



December 6, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: California Consumer Privacy Act Regulations

Dear Attorney General,

We appreciate the opportunity to comment on the regulations proposed by your office to implement the California Consumer Privacy Act (CCPA). Founded in 2001 as the Online Publishers Association, Digital Content Next (DCN) is the only trade organization in the U.S. dedicated to serving the unique and diverse needs of high-quality digital content companies which enjoy trusted, direct relationships with consumers and marketers. DCN's members are some of the most trusted and well-respected media brands that, together, have an audience of 256,277,000 unique visitors or 100 percent reach of the U.S. online population¹. In layman's terms, every person in the U.S. who goes online will visit one of our member companies' websites at least one time each month.

Do Not Sell

As we noted in our letter² dated November 7, when a consumer activates their Do Not Sell right, the CCPA and your proposed regulations would require 3rd party companies on a website or app to limit their data collection and use to the role of a service provider, which means they could not use data about the consumer except on behalf of the website or app publisher as defined by contract with the publisher. For example, Facebook and Google would need to stop collecting data about consumers via the "like" button and ad serving technologies, respectively. Unless and only when the consumer intentionally interacts with those services, Google and Facebook should be considered third parties. Given our experience with

¹ *comScore Media Metrix Multiplatform Custom Audience Duplication*, December 2017 U.S.

² <https://digitalcontentnext.org/wp-content/uploads/2019/11/DCN-letter-to-CA-AG-2019-11-07.pdf>

implementation of the General Data Protection Regulation (GDPR) in Europe, it is important that this point be clear. We are concerned that some third parties may try to implement creative interpretations of the CCPA which would run counter to the law and consumer expectations.

Disclosure Requirements

We are concerned that the requirements for disclosure to consumers of data collection practices, taken as a whole, may be overwhelming for consumers trying to understand how their data is being used and counterproductive to the goals of the CCPA. Specifically, Section 999.308 (b)(1)e.1 of the proposed regulations would require companies to “state whether or not the business has disclosed or sold any personal information to third parties for a business or commercial purpose in the preceding 12 months.” According to Section 1798.140 (d) of the CCPA, business purposes include “auditing,” “detecting security incidents,” “debugging,” “short-term, transient use,” “customer service” and “internal research” among other things. The California Legislature wisely carved out these activities from the scope of a “sale” because they are examples of benign data collection and use that are necessary to providing a service to consumers. We are concerned that, by lumping “business purposes” with “commercial purposes” in the disclosure requirement, the benign activities under “business purposes” may be unfairly characterized. Consumers may be confused about whether “business purposes” would be within the scope of the CCPA’s Do Not Sell right.

In addition, we are concerned about the disclosure requirements in Section 999.317 (g), which require a “business that alone or in combination, annually buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers, shall” disclose several metrics related to the number of consumer requests to know, delete and opt out along with the median number of days it took the business to substantively respond. We believe the threshold of “4,000,000 or more consumers” is very low particularly for businesses that primarily interact with consumers online. According to ComScore, the top 5 most visited “businesses” online each attracted over 200 million consumers in September 2019³ alone. While we support the goal of providing transparency for consumers especially with regard to how big data companies are complying with the CCPA, we are concerned that this obligation will unintentionally fall on small businesses with limited resources. We encourage you to significantly raise the threshold at least for businesses that primarily interact with consumers online or focus on businesses which collect data on consumers across a broad range of unaffiliated websites.

Flexibility for Service Providers

Service providers should use data consistent with their contracts with publishers, thus we applaud the proposed regulations’ allowance in Section 999.314 (c) for service providers to “combine personal information received from one or more entities to which it is a service provider...to detect security incidents, or protect against fraudulent or illegal activity.” Fraudulent or criminal actors often pose as real consumers to either engage in fraudulent

³ <https://www.comscore.com/Insights/Rankings>

advertising or exploit security weaknesses. Allowing publishers to use service providers to weed out these bad actors protects consumers and helps build trust in the internet marketplace.

90-Day Notification Requirement

Section 999.315 (f) requires businesses to “notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business’s receipt of the consumer’s request that the consumer has exercised their right to opt-out and instruct them not to further sell the information.” For example, in a typical behaviorally-targeted advertisement on a website, there are multiple companies involved in serving the ad. In order to comply with Section 999.315 (f), all of the companies involved in serving the ad, assuming it qualified as a “sale,” would need to keep a record of which consumer saw which ad along with the specific pieces of data that were collected. We are concerned that this requirement would be difficult to implement and would inadvertently require businesses to collect additional data about consumers. We urge you to strike this 90-day notification requirement.

Industry Solutions

Over the coming weeks and months, there will be significant discussion about developing an industry-wide solution for compliance with the CCPA. Recently, the Interactive Advertising Bureau (IAB) issued such a proposal⁴ for consideration. While we are still carefully examining the details of the proposal and awaiting additional documentation, we want to publicly support the basic approach of the IAB framework as it relates to the implementation of the consumer’s Do Not Sell (DNS) right. When a consumer exercises their DNS right, the IAB framework requires that the business (e.g. publisher) pass along a signal to all downstream companies that indicates the consumer has opted out of the sale of their information. When those downstream companies receive the signal, they would immediately conform their data collection and use practices to the role of a “service provider,” meaning those downstream companies could not use data for any secondary purpose including the building of a profile about that consumer. We believe this approach satisfies the letter and spirit of the CCPA to give consumers control of how their data is collected and used. This approach also allows for small and large businesses to operate with the same understanding of the law’s requirements and would prevent dominant companies from abusing their market position to circumvent the CCPA.

Browser and Device-Level Signals

Section 999.315 (c) notes that “user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information” should be considered a valid signal. DCN appreciates the desire to find simple solutions for consumers who want to indicate their privacy preferences particularly given the likelihood of multiple consumer options, as well as the involvement of both consumer-facing companies and those that provide functionality from behind the scenes including those that track consumers outside of a consumer’s reasonable expectation. These

⁴ <https://www.iab.com/guidelines/ccpa-framework/>

signals can be useful for consumers as they are persistent and easy to use. They can also be useful for consumer-facing companies as the signals are sent in real-time to all downstream companies. However, there is no widely-adopted industry standard for the messaging and design of these signals that ensures the signals accurately reflect the expressed preferences of consumers. In the absence of additional guidance, we are concerned that there will be a patchwork of signals which could be confusing or misleading for consumers. In addition, we are concerned that some dominant platform companies may develop their own signals in an effort to unfairly tilt the competitive landscape in their favor. Given the potential for confusion and abuse, we encourage your office to rely on the work of-independent, multi-stakeholder, standard-setting groups⁵ to develop guidelines and/or an approval process for how privacy controls such as browser and device-level signals can operate and how they can be advertised to consumers. By developing some common rules for the road, your office will be better able to identify anti-competitive behavior, industry will have more confidence in the signals and consumers will have a better understanding of the benefits and limitations.

Conclusion

Thank you for the opportunity to comment on the proposed regulations regarding the CCPA. We applaud your thoughtful approach to the practical questions for implementing this important law. Please do not hesitate to reach out directly to us with any questions or comments.

Sincerely,



Jason Kint
CEO
Digital Content Next



Chris Pedigo
SVP, Government Affairs
Digital Content Next

⁵ World Wide Web Consortium (W3C) <https://www.w3.org/2011/tracking-protection/>