

Lessons from The First California Consumer Privacy Act (CCPA) Enforcement and Settlement

Sep 22, 2022

Categories:

Publications

Authors:

Jean Paul Yugo Nagashima
Michael E. Nitardy

On August 24, major cosmetics retail store Sephora USA, Inc. entered into a settlement with the California Attorney General ("California AG"). The California AG's complaint (Complaint) alleged that Sephora violated the CCPA because it failed to take three actions under the CCPA:

- notify consumers that it sold consumer's personal information;
- provide a "Do Not Sell My personal information" link; and
- honor consumer opt-outs via the user-enabled Global Privacy Controls (GPC).

In the settlement, Sephora agreed to pay $1.2 million and put in place a compliance program to process consumer requests to opt out of the sale of personal information, including implementing GPC, and provide an annual report assessing the recipient of Sephora's collected personal information.

Disclosing Personal Information for Analytics is a "Sale" of Personal Information

The Complaint alleged that Sephora violated the CCPA by selling consumers' personal information to third parties without informing its customers that Sephora was engaging in the activity. Specifically, the Complaint alleged that Sephora collected customers' personal information on its website and mobile apps using cookies and pixels and made that information available to third-party analytics providers. The California AG stated that providing third parties, such as advertising networks, business partners, and data analytics providers with access to its customers' geolocation and internet or other electronic network activity information in exchange for services was a "sale" of personal information. This disclosure of personal information to third-party analytics services was deemed

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

a “sale” because Sephora benefitted from the disclosure in the form of receiving free or discounted analytics and targeted advertising.

The Service Provider Contracts Exception to Sale of Personal Information Did Not Apply to Sephora

The Complaint further pointed out that Sephora failed to meet the service provider disclosure exception. Under the CCPA, businesses may use or provide a service provider with personal information if it is necessary to perform a business purpose if the following conditions are met:

- The business has provided consumers notice of that information being used or shared in its terms and conditions/privacy notice.
- The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

Cal. Civ. Code 1798.140 (t)(2)(C)(i)(ii). However, the California AG alleged that Sephora did not put in place valid service provider contracts with the third-party analytics providers obligating them to use the personal information only for certain business purposes. This suggests Sephora may have avoided its disclosures to the third-party analytics providers being deemed a “sale” if Sephora had taken steps to have a valid service provider contract with the analytics providers.

Global Privacy Controls Cannot be Ignored

The California AG’s Complaint also alleged that Sephora failed to honor the GPCs of consumers because its website was not configured to detect or process the GPC signals. Under the CCPA regulations, businesses must treat user-enabled global privacy controls that communicate or signal the consumer’s choice to opt out of the sale of their personal information as a valid request. 11 CCR § 7026. However, Sephora did not implement a mechanism to detect the GPC signals. The testing and investigation of California AG revealed that activating the GPC signal had no effect, and the

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

data continued to flow from Sephora to third-party companies, including advertising and analytics providers. Based on the investigation, the Complaint alleged that Sephora had not honored the GPC signal and violated the CCPA's mandate to honor consumer opt-out requests for the sale of their personal information.

Take-Aways from the Sephora Enforcement

The Sephora settlement provides new insight into how the California AG and California Privacy Protection Agency view a "sale" of personal information. Businesses should review their privacy notices and their business practices to confirm that their privacy notice does not state "we do not sell personal information" if they disclose personal information to third-party analytics providers in return for discounted analytics or high-quality targeted advertising.

Companies should also review their service provider agreements and confirm that there is a valid agreement in place that requires the service providers, including third-party analytics providers, to comply with the CCPA service provider obligations so that the businesses can satisfy the service provider exception to the sale of personal information.

From a technical and IT standpoint, companies should review their website to ensure that GPC signals are honored. GPCs are yet to be widely adopted, and businesses have taken a wait-and-see approach to GPC implementation. The Sephora settlement suggests that GPC implementation is not an option but a requirement for CCPA compliance.

In addition, the provisions of the CPRA will also become effective in 2023. Businesses should begin reviewing their privacy and information security policies to ensure that they are in compliance with the CCPA and the CPRA.

For more information, please contact any member of Frost Brown Todd's Privacy & Data Security practice group.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons