THOMPSON HINE

# Privacy & Cybersecurity Update

**September 2022**

## CCPA Enforcement and Preparing for 2023 Data Privacy Rules

California Attorney General Rob Bonta recently announced a $1.2 million settlement against a business for its violations of a California privacy law related to website configurations, targeted advertising, and the “sale” of personal information. This case is not only an important milestone in terms of enforcement of the California Consumer Privacy Act of 2018 (CCPA), but it should serve as a guidepost for how companies update their data protection compliance programs to account for new privacy laws entering into force in 2023 (e.g., California, Connecticut, Colorado, Utah, Virginia). See our state-by-state comparison chart for more information on how these laws address targeted advertising and consumer opt-out rights.

### The Sephora Settlement

The complaint lodged by the state of California against Sephora USA focused on how its e-commerce website (designed to sell personal care and beauty products) collected, used, and disclosed certain types of personal information from its end users. In particular, the complaint alleged that Sephora installed third-party tracking software on its website and in its app so that it can (through these third parties) monitor end users who access its website and online services. This software is known for collecting a broad range of personal data on end users, including geolocation data, information on their device type, and potential product purchases.

According to the complaint, “[s]ome of these third-party companies create entire profiles of users who visit Sephora’s website,” which the third parties then use for Sephora’s benefit (e.g., to generate customer analytics, enabling Sephora to purchase online ads targeting specific consumers) and “[t]his data about consumers is frequently kept by companies and used for the benefit of other businesses, without the knowledge or consent of the consumer.” According to California, **these activities constituted the “sale” of personal data under the CCPA**. The complaint alleged that Sephora failed to (i) disclose to consumers that it was “selling” their personal information in this context, (ii) post a “Do Not Sell My Personal Information” link on its website and mobile application to facilitate do-not-sell opt-out requests, and (iii) process sale opt-out requests submitted through user-enabled global privacy controls in violation of the CCPA.

The settlement agreement between Sephora and California stated that to the extent the business “sells the personal information of consumers, including through using online tracking technology, [Sephora] shall provide notice to consumers” of the same in accordance with the privacy policy requirements set forth in the CCPA. This notice must clearly state that consumers have the right to opt out of the sale of their personal information. In addition, Sephora must also process sale opt-out requests submitted by consumers via a user-enabled global privacy control.

The settlement agreement also provides that Sephora must (i) identify and document the third parties with whom it shares personal data, (ii) describe whether such third parties are considered “service providers” pursuant to the CCPA, and (iii) for such third parties that are not service providers, Sephora must (a) comply with the aforementioned notice and opt-out requirement, (b) enter into contracts with such entities to bring them within scope of the CCPA’s “service provider” framework, or (c) stop disclosing such personal data to them. The settlement agreement also calls for Sephora to continuously undertake assessments and draft reports in this area to demonstrate its compliance with the agreement.

## Complying with the 2023 Data Protection Laws

Notwithstanding the ambiguities in the CCPA, the California attorney general has made clear that when an organization "utilizes third-party tracking technology without alerting consumers and giving them the opportunity to control their data, they deprive consumers of the ability to limit the proliferation of their data on the web." Organizations should closely follow this assessment as they evaluate their website configurations and data processing activities in light of the several new data protection laws entering into force in 2023. For compliance purposes, organizations should undertake the following data processing measures.

***Data mapping***. As highlighted by the Sephora settlement, it is important for organizations to understand how they collect personal data in the online environment and elsewhere. They should memorialize their data processing activities in a data map or inventory, which should describe the purpose of collecting such data; with whom the data is shared; and the retention, security, and disposal criteria with respect to such data. A comprehensive data map or inventory is a fundamental component of any data protection program.

***Privacy and cookie notices***. The central component of drafting website privacy statements and cookie policies is to provide notice to website end users on how their personal information, including online identifiers (e.g., IP addresses), will be collected and used by a business. This notice allows consumers to make informed decisions on whether to permit such activities or refrain from engaging with the business or the data processing. In turn, organizations should ensure they have updated their privacy statements and cookie policies to satisfy their legal obligations and clearly and accurately reflect their data processing activities.

***Opt-out tools***. A key focus of the CCPA and other data protection laws entering into force in 2023 is for organizations to provide end users with mechanisms to enable them to effectively and efficiently prevent their personal data from being sold or used for targeted advertising purposes. This includes building cookie management tools within their website to allow end users to control how the website can deploy cookies, pixels, and tags to collect and process end-user data. It also may include configuring websites to recognize when end users seek to opt out from targeted advertisements or the sale of their personal data via their device's global privacy setting.

***Third-party contracts***. As emphasized in the Sephora settlement, it is important for businesses to have certain data processing clauses within the service contracts they execute with third-party organizations that provide data processing services, including services related to online tracking, advertising, and analytical software and solutions. These clauses must address, among other areas, limited data rights, confidentiality, information security, assistance, and use of subcontractors. These contractual frameworks should be recognized and incorporated into the data mapping processes identified above.

## Conclusion

The Sephora case highlights the importance of ensuring that organizations have comprehensive data protection programs to account for all aspects of their data processing activities, including in the online context. It is also a reminder of how the data protection laws in California, as well as Colorado, Connecticut, Utah, and Virginia, place significant restrictions on how businesses can collect and process online identifiers and other personally identifiable information derived from a website. Our state-by-state comparison chart provides more information on the obligations these state laws and regulations impose on certain organizations regarding collecting and processing information in the online context, particularly for purposes related to targeted advertising and the sale of personal data.

## FOR MORE INFORMATION

For more information, please contact:

**Steven G. Stransky**
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
*Certified Information Privacy Professional/Government (CIPP/G)*
*Certified Information Privacy Professional/United States (CIPP/US)*

**Thomas F. Zych**
216.566.5605
Tom.Zych@ThompsonHine.com

**Thora Knight**
212.908.3971
Thora.Knight@ThompsonHine.com