

CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

TIM DAY
SENIOR VICE PRESIDENT
CHAMBER TECHNOLOGY
ENGAGEMENT CENTER (C_TEC)

HAROLD KIM
CHIEF OPERATING OFFICER
U.S. CHAMBER INSTITUTE
FOR LEGAL REFORM

December 6, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Proposed California Consumer Privacy Act Regulations

Dear Attorney General Xavier Becerra:

The U.S. Chamber of Commerce (“Chamber”) respectfully submits these comments in response to the proposed California Consumer Privacy Act (“CCPA” or “Act”) regulations (“Regulations”) put forward by the Attorney General.¹ As national economic growth becomes increasingly reliant on data-driven innovation, consumers should be able to have certainty that companies respect personal information. Congress should enact a national privacy law that protects *all* Americans equally regardless of which state they call home. The Chamber’s 225-member company Privacy Working Group, comprised of all industry sectors and small, medium, and large businesses, adopted principles for a national privacy framework during October 2018.² In furtherance of these principles, the Chamber proposed model privacy legislation to Congress on February 13, 2019, which draws upon many of the provisions of CCPA including information, opt out and deletion rights.³

Unfortunately, the CCPA, due in part to time pressures on the State of California (“State”) to pass privacy legislation before the deadline to remove a ballot initiative in 2018, contains many inconsistencies and ambiguities that makes it difficult for companies acting in good faith to operationalize its requirements. Complicating matters is the ongoing proposed ballot initiative known as the California Privacy Rights Act (“CPRA”)⁴ which would change many of CCPA’s requirements after companies spent time investing in compliance with the original Act.

¹ See Notice of Proposed Rulemaking, California Department of Justice (Oct. 11, 2019) *available at* <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-nopa.pdf>.

² See U.S. Chamber Privacy Principles (October 2018) *available at* https://www.uschamber.com/sites/default/files/9.6.18_us_chamber_-_ctec_privacy_principles.pdf.

³ See U.S. Chamber Model Privacy Legislation (February 13, 2019 updated June 18, 2019) *available at* https://www.uschamber.com/sites/default/files/uscc_dataprivacymodellegislation.pdf.

⁴ See Proposed California Privacy Rights Act (November 13, 2019) *available at* https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.

Because of statutory deficiencies, an unreasonable amount of time for companies to comply, and many ambiguities and requirements exceeding the authority of the CCPA, the Regulations will have a serious and deleterious effect on the national economy. According to the State’s own Regulatory Impact Assessment (“RIA”), the proposed CCPA Regulations will cost up to **\$55 billion** in compliance costs for California companies alone.⁵ The RIA estimates fail to account for lost revenue for companies, compliance with CPRA (if adopted), and integration of other state frameworks with CCPA. These costs will impose a significant burden on businesses.

Even more worrisome to the Chamber is the fact that CCPA applies to companies outside California in states that are contemplating passage of fundamentally different privacy frameworks. Small businesses in particular will bear the burden of compliance and be competitively disadvantaged. CCPA applies to any company that does business in California and that “[a]lone or in combination, annually buys, receives for the business’ commercial purposes, sells, or shares the personal information of 50,000 or more consumers, households, or devices.”⁶ A food truck operator that takes electronic payments for 137 unique customers per day or an online seller in Arizona that advertises to 137 unique devices per day could be subject to the requirements of the Act and its Regulations. 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.⁷

The Chamber asserts that consumers are entitled robust privacy rights but many small business owners, who are consumers themselves, should be afforded certainty and well-tailored regulations that enable them to operate and offer consumer protections. In addition all companies subject to CCPA should have certainty as to the scope of their requirements.

I. CONSUMERS SHOULD KNOW COMPANIES ARE READY TO PROTECT THEIR CCPA RIGHTS

Any major regulation, including those authorized by CCPA, should give the regulated community adequate time to institute compliance programs. The State’s RIA estimates that the Regulations will cover up to 570,066 California companies, the vast majority of which are small and medium-sized businesses (“SMEs”). 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.⁸ Many small businesses are just becoming aware of CCPA and will need adequate time to develop solutions to protect consumers’ CCPA rights.

⁵ 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.

⁶ CAL. CIV. CODE § 1798.140(c)(1)(B).

⁷ See *supra* note 5.

⁸ See ESET CCPA Survey Results (July 19-22, 2019) *available at* https://cdn1.esetstatic.com/ESET/US/download/ESET_CCPA_Survey_Results.pdf.

