CIVIL JUSTICE
ASSOCIATION OF CALIFORNIA

March 27, 2020

Xavier Becerra, Attorney General
California Department of Justice
1300 I Street, Suite 1740
Sacramento, CA 95814

Lisa B. Kim, Privacy Regulations Coordinator
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

Re: *Comments by the Civil Justice Association of California on Proposed Regulations for the California Consumer Privacy Act, as revised March 11, 2020*

Dear Attorney General Becerra:

The Civil Justice Association of California ("CJAC") appreciates the opportunity to provide comments on this latest version of the proposed regulations implementing CCPA.

CJAC strongly urges the Office of the Attorney General to address two pressing issues that remain completely overlooked in the regulations, namely the need for delayed enforcement of the CCPA and the need to mitigate the private right of action.

We also ask the Attorney General to respond to concerns about previously proposed provisions that remain in the latest version, as well as some of the new changes.

These issues and concerns are detailed below:

1. The regulations should delay enforcement until at least January 1, 2021

CJAC recently signed onto a coalition letter addressed to your Office requesting delay of the enforcement date to January 1, 2021. The business community has repeatedly requested additional implementation time because of the complexity and substantial compliance burden associated with CCPA.

As spelled out in the letter, recent developments surrounding the coronavirus, however, greatly compound the need for additional time. Remote and scattered workforces make development of the complicated systems needed to implement CCPA nearly impossible. The need for delayed enforcement, while important before, is now critical. The fact that implementation of other systems such as tax filing have been delayed underscores the legitimacy of this request.

An even longer implementation time window with an additional year to January 1, 2022 is eminently reasonable and more in line with what was provided for GDPR implementation, which was two years. CJAC previously asked the Attorney General to delay enforcement

until 2022 and again asks for consideration of a longer implementation window.

Alternatively, delayed implementation until at least January 1, 2021 is an extremely modest ask, given the current coronavirus crisis. The regulations should also clarify that any enforcement is prospective only.

2. The regulations should mitigate the potential for unwarranted private rights of action.

CJAC additionally implores the Attorney General to revise the regulations to respond to major concerns expressed by the business community over the potential for unwarranted and unnecessary litigation under the CCPA's private right of action provisions.

There are several ways the Attorney General can mitigate this potential problem while promoting privacy safeguards, including:

- First, the Attorney General should define security standards, such as industry-established standards, that, if met or exceeded by businesses, would serve as a safe harbor from private rights of action under the CCPA. This is critical considering the potential for liquidated damages under the CCPA between $100 and $750 "per incident," without a clear requirement of showing of harm.

- Second, the Attorney General should define what constitutes a "cure," as it is not defined in the CCPA. CJAC proposes that implementation of reasonable security measures should be recognized in the regulations as a cure.

If the policy goal of the CCPA is to discourage consumer data breaches, and the way to prevent data breaches is reasonable security measures, then the regulations should recognize and incentivize this desired behavior. If businesses are subject to private rights of actions and penalties regardless of security steps they take, then the lawsuits and penalties are meaningless hammers and ripe for abuse. On the other hand, adoption of clear standards will promote ubiquitous adoption of best security practices.

3. The requirement to treat global privacy controls as opt-out requests should be eliminated due to technological and consumer choice limitations. (Section 999.315(a), (d).)

We continue to oppose the requirement that a business detect and treat global privacy controls, such as browser plug-ins or device settings, as valid consumer requests to opt out of the sale of personal information. This requirement is not technologically feasible and limits consumer choice.

From a technology standpoint, a major problem is that browser and global device settings are not designed to consistently convey affirmative user choice, versus the pre-selected choice of a third party such as the browser company, operating system provider, or internet service provider. Moreover, not every browser clearly communicates whether a user is a California resident.

Treating global settings as opt-outs will therefore limit consumer choice and access to online content. For example, consumers will likely be asked to pay for what would otherwise by free, ad-supported content or be blocked from access. Moreover, treating settings that may have been pre-selected by third parties, rather than the user, will empower large technology platforms to dictate content access rather than the consumer.

