U.S. Chamber of Commerce
Technology Engagement Center

**JORDAN CRENSHAW**
*Executive Director and Policy Counsel*

1615 H STREET, NW
WASHINGTON, DC 20062-2000
(202) 463-5632
jcrenshaw@uschamber.com

March 27, 2020

**VIA ELECTRONIC FILING**

Ms. Lisa B. Kim
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, California 90013

**RE: Second Set of Modifications to Text of Proposed Regulations (OAL File No. 2019-1001-05)**

Dear Attorney General Becerra and Ms. Kim:

The U.S. Chamber of Commerce ("Chamber") respectfully submits these comments in response to the second set of modifications to the proposed regulations ("Proposed Regulations") to implement the California Consumer Privacy Act ("Act" or "CCPA"). The Chamber continues to pursue a national privacy standard that protects all Americans equally and is working to ensure that privacy laws give consumers and business certainty. It is for this reason that the business community applauds revisions to the proposed regulations that effectively protect consumers without added confusion.

## I. POSITIVE CHANGES TO THE PROPOSED REGULATIONS IN THE INITIAL MODIFICATIONS

The first set of modifications made many significant improvements such as eliminating the two-step deletion mandate at Section 999.312(d). The modification provided needed flexibility for business working to delete personal information.

Another positive change the Chamber applauds revisions in the first set of modification Proposed Regulations at Section 999.313(d)(1). Eliminating the originally proposed requirement that a business treat an unverified request to delete as a request to opt out of sale was a first step in the right direction.

## II. FINANCIAL INCENTIVE PROGRAMS

CCPA prevents covered businesses from engaging in "discriminatory" practices such denying goods or services, charging different prices, or giving a different level of quality, against

consumers that exercise their privacy rights under the Act.[1] An overly broad interpretation of the Anti-Discrimination rights in CCPA threatens the ability of retailers, airlines, restaurants, and entertainment companies to offer loyalty and reward programs that greatly benefit consumers. According to one study, the overwhelming majority of consumers agree that loyalty programs save them money.[2] The Chamber strongly urges the Attorney General to interpret CCPA in a manner that ensures that the consumers continue to enjoy loyalty and rewards programs without disruption to businesses or their customers.

Although the Act prohibits discrimination against consumer who exercise privacy rights, CCPA permits covered businesses to offer financial incentives for data collection, sales, and deletion if the difference in price or quality of goods and services "is directly related to the value provided to the business by the consumer's data."[3] The covered entity must also provide notice to consumers and receive prior opt-in consent to enroll consumers in the incentive program.[4]

The first revisions in February included several guidelines to follow for businesses that offer a financial incentive for a customer based upon the value of that customer's personal information. For example, businesses should provide a notice of financial incentive to customers in a way that is "easy to read" and uses "a format that draws the consumer's attention to the notice." The newest revisions at Section 999.301(j) define a "financial incentive" to be a benefit related to the *"collection, retention, or sale of personal information."*[5] This is a change from the February proposal which defined a financial incentive to be a benefit related to the *"disclosure, deletion, or sale"* of personal information. These changes, as well as the continued reference to a benefit "related to" the collection, retention, or sale of data (as opposed to "compensation" which is the term included in the text of the CCPA), creates uncertainty for businesses and could be broadly interpreted once enforcement begins. Such uncertainty threatens the affinity and loyalty programs consumers enjoy.

## III. PERSONAL INFORMATION.

The clarification language in 999.302 as to what constitutes personal information should be restored. It provides businesses with important clarifications as to what is considered personal information.

## IV. SECURITY

We urge the reinstatement of the critical exception that was included in the original version of § 999.313(c)(3) which provided that:

---

[1] CAL. CIV CODE § 1798.125(a).
[2] Emily Collins, "How Consumers Really Feel About Loyalty Programs," FORRESTER (May 8, 2017) *available at* http://www.oracle.com/us/solutions/consumers-loyalty-programs-3738548.pdf.
[3] *Id*. at §1798.125(b)(1) as modified by the legislature.
[4] *Id* at § 1798.125(b)(2)-(3).
[5] Modified Privacy Regulations Comparison at 2 (March 11, 2020) *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-second-set-mod-031120.pdf?.

*A business shall not provide a consumer with specific pieces of personal information if the disclosure 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 exception was tightly drafted and addressed the very real risk of "pretexting" requests for personal information.

This risk is heightened because other parts of the proposed rules would allow third party authorized agents to obtain access to and delete personal information of individuals. In this environment, fraudsters, cyber criminals and even foreign intelligence services may attempt to abuse the CCPA access right to obtain personal information about California residents to carry out illicit activities to commit fraud, engage in identity theft, access unauthorized accounts, or other harmful practices. By allowing businesses to protect against these threats only through verification procedures, businesses will not be able to prevent harm to consumers since bad actors may well be able to obtain the requisite number of verifying data elements through phishing or other tactics in order to falsify an authorization request.

For these reasons, we encourage the AG to restore this vital exception in order to avoid undermining the privacy of Californians' personal information in ways that can be very damaging and to prevent placing businesses in a position where they have to choose between compliance and security.

