

## Early Steps Toward Rule-Making For Calif. Privacy Act

By **Grant Davis-Denny** (January 9, 2019, 5:01 PM EST)

Informally at least, rule-making is underway for the California Consumer Privacy Act, the most ambitious privacy law in the United States. The CCPA, signed into law in June 2018, charges the California Department of Justice with responsibility for promulgating the law's implementing regulations.[1] On Jan. 8, 2019, the California Department of Justice held its first informal public forum on the CCPA.

More than 150 people attended the public forum, held in San Francisco. As the meeting prepared to begin, the heavy attendance and the buzz in the room suggested a wave of comments would follow. But fewer than 15 people offered comments to the Justice Department, and after one hour of a scheduled three-hour meeting, the event concluded.

Attendees hoping to learn where the Justice Department might be heading with its draft regulations probably left less than satisfied. The supervising deputy attorney general for the Privacy Enforcement and Protection Unit, Stacey Schesser, explained up front that the Justice Department would be in listening mode during these forums and would not be answering questions or providing feedback on public comments.

At the start of the forum, the Justice Department did identify seven areas of focus for CCPA rule-making:

1. The categories of personal information that will be subject to the CCPA.
2. The definition of "unique identifiers."
3. Exceptions to the CCPA.
4. Submitting and complying with consumers' requests.
5. Developing a uniform opt-out logo or button.
6. What notices and information businesses must provide to consumers.
7. How businesses will need to verify consumer's requests.



Grant Davis-Denny

The Justice Department did not, however, offer any signals on how it would approach these regulatory issues.

We began to see where consumer advocates and the regulated community may focus their efforts during the CCPA rule-making process.

### **Anti-Discrimination Rule**

The CCPA contains a confusing anti-discrimination provision that, on one hand, appears to prohibit companies from offering different goods or services or setting different prices for consumers that exercise their new CCPA rights, and on the other, seems to permit businesses to do exactly that in certain circumstances.[2] (For a more thorough discussion of this provision, please see my previous article.)

Industry groups spoke out against the nondiscrimination rule, raising concerns about how it could, for example, affect customer loyalty programs or arguing that businesses needed to have the flexibility to charge reasonable rates for services as opposed to offering only ad-supported content. But even a Bay Area public interest organization, Media Alliance, acknowledged in its comments that the nondiscrimination provision requires clarification.

Notably, the anti-discrimination provision was not one of the areas that the Justice Department identified in its opening remarks as an area of focus for its rule-making. That is probably because the statute that grants the Justice Department rule-making authority does not expressly reference the anti-discrimination provision.[3] It does, however, give the Justice Department authority to “adopt additional regulations as necessary to further the purposes of this title.”[4] We will have to wait to see whether the Justice Department decides to venture into this aspect of the CCPA in its rule-making proceedings.

### **Safe Harbors And Exemptions**

A number of industry speakers offered that there is a need for safe harbors. In most cases, the contemplated harbors’ boundaries and protections were unclear. There were, however, suggestions that businesses that make efforts to avoid collecting information about consumers should be exempt from the CCPA.

Imagine a business that, for example, facilitates online advertisements by tracking a user’s web browsing. The company does not attempt to link such data to particular individuals by name or email addresses, and in fact attempts to minimize the amount of such data it receives. But because the business may receive an internet protocol address, and because the CCPA’s definition of “personal information” can include IP addresses that can even be indirectly linked to a consumer or household,[5] the business could be subject to the CCPA’s restrictions. Worse yet, because the company would then have to verify requests by consumers attempting to access or delete their data, the company could have to receive, maintain and even link data to consumers in a way that the business had attempted to avoid for data privacy and security reasons. By undermining the business’s attempts to minimize the amount of consumer data it collects, the CCPA could actually end up harming efforts to protect consumer privacy.

The California Chamber of Commerce also raised a concern regarding what businesses’ duty to provide consumers with “specific pieces of personal information” requires.[6] If, for example, it requires transmitting sensitive data such as credit card information back to consumers, that could increase the

risk of data theft through fraud or interception.

## **Employees**

Two speakers urged the AG to clarify that the CCPA is limited to California consumers and does not apply to information that California businesses maintain about their employees. The CCPA's focus, from its very name to the class of individuals to whom it grants new rights, is on consumers. And no one at this forum advocated for the CCPA's application to employees. Employee privacy advocates may, however, point to the CCPA's broad definition of "consumer" as meaning a "natural person who is a California resident."<sup>[7]</sup> and the definition of "personal information" as including "[p]rofessional or employment-related information" to support a broad interpretation of the CCPA.

## **Other Issues**

Speakers raised a number of other issues for the Justice Department to consider. Santa Clara University School of Law professor Eric Goldman urged the Justice Department to clarify the CCPA's definition of "business." Two of the thresholds for qualifying as a "business" are (1) having more than \$25 million in revenue; and (2) annually receiving personal information on 50,000 or more consumers, households or devices. He proposed that the Justice Department should clarify whether these thresholds must be met entirely within California (e.g., a company must have \$25 million in revenue originating in California) or instead can be met with revenue or devices worldwide. Goldman also argued for a "ramp-up" period for complying with the CCPA once a company has, for the first time, satisfied a threshold for becoming a business under the CCPA.

Other speakers cautioned the Justice Department's office that efforts to de-identify or anonymize data are not always permanently successful, argued for the incorporation of particular data security standards into the rule-making, or argued for aligning the CCPA as much as possible with other data privacy regimes, such as the EU General Data Protection Regulation.

## **What's Next?**

Between now and Feb. 13, the Justice Department will be holding five more CCPA forums around the state. We expect that the Justice Department will then turn to preparing draft regulations, a process that could take several months. Following its drafting work, the Justice Department will kick off the formal rule-making process by issuing a notice of proposed rule-making. After that notice and the accompanying draft CCPA rules are released, the public will then have another opportunity to submit comments to the Justice Department. Major changes to the draft rules would require another opportunity for public comment. Given that the Justice Department has until July 1, 2020, to promulgate the final CCPA regulations,<sup>[8]</sup> there may be several drafts of the CCPA regulations released, with each resulting in further public-comment periods.

## **Conclusion**

In short, businesses should plan for the likelihood that the CCPA rule-making process will be lengthy and may last well into the first half of 2020. Meanwhile, the CCPA itself will become operative on Jan. 1, 2020,<sup>[9]</sup> and the AG is authorized to begin bringing enforcement actions on the earlier of July 1, 2020, or six months after the final regulations are published.<sup>[10]</sup> If rule-making continues into 2020, the regulated community could then have just months or weeks to adjust their operations to comply with

the new CCPA regulations before these businesses become subject to potential enforcement proceedings.

---

*Grant Davis-Denny is a partner at Munger Tolles & Olson LLP.*

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*

[1] Cal. Civ. Code § 1798.185.

[2] § 1798.125.

[3] § 1798.185.

[4] § 1798.185(b).

[5] § 1798.140(o).

[6] See § 1798.100(a), 1798.110(a)(5).

[7] § 1798.140(g).

[8] § 1798.185(a).

[9] § 1798.198(a).

[10] § 1798.185(c).