Many SMEs 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. As witnessed in Europe, 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.

For a benchmark for a reasonable time for compliance, California should look to the European Union’s General Data Protection Regulation (“GDPR”). The European Union adopted the GDPR’s final regulations in April 2016 with a two-year implementation period before it took effect in May 2018. The GDPR gave regulated entities two full years to review the final regulations and develop or purchase compliance systems to implement into their daily business operations before those regulations took effect. In stark contrast to Europe’s GDPR, CCPA’s deadline for the Attorney General’s rulemaking is July 1, 2020⁹, which is six months after the law becomes effective on January 1st. In fact, as currently written, it is possible that the Attorney General could begin State enforcement of CCPA on July 1, 2020—*the same day that final rules could be published*—leaving companies *little time* to comply with the final rules.

We encourage the Attorney General to begin enforcement on January 1, 2022 giving companies 18 months to comply, which is still fewer than GDPR’s two years. We believe this is a sensible and balanced approach, especially since the GDPR was also predicated on a similar, well-established 1995 Data Protection Directive that EU Member States and businesses had long understood and complied with for many years, whereas the CCPA is an entirely new law with substantial new obligations for companies to undertake for the very first time. This timeline would also enable companies to integrate possible changes to CCPA if ballot initiatives like CPRA are adopted by voters.

Californians deserve to have their privacy protected in ways that are both strong and responsibly implemented. We strongly urge the Attorney General to grant consumers and companies adequate time to understand the yet-to-be published regulations and appropriately comply. Extending the implementation timeline until January 1, 2022 is responsible because it 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 built well-planned compliance and accountability programs to protect their statutory privacy rights.

II. THE PROPOSED REGULATIONS SHOULD BE MODIFIED TO ENHANCE CONSUMER PROTECTIONS AND COMPLY WITH CCPA AND ITS AMENDING STATUTES

A. Notice at Collection of Personal Information

Covered business under CCPA must “at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the

⁹ CAL. CIV. CODE § 1798.185(a).

categories of personal shall be used.”¹⁰ CCPA prohibits covered entities from collecting additional categories of personal information or alter the purposes for use without providing a consumer notice.¹¹

Section 999.305(a)(3) of the proposed Regulations would require covered businesses to obtain “explicit consent” from consumers to use data for purposes not described in the initial collection notice. No language in the Act authorizes the Attorney General to include an opt-in requirement for the use of data, especially in this context. From a policy standpoint, such a requirement would incentive companies to provide less specificity in their privacy policies weakening the Act’s intent to provide consumers notice. Additionally, the Regulations do not provide clarification as to how “explicit consent” is given. The final Regulations should focus on required updates to privacy policies as opposed to new obligations outside the scope of the statute.

B. Methods for Submitting Requests to Know and Requests to Delete

1) Companies Operating Exclusively Online

In October 2019, the Governor of California signed AB 1564 amending CCPA to enable companies doing business exclusively online to have to provide at a minimum an email address to accept consumer privacy rights requests. Prior to enactment of the amending statute, these companies would have been required to provide a toll-free telephone number to consumers for this purpose as well.¹² Companies that do not operate exclusively online still must provide a toll-free telephone number. The proposed Regulations at Section 999.312 do not account for this change and the Attorney General should modify the Regulations to comport with AB 1564.

2) Two-Step Deletion Requests

CCPA gives consumers the right to have any personal information, subject to exceptions, deleted.¹³ The Proposed Regulations at Section 999.312(d) would require companies to “use a two-step process for online requests to delete where the consumer must first, clearly submit the request to delete and then second, separately confirm that they want their personal information deleted.” The Chamber asserts that companies should have the flexibility to determine how deletion requests are processed. For example, consumers may prefer a “self-serve” process in which they are empowered to determine which types of data to delete.

3) Primary Interaction Method for Deletion and Right to Know Requests

In addition to providing at least two methods for receiving requests to delete and know information, the Regulations at Section 999.312(c) require that “[a]t least one method offered shall reflect the manner in which the business primarily interacts with the consumer, even if it requires a

¹⁰ CAL. CIV. CODE § 1798.100(b)

¹¹ *Id.*

¹² CAL. CIV CODE § 1798.130(a).

¹³ *Id.* at § 1798.105.

business to offer three methods for submitting requests to know.” The text of the CCPA does not contemplate this requirement; thus, the Attorney General lacks the authority to create an additional required submission procedure. The Regulations also fail to address how a business can determine its primary interaction channel with consumers.