## V. GLOBAL PRIVACY CONTROLS.

The Chamber once again requests the removal of the provisions on global device settings contained in sections 999.315(a) and (d), as these present challenges for both competition and implementation. In 999.315(d)(1) the sentence was removed relating to pre-selected settings. Note that as originally written it was confusing because it was not clear that allowing sale should be the default (i.e., the "pre-selected" setting), but at a minimum, the first clause must be restored ("The privacy control shall require that the consumer affirmatively select their choice to opt-out"). Without this, there exists a risk that consumers will inadvertently be opted-out of sale without having had an opportunity to actually make that selection. Consumer control is a fundamental tenet of the California Consumer Privacy Act. A number of services feature pre-selected settings that would seem to have the effect of opting consumers out of sale automatically. By establishing that these services can constitute a valid request to opt out, the regulations would deprive consumers of the information and tools necessary to make this choice and to exercise this control independently. Nor would mere use of such a service constitute authorization for another person to opt a consumer out of sale, if the elements of notice and choice are missing.

Products containing pre-selected settings have also been developed in a context and for a purpose that differ from the CCPA and its concept of sale. As such, they do not "clearly communicate or signal that a consumer intends to opt out of the sale of personal information," as

section 999.315(d)(1) of the proposed Regulations provides. For these reasons, the Chamber continues to oppose the requirement that a global device setting constitute a valid consumer request to opt out of the sale of personal information. If this requirement must remain, the Chamber requests the re-insertion of the sentence that has been deleted from section 999.315(d)(1).

## VI. The Requirement in § 999.305(a)(5) to Obtain Opt-in Consent for Specific Data Uses Is Inconsistent with the Statute

We appreciate that the explicit consent requirement in this section has been cabined somewhat through a "materially different" standard. However, we remain concerns that the requirement that an entity must "directly notify" and "obtain explicit consent" from consumers in order to use a consumer's personal information for a purpose materially different than what was disclosed in the notice at the time of collection goes beyond the scope of what the underlying statute provides. Civ. Code §1798.100(b) clearly states that use of collected personal information for additional purposes should be subject to further notice requirements only.

The drafters of the CCPA required the further step of obtaining explicit consent from a consumer only for the sale of a minor consumer's personal information[6], participation in an entity's financial incentive program[7], and retention of a consumer's personal information for the purposes of peer-reviewed scientific, historical, or statistical research in the public interest[8]. Requiring explicit consent beyond these well-defined and clearly cabined use cases in the statute goes beyond the scope of the CCPA.

## VII. REPORTING REQUIREMENTS

The reporting requirement in Section 999.317(g) should be deleted or at the least be greatly simplified and eliminate the requirement to have the metrics posted in the privacy policy. This reporting requirement does not exist in the CCPA and has no support in the law. In addition, the requirement is very burdensome -- a business that buys, sells, or receives/shares for a commercial purpose, the personal information of 10 million+ consumers in a year shall compile metrics on data rights requests and disclose them in its privacy policy.

## VIII. THE ATTORNEY GENERAL SHOULD DELAY ENFORCEMENT TO ENABLE EFFECTIVE COMPLIANCE

As previously asserted in the Chamber's initial comments on the Proposed Regulations, any major rules should give the regulated community adequate time to institute compliance

[6] Civ. Code §1798.120(d).
[7] Civ. Code §1798.125(b)(3).
[8] Civ. Code §1798.105(d)(6).

programs. The State's Regulatory Impact Analysis ("RIA") estimates that the Regulations will cover up to 570,066 California companies, the vast majority of which are small businesses and will cost up to **$55 billion** in compliance costs for California companies alone.[9] The State's RIA assumes that the Regulation will require companies with fewer than 20 employees to incur up to $50,000 in compliance costs.[10] In order to give consumers more certainty about proper implementation of CCPA, giving companies the ability to know what the final Regulations are and have adequate compliance time will be paramount. Unfortunately, according to a July 2019 nationwide survey that poll mostly small businesses, only 11.8 percent of companies knew if CCPA applied to them.[11] Many small businesses are just becoming aware of CCPA and will need adequate time to develop solutions to protect consumers' CCPA rights.

Many small businesses must rely on technological solutions to be developed and become available many months before the new law's effective date in order to implement the CCPA's new requirements. With regulations anticipated to be finalized no more than a couple months before the statutory enforcement date, the narrow window of compliance time makes the successful adoption of these solutions industrywide unlikely. As witnessed in Europe's implementation of the General Data Protection Regulation ("GDPR), a robust market for solutions to new privacy regulations takes time to develop and can only get started once the implementing regulations are in final form. The Chamber asserts that the time Europe gave companies to comply with GDPR-two years—represented an adequate and reasonable timeframe. Unfortunately, given the current status of the Proposed Regulations, businesses now have no more than three months between final promulgation of rules and the July 1, 2020 enforcement date.

In addition to the reasons stated in previous comments and above, the COVID-19 pandemic is also causing heavy financial strain for companies—particularly small businesses. The coronavirus outbreak further compounds the problems that small business will face having to change business models within a short timeframe before July 1. For the time being, businesses should focus their resources on coronavirus efforts and operations affected by government responses to the pandemic. Although the Chamber has advocated for delaying enforcement until 2022, in light of recent circumstances, we ask the Attorney to give companies an extra six months at a minimum.

Californians deserve to have their privacy protected in ways that are both strong and responsibly implemented. A delayed enforcement date protects consumers from rushed and potentially incomplete compliance programs, and maximizes the ability of businesses to provide consumers with their privacy rights. Consumers benefit when they can trust that companies have

---

[9] *See* Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, State of California Department of Justice and Office of the Attorney General at 11 (August 2019) *available at* http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

[10] *Id.*

[11] *See* ESET CCPA Survey Results (July 19-22, 2019) *available at* https://cdn1.esetstatic.com/ESET/US/download/ESET_CCPA_Survey_Results.pdf.

built well-planned compliance and accountability programs to protect their statutory privacy rights.

Sincerely,

Jordan Crenshaw
Executive Director & Policy Counsel
Chamber Technology Engagement Center