CIVIL JUSTICE
ASSOCIATION OF CALIFORNIA

February 25, 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 February 10, 2020*

Dear Attorney General Becerra:

The Civil Justice Association of California ("CJAC") is a more than 40-year-old nonprofit organization representing a broad and diverse array of businesses and professional associations. A trusted source of expertise in legal reform and advocacy, we confront legislation, laws, and regulations that create unfair litigation burdens on California businesses, employees, and communities.

As noted in our prior comments, many businesses attempting to comply with the CCPA find it complex and vague, making implementation difficult. CJAC appreciates the additional clarifications the Office of the Attorney General provided in the February 10, 2020 revisions, such as clarifying the definition of personal information, but we are concerned the revised regulations still have gaps or impose unnecessary burdens. Below, we itemize our concerns and requests.

1. **The regulations should provide that enforcement is effective on January 1, 2022 and prospective only given the complexity and burden of implementation.**

CJAC reiterates our request for additional time for businesses to implement the regulations before they are enforced, to January 1, 2022. The latest revision does not specify an extended effective date for enforcement purposes, notwithstanding requests from CJAC and a multitude of other commenters to so do.

While the CCPA states the Attorney General should adopt regulations by July 1, 2020 and enforce no earlier than that date, there is nothing limiting the Attorney General from specifying an extended enforcement date. Given the complexity of the CCPA and the proposed regulations and the substantial compliance burden on businesses, a delayed enforcement date is necessary and justified. For the same reasons, the regulations should also provide that all enforcement of the CCPA and the regulations is prospective only, from the extended enforcement date.

If not an overall extension, at a very minimum, the Attorney General should provide delayed enforcement for the regulations that are more burdensome and complex to implement, such as the requirement to treat global controls as opt-out requests under section 999.315.

2. **Businesses should not be required to treat global privacy controls as opt-out requests because it is technologically unworkable and limits consumer choice. (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 feasible from a technology standpoint and limits consumer choice.

These global control technologies were designed for other contexts that are not compatible with the CCPA's complex and extremely broad definitions of "sale" and "personal information." As a result, this regulation will be very difficult to operationalize and will lead to inconsistent approaches. One reason is lack of uniformity in what constitutes a browser setting or plug-in and which mechanisms reflect genuine user intent. Also, not every browser communicates clearly which users are in California. Finally, there is insufficient interoperability among the technologies to be workable.

This requirement also runs contrary to consumer choice. Plug-ins and device settings do not clearly convey whether a consumer truly wants to opt out of the sale of personal information in every context. Moreover, treating global controls as opt-outs will also harm competition by favoring a few large advertisers who have direct relationships with consumers. This will lead to lower revenues and higher costs for smaller operators. Ultimately, the result will be less free and beneficial content online for consumers. Consumers will not be aware of these trade-offs when they click on a global device setting.

Alternatively, if the Attorney General continues to require treatment of these technologies as opt-outs, then the regulations should provide industry with additional time, until January 1, 2022, to implement this requirement so that industry can work to develop consistent and accurate technical signals that truly reflect consumer choice.

3. **The record-keeping requirements are unduly burdensome and need to be simplified. (Section 999.317(g).)**

While CJAC appreciates that the revised regulations narrowed the category of businesses that must comply with record keeping requirements, unfortunately, the revisions also created new reporting requirements making them even more onerous. The costs and burden associated with these record-keeping requirements far outweigh any possible benefit to consumers. These requirements need to be simplified rather than expanded.

4. **The requirement to quantify financial incentives and the value of consumer data should be eliminated as impractical and misleading. (Sections 999.307(b), 999.336, and 999.337.)**

Rather than require businesses to make calculations about financial incentives and data value, the Attorney General should simply require businesses to disclose whether they have a financial incentive or whether the data has value. Most consumers are savvy enough to know this is often the case in any event.

Requiring businesses to assign a number to incentives and data value provides little or no consumer benefit and could be misleading. Any metric or value assignment is subject to numerous variables that can change from day to day, such as a business's operational changes and market fluctuations. Additionally, 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. Finally, a single customer's business or data holds little independent "value," since data gains value when it is aggregated. These factors render any attempt to quantify and disclose financial incentives or data values an unreliable and unproductive exercise.

The Attorney General should remove this quantification requirement from the regulations.