C. The Presumption of a Request to Opt-Out of Sale

Section 999.313(d)(1) proposes that with regard to deletion requests, “if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified and shall instead treat the request as a request to opt-out of sale.” CCPA only requires that businesses delete data and request service providers do so upon verifiable request.¹⁴ The proposed Regulations exceed statutory authority because CCPA does not explicitly direct companies to treat unverified deletion requests as requests to opt out of sales.

From a practical perspective, the proposed Regulation may practically require companies that do not sell personal information—and for that reason do not offer a “Do Not Sell” button—to unnecessarily develop processes regarding opt-out requests. Secondly, the proposed Regulations threaten the trust relationship between companies and their consumers because the rules could force companies to stop sharing information at the request of individuals making fraudulent and unverifiable deletion requests in the name of another consumer.

D. Request to Opt-Out of Personal Information Sales

1) Browser-Initiated Opt-Out

CCPA requires that covered businesses honor requests by consumers directing them not to sell personal information.¹⁵ The Act further states that companies bound to this requirement must “[p]rovide a clear and conspicuous link on the business’s Internet homepage, title ‘Do Not Sell My Personal Information,’ to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer’s personal information.”¹⁶

The proposed Regulations create requirements that go beyond what CCPA mandates. Section 999.315(c) of the Regulations would obligate covered entities collecting information online to “treat user-enabled privacy controls, such as a browser plugin or privacy 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.” Although CCPA enables “authorized agents” to make opt-out requests on behalf of consumers, Section 999.135(g) would consider browser plugin or settings “requests” to be a request received directly from a consumer.

¹⁴ *Id.* at § 1798.105(c).

¹⁵ CAL. CIV CODE § 1798.120.

¹⁶ CAL. CIV CODE § 1798.135(a)(1).

A requirement that browser settings or plugins be construed as an opt-out request for purposes of CCPA fails to consider that these types of technology were designed in other contexts, and are not aligned with the Act’s complex and extremely broad definitions of “sale”¹⁷ and “personal information.”¹⁸ The CCPA emphasizes consumer choice and specifically defines the “Do Not Sell” button as a mechanism for opt-out. It is neither consistent with the statute to create this additional mechanism nor clear that consumers who use plugins intend to opt out of CCPA-defined sales.

Currently, browser-based opt-out technology is not sufficiently interoperable and developed to ensure that all parties that receive such a signal can operationalize it. Instead, the Chamber supports industry-based efforts to develop consistent technical signals for “Do Not Sell” technology, an effort that has been underway for over a year. Accordingly, the Regulations should clarify that any mechanisms not designed specifically for CCPA need not be honored as intending to effectuate a choice under CCPA.

2) Notifying Third Parties of Opt Out Requests

Consumers under the CCPA have the right to direct businesses not to sell personal information to third parties.¹⁹ Once a covered business has received the opt-out request, the statute mandates they refrain from selling personal information about the consumer to third parties and wait 12 months to contact the consumer about opting back into sales.²⁰

Section 999.315 of the Regulations though exceeds its statutory authority by imposing an additional requirement of notifying third parties of an opt-out request. Under the proposed Regulation,

A business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business’s receipt of the consumer’s request that the consumer has exercised their right to opt-out and instruct them not to further sell the information. The business shall notify the consumer when this has been completed.

CCPA Sections 1798.120 and 1798.135, granting the consumer opt-out right, do not state an obligation upon covered businesses to notify third parties of an opt-out request. Such a request

¹⁷ CAL. CIV CODE § 1798.140(t)(1). “Sell,” “selling,” “sale,” or “sold,” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.

¹⁸ See AB-874 (signed into law amending CCPA October 11, 2019) “Personal information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it 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.

¹⁹ CAL. CIV CODE § 1798.120(a).

²⁰ *Id.* at § 1798.135(a)(4)-(5).

unnecessarily burdens the operations of covered businesses, as they would not have control over how third parties have treated personal information.

E. *Training and Recordkeeping*

Section 999.317 of the proposed Regulations requires businesses to maintain records of consumer requests and responses for at least 24 months. In particular, the Regulations mandate unnecessary and arbitrary recordkeeping and notice requirements for companies dealing with the personal information of 4,000,000 or more consumers. Under the proposal,

A business that alone or in combination, annually buys, receives for the business's commercial purposes, sells or shares for commercial purposes, the personal information of 4,000,000 or more consumers, shall:

- (1) Compile the following metrics for the previous calendar year:
 - a. The number of requests to know that the business received, complied with or in part, and denied;
 - b. The number of requests to delete that the business received, complied with in whole or in part, and denied;
 - c. The number of requests to opt-out that the business received, complied with in whole or in part, and denied; and
 - d. The median number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.
- (2) Disclose the information compiled in subsection (g)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy.”

