



CIVIL JUSTICE
ASSOCIATION OF CALIFORNIA

December 6, 2019

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

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*

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 burdens on California businesses, employees, and communities. Toward that end, CJAC offers research and guidance on policy issues that impact civil liability issues, including the following comments on the Attorney General's proposed regulations (§§ 999.313(c)-(d), 999.323) defining the scope and application of the California Consumer Privacy Act (CCPA).

Many businesses attempting to comply with the CCPA find it complex and vague, making implementation difficult. The regulations can serve to provide needed clarifications and guidance to businesses. CJAC appreciates the significant work of the Office of the Attorney General to date in developing the proposed regulations and the clarifications they do provide. For example, the balancing tests laid out for responding to personal information requests – weighing the benefit to the consumer versus security risks – is a helpful clarification. (§§999.313(c.), 999.323.) Additionally, providing guidance on acceptable forms of deletion, such as deidentification, also provides guidance that strikes a proper balance between consumers' rights and business and public benefit. (§999.313(d).)

As spelled out below, however, CJAC has some concerns, that some areas of the regulations do not provide necessary clarifications, are too burdensome, or have significant gaps.

Regulations needing revision due to lack of clarity or undue burden:

- **§ 999.313(b) Responding to Requests to Know and Requests to Delete.** This proposed regulation states that the 45-day deadline to respond begins to run on the day the business "receives a request, regardless of time required to verify the request." This deviates from the CCPA which states that a business must disclose

and deliver required information to a consumer within 45 days upon “receiving a *verifiable* request.” (Civil Code § 1798.130)(a)(2)(emphasis supplied).) Rather than making the 45-day deadline more stringent than the statute, the regulations should provide guidance on what is a reasonably verifiable request, as directed by the CCPA under Civil Code §1798.140(y): “‘Verifiable consumer request’ means a request made by a consumer ... that the business can reasonably verify, pursuant to regulations adopted by the Attorney General.” Accordingly, the 45 days should only begin to run if the consumer request is reasonably verifiable. Indeed, under the same section, a business has no obligation at all to provide the information if the business cannot verify the consumer. (Civil Code § 1798.140(y).)

Alternatively, this regulation should clarify that the “necessity” required to “take up to an additional 45 days” [beyond the first 45 days to respond to a consumer’s request to know or delete information] is satisfied if the business has been unable to “verify” the consumer’s identity. The regulation recognizes businesses’ responsibility to verify requests properly, a task that may take days or weeks to complete and is reliant upon a consumer’s cooperation in providing accurate information in a timely manner. After a request is “verified,” a company must then find the information it holds on a consumer – information which may be kept in separate databases – and convert it into a form which can be delivered to the consumer. Since “receipt of the request” itself initiates the initial 45-day period, businesses seeking to comply and avoid liability are spurred to ascertain that the request is made by the consumer and not an imposter. Specifying that a business is entitled to the 45-day extension if the consumer’s identity cannot be verified within the first 45-day period furthers the public interest.

- **§ 999.313(d)(1) Responding to Requests to Delete.** Consumer requests to delete personal information that cannot be verified should not be treated as “opt-out” requests. Businesses should act upon requests when a consumer expresses a clear preference, but regulations should not presuppose a consumer’s choice by treating an unverified delete request as a “do not sell” preference. Additionally, this presupposition could result in businesses having to opt out all non-Californians who make a deletion request, if they are unable to verify the consumer’s California residency status. The CCPA provides consumers with several distinguishable rights to exercise. Requiring businesses to conflate these requests reduces real consumer choice inconsistent with the CCPA.
- **§ 999.315(c) & (g) Requests to Opt-Out.** CJAC has serious concerns and doubts about the viability of the requirement that businesses treat browser plug-ins or settings as “opt-out” requests under the CCPA. These technologies were designed for and in other contexts that are not compatible with the CCPA’s complex and extremely broad definitions of “sale” and “personal information.”

The CCPA emphasizes consumer choice and defines a mechanism – the “Do Not Sell” button – that businesses must make available on their Web sites so consumers can exercise choices. It is not consistent with the statute to create this additional mechanism, nor is it clear that consumers, who use plug-ins, intend to use them to opt out of CCPA sales.

Browser-based opt-out technology is not now sufficiently interoperable and developed to ensure that all parties that receive such a signal can make it operable. Accordingly, CJAC instead supports industry-based efforts for more than a year to develop consistent technical signals for “Do Not Sell” technology.

- **§ 999.325 (c) Verification for Non-Accountholders.** This regulation should be revised to clarify that a business's execution and maintenance of "a signed declaration under penalty of perjury" to verify consumer requests is optional. The regulation indicates this is an option among others by stating that "a reasonably high degree of certainty *may* include ... a signed declaration under penalty of perjury" (emphasis supplied). An optional approach is appropriate, as a blanket requirement would be burdensome and unnecessary given the technological ability to obtain "verification."
- **§ 999.314 (c) Service Providers.** This regulation restricts service providers beyond the intent of the CCPA, which allows a business, under certain circumstances, to use or share personal information with a service provider that is necessary for a legitimate business purpose. The proposed regulation, however, limits what businesses and service providers may do with data in a way that is unnecessary and threatens to harm the data economy. For example, given the broad definition of "personal information," this provision restricts a business's ability to use its data for legitimate business purposes agreed to by contract where personal information will not be sold but only used by the service provider to provide services to the business. This proposed regulation goes beyond the standards defined by the CCPA.
- **§ 999.316(a) Requests to Opt-In to the Sale of Personal Information.** Requiring a two-step opt-in process as this provision would do is unnecessary and creates consumer confusion. This requirement is neither consistent with other laws nor consumer expectations. It requires businesses to build new systems that make users jump through unnecessary hurdles to express a preference. It nudges consumers toward a course of action rather than empowering them to make their own decisions in a straightforward manner.

