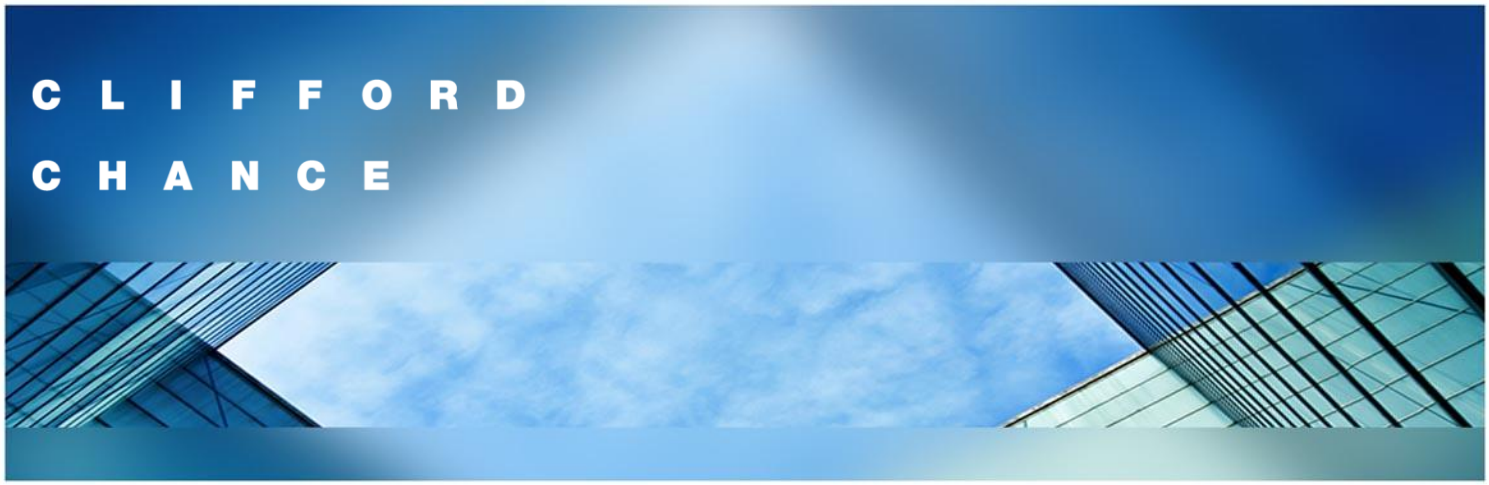

ONE "FINE" DAY? INSIGHTS FROM THE FIRST FINE ISSUED BY THE CALIFORNIA ATTORNEY GENERAL UNDER THE CCPA

On August 24, 2022, the California Attorney General (CAG) announced a $1.2 million settlement with Sephora to resolve allegations that the consumer goods retailer violated the California Consumer Privacy Act (CCPA) by failing to disclose to consumers that it was selling their personal information. The settlement is notable not only because it is the first civil penalty issued under the statute, but also because it confirms a broad interpretation of what constitutes a "sale" of personal information under the law and the requirement for websites to respond to global privacy controls. The action also gives insight into the state's focus with regards to enforcement of the CCPA as the state prepares for changes to come in 2023.

Key issues

- The California Attorney General has issued its first monetary penalty against consumer goods retailer Sephora.
- The settlement confirms that the California Attorney General considers quid pro quo use of third-party tracking technologies (i.e., analytics in exchange for access) to be "sales" of personal information under the CCPA.
- The California Attorney General also interprets the statute to require the ability to respond to GPC opt-out requests.
- Proper service provider contracts may be effective to avoid obligations to make certain Do Not Sell disclosures.

INSIGHTS FROM THE SEPHORA INVESTIGATION AND SETTLEMENT

The proposed settlement with Sephora resolves two primary allegations of noncompliance with the CCPA. First, the CAG alleged that the consumer goods retailer failed to disclose to consumers that it was collecting and selling personal information from users who browse Sephora's website and use the retailer's mobile app. Sephora installed third-party tracking software on its website and mobile application that collect personal information from users such as shopping habits, and precise geolocation data to create user profiles. According to the CAG, Sephora provided this personal information to third parties in return for detailed analytics information and targeted advertising opportunities. Second, the CAG alleged that Sephora failed to honor Global Privacy Control (GPC) signals sent by consumers to opt out of such personal information collection and sales. Sephora's website was not configured to detect or respond to GPC signals.

Both allegations of noncompliance provide important insights into the CAG's interpretation of the requirements of the CCPA:

1. Analytics for Access "Quid Pro Quo" Constitutes a Sale of Personal Information

The CCPA imposes several obligations on companies that sell personal information. Companies that sell personal information must provide notice to consumers about what personal information they sell and the categories of recipients. They must also provide consumers with the right to stop such sales and include instructions on how to do so in their privacy notices, with an easy-to-identify link on their website.

The statute defines a "sale" of personal information as any disclosure to a third party for "monetary or other valuable consideration." Until now there has been an active debate about how the CAG would interpret this provision with respect to common third party tracking technologies such as cookies. With the Sephora settlement, the CAG has now made clear that it takes a broad view of what constitutes a sale of personal information under the statute. According to the complaint, Sephora's "sales" consisted of its decision to allow third-party trackers to collect personal information on its website, in exchange for services from those entities. The CAG explained that in return for providing these third parties with access to customer data, Sephora received free or discounted analytics and advertising benefits.