CCPA requires that company privacy policies need only include a description of a consumer's privacy rights and categories of data collected and shared.²¹ The statute does not require any metrics about consumer privacy rights requests and denials in its required privacy policy language.

The Attorney General delineates the recordkeeping requirements at businesses dealing with the personal information of 4,000,000 or consumers. The Attorney General's Initial Statement of Reasons (“ISOR”) indicates that the Office of Attorney General held discussions with SMEs about compliance. According to the ISOR, “[b]ased on these discussions and internal analysis, the Attorney General took a hybrid approach, limiting the more rigorous training and record-keeping requirements to businesses that handle the personal information of approximately 10% of California's population.”²² The reasoning to differentiate recordkeeping requirements based upon the 10 percent threshold arbitrarily fails to explain why the Attorney General settled on this number.

²¹ CAL. CIV CODE § 1798.130(a)(5).

²² See Initial Statement of Reasons, Proposed Adoption of California Consumer Privacy Act Regulations, at 44 (October 11, 2019) available at <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf>.

As noted above, the Regulations under Section 999.315 could also force covered entities to treat undefined user-enabled controls like a “browser plug-in” as a request to opt out of data sales. The contemplated signal requirements create operationalization challenges, as it is not clear that a covered business would or could actually count the number of “requesters” that have made opt-out requests, as those requests would not be moved through an active, business-tracked process.

Give the technological challenges associated with implementation of Section 999.315, the arbitrary decision to delineate recordkeeping requirements at 4,000,000 consumers, and the lack of statutory authority to implement such a requirement, the Chamber respectfully requests that the Attorney General eliminate the proposed Section 999.317 from the final Regulations.

F. Loyalty Programs and Financial Incentive Notice

1) Loyalty Programs

CCPA prevents covered businesses from engaging in “discriminatory” practices such as denying goods or services, charging different prices, or giving a different level of quality, against consumers that exercise their privacy rights under the Act.²³ An overly broad interpretation of the Anti-Discrimination rights in CCPA threatens the ability of retailers, banks, 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.²⁴ 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.

2) Financial Incentive Notice

Although prohibiting discrimination against consumer who exercise privacy rights, the Act 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.”²⁵ The covered entity must also provide notice to consumers and receive prior opt-in consent to enroll consumers in the incentive program.²⁶

The Regulations at Section 999.307(b)(5) propose that as part of the financial incentive disclosure, covered businesses must provide:

An explanation of why the financial incentive or price or service difference is permitted under the CCPA, including:

²³ CAL. CIV CODE § 1798.125(a).

²⁴ 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>.

²⁵ *Id.* at §1798.125(b)(1) as modified by the legislature.

²⁶ *Id.* at § 1798.125(b)(2)-(3).

- a. A good-faith estimate of the value of the consumer’s data that forms the basis for offering the financial incentive or price or service difference; and
- b. A description of the method the business used to calculate the value of the consumer’s data.

Currently, it remains a challenge for any business to assign value to a single consumer’s data, and data often gains value when aggregated. The valuation of data is difficult for raw and individual data as opposed to insights from data that are dependent on context.²⁷ Every business and service is different, and requiring a business to disclose its methods and calculations could likely require disclosure of competitively sensitive information. Any Regulation regarding the financial incentive notice should specifically relieve companies from having to reveal trade secrets or proprietary information. CCPA already sufficient protects consumers with regard to discounts and such a requirement is unnecessary and could have a chilling effect on discounts.

G. Special Rules for Minors Under 13 Years of Age

CCPA requires that in order for a covered business to sell legally the personal information of children under 13 years of age, a consumer’s parent or guardian must provide affirmative authorization.²⁸ Section 999.330 of the Regulations would require covered businesses with actual knowledge of collecting or maintaining personal information of children under 13 to “establish document, and comply with a reasonable method for determining that the person authorizing the sale of the personal information about the child is the parent or guardian.” The Chamber strongly recommends that if a covered business follows comparable provisions of the Children’s Online Privacy Protect Act to CCPA, the Attorney General should deem such business to have complied with those provisions of the Act.

III. THE CALIFORNIA ATTORNEY GENERAL SHOULD REMEDY THE MISSED OPPORTUNITY TO PROVIDE REGULATORY CERTAINTY THROUGH SAFE HARBORS IN ITS DRAFT REGULATIONS.