5. **The regulations need to further clarify and define information exempted from disclosure and deletion requests for security and other reasons. (Sections 999.302, 999. 313(c)(3), 999. 313(d)(3).)**

CJAC welcomes the Attorney General's added guidance recognizing that certain information should not be provided upon request, for consumer protection and other important reasons. However, this guidance needs further clarification and expansion to recognize other circumstances in which personal information should not be provided, including the following:

- The new guidance provided in section 999.302 for interpreting the term "personal information" is helpful but should be expanded to include pseudonymous or de-identified information. While such information could be linked to an individual, it is not in practice. A business often maintains such information in de-identified fashion as a privacy safeguard, using technical and administrative controls such as hashing, encryption, and contractual safeguards to prevent its linkage to an individual. The European Union's General Data Protection Regulation recognizes this as a good practice. Thus, we propose the following edit to section 999.302:

> Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household." For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, ~~and could not reasonably link the IP address with a particular consumer or household,~~ then the IP address would not be "personal information."

- Similarly, the clarifications in section 999.313(c)(3) are helpful in exempting from right to know requests personal information that a business maintains in backup or archive systems. However, the deleted portion that allowed a business to forgo disclosure if it "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" should be restored. This is a critical basis for not disclosing information and is in the public interest.

- Finally, the clarifications a.-d. added in the revisions to section 999.313(c)(3) are also applicable to, and should be added to, deletion requests in section 999.313(d)(3).

6. **The regulations should recognize WCAG version 2.0, in addition to version 2.1, as an acceptable standard for accessibility of online notices. (Sections 999.305(a)(2)d., 999.306(a)(2)d., 999.307(a)(2)d., and 999.308(a)(2)d.)**

The notice sections of the revised regulations newly require businesses to follow generally recognized industry standards for web accessibility. CJAC agrees with this requirement, but it is now unclear whether the Attorney General will enforce the provided example of industry standards – Website Content Accessibility Guidelines (WCAG), version 2.1, recently adopted on June 5, 2018.

CJAC agrees that 2.1 is a recognized industry standard, but so too is the earlier 2.0 standard. The United States Access Board recently adopted and applied 2.0 in the latest refresh of Section 508 of the Rehabilitation Act of 1973. While the 2.1 standard is the most recent issued by the World Wide Web Consortium, many businesses are already in the process of bringing their website accessibility up to the 2.0 standards. Web updates are a lengthy and costly undertaking for small businesses in particular. If they must now pivot their development to 2.1, this will require substantial new development which will be a heavy burden, especially when combined with the other weighty burdens of complying with CCPA.

Therefore, we request the Attorney General to revise these sections to specify WCAG version 2.0 and above as the example of an acceptable industry standard. Alternatively, the Attorney General should provide a delayed enforcement date of January 1, 2022 before holding any business to the 2.1 standard.

7. **The Attorney General should provide more flexibility for what is required in the notice at collection to allow for a better customer experience. (Section 999.305(a), (b).)**

The requirements of additional detail that must be included at the notice of collection in the revised regulations under section 999.305(a)(3)-(4) and (b) are burdensome and do not leave enough flexibility for businesses to provide a good customer experience. Most online users want their experience to be seamless, quick, and simple. The additional requirements will create a cumbersome and clunky customer experience. We ask the Attorney General to revisit these requirements and either scale them back or build in flexibility so that consumers get the notification they need without compromising their user experience.

8. The requirement that businesses reimburse consumers for costs associated with verification is unworkable. (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 do object to businesses having to provide reimbursement for steps individuals may need to take to verify their identity.

For example, this section provides obtaining a notarized affidavit as an example of verification that a business must reimburse. In some cases, such as when the individual does not have an account or sufficient information on-hand, securing a notarized document may be the only way to verify identity. As another example, if a consumer decides to verify by providing a copy of a government record, should a business be required to reimburse the cost of obtaining the record?

Requiring businesses to provide reimbursement for all the ways in which consumers may verify their identity overlooks the potential volume of these requests and will create tremendous operational challenges for businesses.

9. The Attorney General needs to mitigate the potential for unwarranted private rights of action.

CJAC is extremely disappointed the revisions do not respond to a major concern expressed by the business community – mitigation of unwarranted and unnecessary litigation under the CCPA's private right of action provisions. The Attorney General, though regulations, is well-positioned to promote adoption of security practices that protect consumers by providing clarity on security standards that satisfy CCPA and incentivizing businesses to meet these security standards.

There are several ways the Attorney General can accomplish this, 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. 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 a related note, 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 not that, what else qualifies as a cure?

CJAC urges the Attorney General to mitigate potential abuses of the private right of action and to promote ubiquitous adoption of best security practices through these additional revisions to the regulations.

Conclusion

CCPA regulations that are unworkable or unduly burdensome will give rise to unnecessary and unproductive enforcement actions and litigation. The goal of the regulations should be to facilitate implementation of and compliance with the CCPA. This is a win-win for consumers and businesses – not to mention a reduced enforcement burden for 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