2. Responding to Global Privacy Control Signals is Mandatory, not Optional

With the Sephora settlement, the CAG also makes clear that it considers the statute to require covered entities to honor Global Privacy Control (GPC) signals. GPC is a technical specification that browsers and mobile devices can implement to allow users to notify companies of their privacy preferences, including whether to allow their personal information to be collected and sold. The specification is developed by a group of privacy advocates, technology companies, and advertisers, including browser developers like Mozilla, search engine providers like DuckDuckGo, and media companies like the New York Times.

Notably, neither the CCPA nor California Privacy Rights Act (CPRA, the set of amendments passed in 2020 scheduled to go into effect in 2023) specifically require compliance with something like the GPC; the CPRA merely permits companies to facilitate sale (and sharing) opt-out requests through a "preference signal" like the GPC. In 2021, however, the CAG made clear in guidance that it considered GPC signals to be an opt-out request that companies must recognize and action. The requirement to abide by GPC requests is also present in regulations issued by the CAG (currently under consideration by the CPPA, the new regulatory agency created by the CPRA).

3. Proper Service Provider Contracts Can Avoid "Sales"

One interesting note of the complaint is the CAG's allegation that Sephora did not have valid service provider contracts in place with the third parties that operated the tracking technology present on the retailer's website. The CCPA requires companies that disclose personal information to "service providers" to have in place certain contractual provisions that describe (and limit) the purposes for

which the disclosed personal information is to be used, and that impose certain obligations on the service provider. Providing personal information to a service provider is not considered a sale under the CCPA. The CAG suggests in its complaint that had Sephora had such provisions in place, its disclosures may have not been considered sales under the statute.

4. Take the Opportunity to Cure While You Can

According to the complaint, the CAG first learned of Sephora's potential noncompliance with the statute last summer. In June 2021, the CAG conducted a compliance review of a number of large retailers specifically to determine whether they continued to sell personal information of a consumer after they had received a GPC opt-out signal. This investigation determined that: (i) Sephora allowed third parties to collect personal information from consumers who browsed Sephora's website; and (ii) Sephora's website did not recognize or action GPC opt-out signals, continuing to permit third-party data collection even after users had sent a GPC opt-out signal.

Notably, the CAG appears to have first tried to persuade Sephora to cure these alleged violations. The CAG notified Sephora of its noncompliance on June 25, 2021 and gave Sephora the statutorily mandated 30-day period to cure its identified deficiencies. Had Sephora taken action to address the CAG's concerns, the retailer likely would not have been faced with any penalties.[1] Sephora failed to do so, however, and after further investigation by the CAG, the office commenced this enforcement action.

In addition to a USD 1.2 million fine, Sephora also agreed to take a number of corrective actions to address its identified noncompliance with the CCPA. These measures include: (i) revising its privacy notices to disclose its sale of personal information using online tracking technology and informing consumers of their right to opt out of such sales; (ii) implementing measures to respond to and action GPC opt-out signals; and (iii) revising its service provider agreements as necessary to comply with the statute. The proposed settlement would also require Sephora to undergo regular assessments and report on compliance to the CAG for the next two years.

CONCLUSION & TAKEAWAYS

With the issuance of this first monetary penalty under the CCPA, the CAG has made a strong statement about what it considers to be required for compliance with the statute, particularly with regards to what constitutes a "sale" of personal information under the law. In its complaint against the Sephora, the CAG noted that the retailer had installed a "widely-used analytics and advertising software package," which many have speculated to be Google Analytics, a widely-used analytics and advertising tool that has faced privacy scrutiny from regulators around the world. If that is true, Sephora may just be the tip of an impending wave of enforcement action—indeed, in the press release announcing the settlement, the CAG also added that he had just sent notices to several businesses notifying them that their failure to process consumer opt-out requests (including GPC signals) violated the law.

[1] Prior to this complaint, the CAG's enforcement efforts have been limited to notices of noncompliance.

All companies that are in scope of the law should take heed of the CAG's warning and review their personal information processing activities—especially if they use third-party advertising and analytics services on their websites or mobile applications. While the Sephora settlement may be surprising in some of its interpretations of the statute, it also provides guidance to companies on how to avoid noncompliance. Companies should follow the roadmap provided by the CAG by: updating their privacy notices if appropriate to disclose any sales of personal information; ensuring any data processing portals respond to GPC signals; and implementing contractual provisions with third parties to which they disclose personal information to avoid such transfers being considered "sales" under the statute. This is particularly important as the CPRA's elimination of the 30-day cure period looms in 2023.

CLIFFORD CHANCE

CONTACTS

Devika Kornbacher
Partner

T +1 212 878 3424
E devika.kornbacher@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver@cliffordchance.com

Thomas Chapman
Associate

T +1 202 912 5921
E thomas.chapman@cliffordchance.com

Shannon O'Brien
Associate

T +1 212 880 5709
E shannon.obrien@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.