With this rulemaking, the Attorney General has the opportunity to clarify and strengthen the CCPA’s statutory safe harbors that were designed to protect well-meaning businesses that take reasonable precautions to protect consumer data.²⁹ The CCPA provides that businesses are subject to a private right of action where they do not “implement and maintain reasonable security procedures and practices appropriate to the nature of the information,” which results in the “unauthorized access and exfiltration, theft, or disclosure” of a consumer’s “nonencrypted and

²⁷ See Testimony of Will Rinehart, Hearing on Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation at 2 (October 24, 2019) available at <https://www.banking.senate.gov/imo/media/doc/Rinehart%20Testimony10-24-19.pdf>.

²⁸ CAL. CIV CODE § 1798.120(C)-(d).

²⁹ See *Understanding the Rights, Protections, and Obligations Established by the California Consumer Privacy Act of 2018: Where should California go from here?: Informational Hearing Before the Comm. On Privacy and Consumer Protection*, 2019 Leg. Sess. (Cal. 2019) (statement of Alastair Mactaggart, Chairman, Californians for Consumer Privacy, explaining purpose of safe harbor provisions), available at <https://www.assembly.ca.gov/media/assembly-committee-privacy-consumer-protection-20190220/video>.

nonredacted personal information[.]”³⁰ The law allows businesses to quell private suits by “cur[ing]” an alleged violation.³¹ It was a mistake for the Attorney General not to address these statutory safe harbors in the draft rules, and that mistake should be remedied. The final rules should contain concrete guidance for organizations attempting to comply with the law. Doing so will provide needed regulatory certainty and protect businesses operating in good faith from abusive litigation.

Regulatory guidance is needed here given that the CCPA’s private right of action provision—absent clarification and strengthening of the safe harbor provisions—can result in substantial and unnecessary costs for businesses. The CCPA’s private right of action for certain security breaches authorizes consumers to sue for liquidated damages between \$100 and \$750 “per incident.”³² Moreover, the statute does not clearly require a showing of harm. This approach—which allows for uncapped statutory damages that are untethered from any real-world harm—is dangerous. As the U.S. Chamber of Commerce Institute for Legal Reform outlined in a July white paper, private rights of action in the privacy context can have disastrous consequences for businesses with little real benefit to consumers.³³ And those potential consequences are even more acute now, in light of the recently approved AB-1130, which broadens the categories of information for which businesses may be liable under the CCPA’s private right of action.³⁴

One way to partially alleviate the unintended consequences of private rights of action is to establish safe harbors—statutory or regulatory provisions that preclude liability if certain enumerated conditions have been met. Safe harbors benefit both businesses and consumers. *Businesses* are able to discern what their compliance obligations are and thus meet consumer protection mandates, without fear of undue liability or abusive litigation. *Consumers* reap the benefits of increased compliance, as businesses utilize the clear guidance to implement protections for personal information. For these reasons, among others, safe harbors are routinely used in consumer protection statutes in California and beyond.³⁵

³⁰ Cal. Civ. Code § 1798.150(a)(1); *see also* AB-1355, *available at* https://leginfo.ca.gov/faces/billCompareClient.xhtml?bill_id=201920200AB1355 (amending, *inter alia*, § 1798.150).

³¹ *See id.*, § 1798.150(b).

³² *Id.* § 1798.150(a)(1)(A).

³³ *See Ill-Suited: Private Rights of Action and Privacy Claims*, at 14, Chamber Institute for Legal Reform (July 2019), https://www.instituteforlegalreform.com/uploads/sites/1/Ill-Suited_-_Private_Rights_of_Action_and_Privacy_Claims_Report.pdf (“[P]rivate rights of action are routinely abused by plaintiffs’ attorneys, leading to grossly expensive litigation and staggeringly high settlements that disproportionately benefit plaintiffs’ lawyers rather than individuals whose privacy interests may have been infringed.”).

³⁴ *See* AB-1130, *available at* https://leginfo.ca.gov/faces/billCompareClient.xhtml?bill_id=201920200AB1130 (broadening definition of “personal information” in Cal. Civ. Code § 1798.81.5(d)(1)(A) to include additional identification numbers or biometric data, in combination with an individual’s first name or initial and last name); *see also* Cal. Civ. Code § 1798.150(a)(1) (incorporating definition of “personal information” from Cal. Civ. Code § 1798.81.5(d)(1)(A)).

