California AG Announces First CCPA Settlement and There is More Enforcement to Come

October 3, 2022 – The TMCA
by Austin T. Chambers and Deb Howitt

The first California Consumer Privacy Act (CCPA) settlement was announced on August 24, together with a strong message from California Attorney General Rob Bonta regarding compliance with the CCPA. The settlement involves Sephora USA, Inc., and resulted from a sweep of enforcements by the Attorney General last year. As part of the settlement, Sephora agreed to pay $1.2 million and comply with requirements related to its CCPA obligations. Prior to the AG investigation, Sephora was notified of its alleged CCPA violations but failed to cure within the 30-day period allowed under law. This failure prompted the AG to initiate the enforcement action.

The definition of "sale" under the CCPA is extremely broad, and includes *"selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating" personal information "for monetary or other valuable consideration." According to the complaint,* Sephora made consumers' information available to third parties in connection with targeted advertising and "analytics" services, both of which the complaint indicated constituted a "sale." The complaint alleges further that Sephora's vendors were not subject to appropriate "service provider" contracts necessary for the vendor's processing to not be considered a sale for purposes of CCPA. At the time, the Sephora privacy policy stated that it did not "sell" personal information, and did not include an opt-out of sale link.

Taking these issues into account, the complaint alleged that Sephora violated the CCPA

Related People

- Austin T. Chambers

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

by failing to: (i) display a “do not sell my personal information” link on its homepage, (ii) describe the categories of personal information sold or shared in its privacy policy, and (iii) honor opt-out requests, including through response to the Global Privacy Control (GPC), a browser plugin designed to enable consumers to automatically opt-out of data sales on numerous websites with a single setting. In addition to curing these violations, the settlement also requires Sephora to conform its service provider agreements to the CCPA’s requirements, properly configure service provider products and services, and provide reports to the California Attorney General relating to its sales of personal information, its relationships with service providers, and its ability to honor requests via GPC settings. The complaint also previewed to Sephora that the technologies it used may create additional risks for consumers’ sensitive information related to health conditions. This, by extension, could create risk of non-compliance with forthcoming CCPA requirements applicable to businesses’ processing of sensitive personal information.

Companies should note that CCPA requirements are complex to implement, and the 30-day cure period may be insufficient to make all needed changes. In addition, the cure period currently allowed under the law will expire as of January 1, when the CPRA amendments to the CCPA becomes effective.

It is therefore critical for companies to evaluate their CCPA compliance posture prior January 1, 2023, as the California Attorney General’s office, together with the new California Privacy Protection Agency, appear poised to increase their enforcement efforts, and may be less tolerant of non-compliance. In a press release issued together with the Sephora settlement, Attorney Rob Bonta stated:

“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.”

Together with announcing the Sephora settlement, the Attorney General’s office also issued notices to a number of other businesses alleging non-compliance relating to their failure to honor opt-out requests via the GPC or similar controls. Recipients of these notices will have 30 days to cure the violations, or they will face enforcement actions. Businesses receiving such notices after January 1, 2023, however, will have no such opportunity to cure. Examples of the notices to cure sent by Bonta’s office can be found at oag.ca.gov/ccpa.

There are several important lessons in the Sephora settlement.

1. The California AG is treating GPC as a requirement, rather than an option. Although the statutory text of the CCPA does not mandate compliance with the GPC, the AG suggested this was a requirement in the 2021 amendments to the CCPA regulations, and in the CCPA FAQ page in July, 2021. Whether or not this constitutes sufficient notice and a true statutory requirement is somewhat debatable, but companies should take notice and ensure GPC compliance in order to avoid potential enforcement for

non-compliance.

2. Any doubts regarding whether third-party online behavioral advertising and profiling constitute data sales have now been removed (though such relationships are likely to fall within the scope of the CPRA's new "sharing" opt-out requirements once the CPRA amendments take effect).
3. Privacy policies must clearly disclose the categories of data sold, the fact that sales are taking place, and other requirements specified in the CCPA.
4. Companies engaging in data sales must have a "do not sell" link on their homepage and in their privacy policy, with the required means to opt-out enabled.
5. Service provider contracts must meet CCPA's service provider contract requirements in order for the relationship to be exempt from the "sale" definition. Note that each relationship must, in fact, meet relevant service provider requirements, and language alone will not accomplish this. Similarly, service provider technologies may require additional configuration for processing to be in scope of the service provider agreement.
6. Companies should be aware of using targeted advertising in a manner that implicitly reveals sensitive information (e.g. pregnancy or other health conditions).

With the CPRA and other state laws becoming effective in the next year, companies have numerous tasks to do to prepare. For companies engaging in data sales, GPC implementation should be near the top of the to-do list, and more information is available at Global Privacy Control — Take Control Of Your Privacy