It is also inconsistent with the regulation allowing businesses to use personal information for additional purposes beyond those previously disclosed to the consumer with explicit consent rather than a two-step opt-in process. (§999.305(a)(3)). The CCPA expressly adopts an "opt-out" regime rather than one that is "opt-in", making this proposal inconsistent with the statute. (*See*, §§1798.115, 1798.120.) Further, data protection principles typically do not require additional consent for use of data that is consistent with the context in which the consumer receives the service.

- **§ 999.317 Training; Record-Keeping.** The reporting requirements exceed the scope of the CCPA and are not related to its purposes. Nowhere in the CCPA is there a provision regarding record-keeping, and it is unclear what policy goal this requirement seeks to fulfill. It imposes a burden on businesses which does not appear tied to consumer benefits or rights and requires the collection of additional personal information beyond the scope of the CCPA.

Imposing additional record-keeping and disclosure requirements on businesses that handle the personal information of 4 million or more consumers is unwarranted. The CCPA requires businesses to provide multiple disclosures to consumers, and this regulation's requirement for more information does not provide them with a greater understanding of their privacy protections.

- **§ 999.307(b)(5) Notice of Financial Incentive.** This regulation requiring disclosures about financial incentives is impractical and threatens confidential, competitively sensitive information. It is challenging for any business to assign value to a single consumer's data, and data often gains value when it is aggregated. Consequently, financial incentive programs will more likely be based on a complex calculation of costs to the business and market comparisons that is unlikely to be meaningful to consumers.

There are significant differences between businesses and the services they provide. Requiring all businesses to disclose its methods and calculations will likely require disclosure of competitively sensitive information. The CCPA is sufficiently protective of consumers with regard to discounts; and this regulation unnecessarily goes beyond that protection.

- **§ 999.305(d)(2) Notice at Collection of Personal Information.** Greater flexibility respecting notice before resale of data is needed. Regulations should clarify that a business receiving personal information from an indirect source may comply with CCPA obligations by written agreement requiring other businesses to provide the requisite notice to consumers. Requirements to contact the "source" and obtain "signed attestations" are burdensome and unnecessary.
- **§ 999.301(e) "Categories of third parties".** The definition of "categories of third parties" is overly broad. Internet service providers (ISPs) and social networks, for example, generally have a direct relationship with consumers. Although some may receive personal information indirectly at times, ISPs and social networks that do not do so should be removed from the third-party definition.

Regulations that are missing:

- **Regulations should specify that enforcement will be delayed until January 1, 2022.** Since the CCPA does not dictate an effective date for regulations, the Attorney General has discretion to establish an effective date for enforcement purposes. The CCPA merely states the Attorney General should "adopt regulations" by July 1, 2020 and provides that the *earliest* date that such enforcement could be brought is "six months after the publication of the final regulations ... or July 1, 2020, whichever is sooner" (emphasis supplied). Given the complexity of the CCPA and the proposed regulations and substantial implementation and compliance burden on businesses, a delayed enforcement date is necessary and justified.
- **Regulations should clarify the jurisdictional scope of the CCPA.** The CCPA's broad definition of "business" suggests a sweep within its ambit of non-U.S. businesses that incidentally collect personal information about a single California resident. Regulations should clarify that a business whose operations are outside of California and who only collect a *de minimis* amount of personal information from California residents are not required to comply with CCPA. Alternatively, the regulations should provide that businesses operating outside California that do not target their services to California residents are not subject to the CCPA.
- **Regulations are needed to clarify the CCPA's "private right of action."** The CCPA specifies that recoverable "statutory damages" – *i.e.*, those "not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per

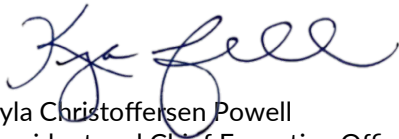
consumer per incident” – may only be sought if a consumer first gives the defendant 30 days written notice of the violations and an opportunity to “cure” them.

“Cure” is not defined in the CCPA provision. While not the subject of the proposed regulations, the proposed privacy initiative for the November 3, 2020 ballot adds a sentence to this section (which does not take effect until January 1, 2023, three years after its enactment) stating that the “implementation and maintenance of reasonable security procedures and practices . . . following a breach does *not* constitute a cure with respect to that breach.” So while we know what does *not* constitute a “cure” from the initiative, we don’t know what qualifies as one under it or CCPA.

Does omission of this sentence in the CCPA mean that the “implementation and maintenance of reasonable security procedures and practices” by a business within the 30-day notice period *does* count as a “cure”? CJAC submits that it should. Additionally, the regulations do not provide guidance on what is “reasonable security,” which is also not defined by the CCPA and ripe for litigation. These uncertainties can and should be clarified by regulation.

Gaps in needed clarification or regulations that are too 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 – a win-win for consumers and businesses.

Thank you for your consideration,

A handwritten signature in blue ink, appearing to read 'Kyla Powell', written in a cursive style.

Kyla Christoffersen Powell
President and Chief Executive Officer