In this vein, CJAC requests the that "shall" be changed to "may" under 999.315(d) and the last sentence of (d)(1) be reinstated:

> (d) If a business collects personal information from consumers online, the business ~~shall~~ may treat user-enabled global privacy controls, such as a browser plugin or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.
>
> (1) Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to the opt-out of the sale of personal information. The privacy control shall require that the consumer affirmatively select their choice to opt-out and shall not be designed with any pre-selected settings.

Without these changes, the result will ultimately be less free and beneficial content online for consumers. Already-struggling content providers such as independent publishers and news outlets will see less traffic and fewer opportunities to generate revenue through advertising.

4. New restrictions on service providers should be removed, as they are inconsistent with the CCPA. (Section 999.314(c).)

The new restrictions placed on service providers in section 999.314(c) concerning the use, disclosure, and retention of personal information go beyond the statute. Civil Code section 1798.140(v) permits service providers to use personal information pursuant to ***any*** contract for a business purpose, not just contracts for services required by CCPA. Furthermore, it allows processing of information by the service provider so long as it is for the specific purpose spelled out in the contract or otherwise permitted by statute:

> (v) "Service provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, ***that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the***

> ***business, or as otherwise permitted by this title,*** including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business (emphasis provided).

We therefore ask that section 999.314(c) be struck in its entirety, since it exceeds the scope of the statute. Alternatively, the section should be restored to the February 10 version.

5. **The requirement to quantify financial incentives and the value of consumer data should be eliminated because it provides no benefit and could be misleading. (Sections 999.307(b), 999.336, and 999.337.)**

We again ask the Attorney General to eliminate the requirement that businesses make and disclose calculations about financial incentives and data value.

Requiring businesses to assign a number to incentives and data value provides little or no consumer benefit and can be misleading. Financial incentive programs are often based on a complex calculation of costs to the business and market comparisons, and they are designed to reward loyal customers rather than to serve as a value exchange. Additionally, a single customer's business or data holds little independent "value," since data gains value when it is aggregated.

The Attorney General should remove this quantification requirement from the regulations altogether, or alternatively, the Attorney General could simply require businesses to disclose whether they have a financial incentive or whether the data has value.

6. **The requirement that businesses reimburse consumers for costs associated with verification is unworkable and should be removed. (Section 999.323.)**

Section 999.323 prohibits a business from requiring the consumer to pay a fee for verification. While CJAC does not oppose a prohibition on businesses collecting a fee, we continue to object to businesses having to provide reimbursement for steps individuals may need to take to verify their identity. Requiring businesses to provide reimbursement for the multitude of ways in which consumers may verify their identity fails to consider the potential volume of these requests and resulting operational burdens on businesses.

7. **The regulations should restore and expand guidance on information exempted from disclosure and deletion requests for security and other reasons. (Sections 999.302, 999. 313(c)(3), 999. 313(d)(3).)**

In our last set of comments, CJAC expressed our appreciation for the new guidance provided in now-deleted section 999.302 interpreting the term "personal information." We are disappointed to see the latest proposed revisions eliminate this guidance and ask that it be restored.

Additionally, we had asked previously that the deleted portion of section 999.313(c)(3) be restored, but it was not. The deleted portion allowed a business to forgo disclosure that "creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks." This is a critical basis for not disclosing information and should be

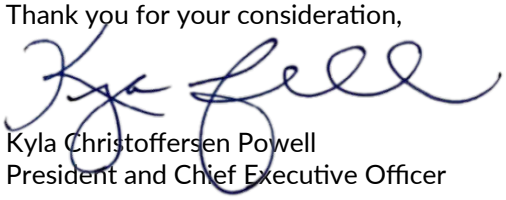
restored. Finally, we re-ask that clarifications a.-d. that were added in the February 10 revisions to section 999.313(c)(3) be added to deletion requests in section 999.313(d)(3).

Conclusion

CCPA regulations that are unworkable or unduly burdensome will give rise to unnecessary and unproductive enforcement actions and litigation. We again stress that the goal of the regulations should be to facilitate implementation of and compliance with the CCPA. This will benefit consumers, while reducing unnecessary litigation burdens on businesses, the courts, and your Office.

We are happy to answer any questions you may have and look forward to the opportunity to work with your Office on improvements to the regulations.

Thank you for your consideration,



Kyla Christoffersen Powell
President and Chief Executive Officer