KILPATRICK TOWNSEND

KTS Advertising Law Guides

The Impact of the CCPA on Advertising: What You Need To Know

By: Michelle Tyde and John Brigagliano

As brands increasingly use data management platforms or customer relationship management platforms to enhance sales, the California Consumer Privacy Act ("**CCPA**") will significantly impact a brand's data practices as the law increases the required level of data privacy transparency and choice for consumers. Compliance with the CCPA represents a major change in how most businesses operate and manage data; the law provides broader rights to consumers and stricter compliance requirements for businesses than any other state or federal privacy law. Accordingly, brands need to understand the new privacy framework established by the CCPA in order to prepare for compliance.

Below are 10 key facts you need to know.

1 New Privacy Rights for California Residents.

The CPPA applies to "consumers," who are natural persons and California residents. A California resident is not a visitor, and does not have to physically be in California when the personal information is collected. The consumer rights created by the CCPA include access, deletion, and opting-out of the sale of personal information. The CCPA covers not only the collection and processing of personal information, but also the sale of such information which is defined very broadly to include any communication or transfer of personal information to a third party "for monetary or other valuable consideration." That broad definition of sale is in contrast to the GDPR.

2 Extraterritorial Reach.

The scope of the CCPA extends outside of California to companies that may not have offices or employees in California, but that do "business" in the State, collect or sell the personal information of California residents, and meet one of the following thresholds:

- Annual gross revenue in excess of $25 million;
- Alone or in combination, annually buys, receives for the entity's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households or devices; or
- 50% or more of annual revenue is derived by the company selling consumers' personal information.

3 Common Branding.

Parent companies and subsidiaries that share common branding as an affiliated company subject to the CPPA are covered in the definition of "business," even if they themselves do not exceed the applicable thresholds. Though the CCPA provides no guidance as to the requisite degree of sharing, having a common designator on digital properties may suffice to meet common branding.

4 Expansive Definition of Personal Information.

The CCPA's definition of "Personal Information" is the most far-reaching in the United States. It includes any information that "identifies, relates to, describes, *is capable of being associated with*, or *could reasonably be linked*, directly or indirectly, with a particular *consumer or household*." The CCPA enumerates specific categories of personal information, several of which specifically impact advertising:

- geolocation data;
- identifiers, such as a "unique personal identifier" or IP address;
- commercial information, such as records of products or services purchased;
- internet information, such as "interaction … with an advertisement"; and
- inferences, which are derived from data drawn from any other personal information to create a consumer profile.

Consequently, the CCPA regulates information not previously considered within the scope of personal information under U.S. state and federal laws. This sweeping definition will dramatically impact digital marketing.

5 De-Identified and Aggregate Information.

While the CCPA does not apply to aggregate or de-identified data, ambiguity surrounds these exemptions in light of the fact that the CCPA defines aggregation and de-identification as distinct and separate concepts. Furthermore, the de-identification exception requires companies to implement internal policies for prohibiting re-identification and preventing inadvertent releases of de-identified information. The CCPA's definition of de-identified and aggregate are seemingly inconsistent with HIPAA and GDPR, and much more limited than that defined by the FTC. Given the lack of clarity surrounding these exemptions and the exceptionally broad definition of personal information, the CCPA will affect current business practices that involve information currently considered to be de-identified or aggregate information.

6 Access Right.

Within 45 days of receiving a verified request from a consumer or his or her authorized representative, a company must provide the following personal information ("**PI**") to the consumer:

- The categories of PI collected about that specific consumer.
- The categories of sources from which the PI is collected.
- The specific pieces of PI collected about that consumer.
- The business and commercial purpose(s) for collecting or selling the PI.
- The categories of third parties with which the business "shares" PI.
- For PI that is sold, the categories of the consumer's PI sold about the consumer and the categories of third parties to whom the PI was sold, by category or categories of PI for each third party to whom the PI was sold.
- For PI that is disclosed for a business purpose, the categories of the consumer's PI that were disclosed.

Companies must offer at least two methods for submitting requests, including at minimum a toll-free number and an online mechanism.

7 12 Month Look Back Requirement.

Although the CCPA does not go into effect until January 1, 2020, a key provision known as the "look back" requires California businesses covered by the CCPA to begin preparing now. Once the law goes into effect, any data access request received from a consumer will require a look back at the previous 12 months of data. Thus, compliance necessitates that companies begin the inventory and mapping of personal information of California consumers as of January 1, 2019.

8 Opt-Out Right.

The CCPA is a game changer in privacy regulations as it allows consumers to opt-out of the sale of their personal information and requires companies to include a conspicuous

"Do Not Sell My Personal Information" link on their home page. Moreover, companies must describe this right and include a link to the opt-out in their Privacy Policy. The PI of children 13 – 16, however, cannot be sold unless the consumer specifically opts-in (gives affirmative consent) to the sell. Willful disregard of a consumer's age will be treated as actual knowledge of their age, subjecting a company to potential liability for violation of the CCPA.

The CPPA prohibits companies from discriminating against consumers who exercise their rights under the CCPA. Consequently, when a consumer opts-out of the sale of PI, a company is prohibited from denying goods or services, charging a different price, imposing penalties, providing a different level or quality of service, or suggesting that the consumer will receive a different price or rate or different level or quality of goods or services. Though there are a couple of ambiguous exemptions to this requirement, the current understanding is that this will affect customer loyalty programs. One of the current pending amendments to the law will expressly allow loyalty programs without violating this requirement.

9 Compliance Is Challenging Due To The Law's Ambiguities.

The CCPA was rushed through the California legislature to avoid a consumer-driven ballot initiative. Consequently, the fast-tracked process produced a law with confusing and contradictory language that leaves many details unexplained or open for interpretation. While lawmakers left the door open for the state Attorney General to provide guidance and clarification through its rulemaking process, there are also currently over 50 amendments pending before the legislature. Thus, is it likely that the definitions, scope, and requirements may change before the law goes into effect in January of 2020.

10 The CCPA's Enforcement Mechanism Includes Statutory Fines and Private Actions.

The CCPA includes the possibility of enforcement through private litigation and statutory fines for violations. For violations brought by the California Attorney General's Office, statutory fines are $7,500 per intentional violation of any provision of the CCPA, or, for unintentional violations, $2,500 per violation.

The private right of action is limited to violations of the data security requirements. Statutory damages for such actions are $100 to $750 per California consumer and incident, or actual damages, whichever is greater. A pending amendment to expand the private right of action to any violation of the CCPA recently died in the California legislature. Such expansion, however, could be proposed again in the future.

Hence, non-compliance with the CCPA will be costly for any company subject to its requirements.

For more information, contact:
Michelle Tyde at mtyde@kilpatricktownsend.com
John Brigagliano at jbrigagliano@kilpatricktownsend.com