SpencerFane®

Landmark $1.2M Sephora Settlement Highlights the Importance of CCPA Compliance

The Attorney General (AG) for California just settled a California Consumer Privacy Act (CCPA) enforcement case against Sephora for $1.2 million. While Sephora denies liability in the settlement, the outcome of this settlement should send shivers down most companies' spines who may engage in some of the same conduct that landed Sephora in trouble. Read below for some of the major takeaways from this landmark decision.

The stereotype goes that California is "bad for business," and the Sephora settlement furthers engrains that stereotype. The settlement confirms that companies who are subject to the CCPA will need to remain vigilant about ensuring their companies remain compliant with a web of not-so-easy-to-manage data privacy issues. This includes ensuring easy ways for consumers to opt out of information collection and sales; easily understand what information businesses collect on them; and understand how tracking technologies are used. Companies have an obligation to ensure that their technology vendors and business partners are living up to CCPA obligations, including how "do not sell" and "do not track" web browser settings are interpreted and acted upon.

While some companies believed that if they were not physically located in California, they would not have to comply with California law and/or the risk of enforcement against them would be low, the remarks from the California Attorney General regarding the Sephora case make clear these are incorrect assumptions. While Sephora did have a physical presence in California, the settlement makes clear that even businesses without a physical presence in California can, and will, be targeted in compliance actions. From a legal standpoint, we agree, the CCPA does not distinguish between companies that are physically located in or outside of

California, instead, focusing on the conduct of the business as it relates to California consumers.

The California AG has provided a stark warning to other companies, "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. Follow the law." Starting January 1, 2023, the CCPA's current 30-day notice and cure grace period expires. In other words, companies who are not CCPA compliant will automatically be liable for violations and not have an opportunity to cure them. If your companies has not already implemented CCPA compliance, they should immediately do so. Even for those companies who have CCPA compliance regimens, it is prudent to do the following:

- (Re)Confirm if the CCPA applies.
- If the CCPA applies, audit technology safeguards, including for global data privacy controls and how opt-out requests are being processed.
- Review and update privacy policies.
- Review and update internal procedures for acquiring, storing, and handling data, including opt-out privacy requests.
- Identify all vendors and partners with whom consumer data is acquired or shared.
- Revise contracts with vendors and partners as applicable to ensure they are compliant with the CCPA.
- Review and limit sharing and sale of personally identifiable information, where possible.

While the Sephora case is the first high profile case involving CCPA enforcement, more enforcement actions are expected to come. Even companies who are not subject to the CCPA should be aware that four additional states are set to have similar laws go into effect in 2023, including Colorado, Connecticut, Utah, and Virginia. There is clearly a prevailing movement of legislatures to enact stricter consumer data privacy laws. At a minimum, all companies who may be subject to these laws should promptly consult with a data privacy attorney to start enacting necessary safeguards.

This blog post was drafted by Jon Farnsworth, a partner in the Minneapolis, Minnesota, office of Spencer Fane. For more information, please visit

www.spencerfane.com.