³⁵ *See* Comments of the United States Chamber of Commerce re the California Consumer Privacy Act Rulemaking, at 9 n.41–46 (Mar. 8, 2019), *available at* https://www.uschamber.com/sites/default/files/ca_ag_privacy_comments.pdf (“*Chamber CCPA Comments*”).

Given the plain text of the statute, which clearly establishes safe harbors,³⁶ the clear intent of its drafters,³⁷ and the numerous comments that the Attorney General received—including from the Chamber—urging for the regulations to include safe harbors,³⁸ the Attorney General should have clarified and strengthened the CCPA’s safe harbors in the draft regulations.³⁹ The Attorney General did not address this in the first drafts,⁴⁰ but can and should remedy this missed opportunity by adopting discrete safe harbor rules, including rules that:

- Clarify that a business that has implemented “reasonable security procedures and practices appropriate to the nature of the information” where it adopts information or data security practices recommended by an appropriate body, such as a standard-setting organization, a regulator, or a trade association, or when businesses can otherwise show that they have made good faith efforts to adopt compliance programs appropriate for the risks associated with the data they maintain;⁴¹ and
- Clarify that a business that implements “reasonable security procedures and practices”—as defined above—following a data breach will be found to have “cured” the breach within the meaning of the CCPA.⁴²

³⁶ Cal. Civ. Code § 1798.150(a)(1) (“Any consumer whose **nonencrypted and nonredacted** personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain **reasonable security procedures and practices appropriate to the nature of the information to protect the personal information** may institute a civil action” (emphasis added)); *id.* § 1798.150(b) (“In the event a cure is possible, **if within the 30 days the business actually cures the noticed violation** and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, **no action for individual statutory damages or class-wide statutory damages may be initiated against the business.**” (emphasis added)).

³⁷ See *supra* note 28.

³⁸ See, e.g. *Chamber CCPA Comments* at 9–11; Comments of the California Chamber of Commerce at 34 (CCPA 00000112) (urging adoption of a “reasonable security” safe harbor consistent with the California Data Breach Report); Comments of the Toy Association at 7 (CCPA 00000191) (“We urge the Attorney General to consider a process to recognize [safe harbor] programs. At a minimum, the Attorney General should provide examples of ‘reasonable security’ of the covered sensitive data that would insulate companies from unnecessary litigation, recognizing that security continues to evolve and that a measure of flexibility is essential.”); Comments of Experian at 7 (CCPA00000259) (“[W]e ask the Attorney General to recognize that a business’s documented adherence to accepted cybersecurity remediation standards (such as those proposed by the National Institute of Standards and Technology, the SANS Institute, the International Organization for Standardization, or the Center for Internet Security) constitutes satisfaction of the duty to implement and maintain reasonable security procedures and practices under the CCPA.”); Comments of Okta, Inc. at 5 (CCPA 00000309) (requesting “safe harbor for reasonable security”); Comments of International Pharmaceutical & Medical Device Privacy Consortium at 2 (CCPA 00000417) (“A safe harbor to the private right of action should be included for businesses that have implemented a data security program consistent with recognized industry standards.”); Comments of the Los Angeles Area Chamber of Commerce at 1 (CCPA 00000553) (proposing safe harbor for implementing “recognized information security standard” (internal quotation omitted)); Comments of HITRUST at 1 (CCPA 00000604) (“HITRUST supports suggestions made at public meetings you have held on the CCPA in support of a safe harbor option for entities that complete recognized certification programs.”); Comments of Genetech at 8 (CCPA 00001364) (“The CCPA’s consumer private right of action enforcement mechanism should include a safe harbor for businesses that have implemented a data security program that is reasonable and consistent with recognized industry standards.”).

³⁹ See Cal. Civ. Code § 1798.185(a) (allowing for the Attorney General to engage in gap-filling and thus define safe harbors).

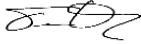
⁴⁰ See generally Proposed Text of California Consumer Privacy Act Regulations, available at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf>.

⁴¹ See *Chamber CCPA Comments* at 10.

⁴² See *id.* at 10–11.

Clarifying and strengthening the statute's safe harbors in these ways will allow businesses to better operationalize and incorporate the CCPA's mandates. As a result, the safe harbors will provide certainty for businesses and better protect consumers.

Respectfully Submitted,



Tim Day
Senior Vice President
Chamber Technology Engagement Center



Harold Kim
Executive Vice President
U.S. Chamber Institute for Legal Reform