one compliant process for all the varied requests their organizations may receive.

Implementation Tip: Businesses may want to audit their current program through "secret shopper" initiatives globally, which would allow the business to see not only how the business in responding to data subject requests, but also within what timeframe.

Prepare Now for January 1, 2023. While August 24 was significant for the announcement of the first CCPA settlement, the CPPA also held a public hearing on the same day regarding the draft CPRA regulations. These public hearings are an important part of the rulemaking process, and these rules will further shape how the CCPA is enforced. Not only will businesses need to comply with further regulations, but businesses will also lose the 30-day notice to cure on January 1, 2023. To prepare for the CPRA coming into force on January 1, 2023, and for the promulgation of further regulations, businesses should review current privacy practices, policies, and procedures now.

As always, Troutman Pepper's Privacy + Cyber Practice stands ready to assist with global privacy and security compliance, including developing and conducting threshold analysis and security assessments under the CCPA, as needed.

Please contact Jim Koenig, Kim Phan, Sadia Mirza, Robyn Lin or any member of our Privacy + Cyber Practice with questions.

[1] For additional information relating to the CPRA, *see* Troutman Pepper's five-part series at https://www.troutman.com/insights/california-privacy-rights-act-series.html. The series consists of the following sections: (1) introduction and overview; (2) consumer rights; (3) notice and disclosure obligations; (4) data processing obligations; and (5) litigation and enforcement.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber