November 18, 2022

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd.
Sacramento, CA 95834
Via email to regulations@ccpa.ca.gov

RE: Modified Text of the California Consumer Privacy Act Proposed Regulations

Dear Mr. Soublet and the California Privacy Protection Agency:

On behalf of the Software & Information Industry Association (SIIA), we write in response to the California Privacy Protection Agency's draft modified rules to implement the California Privacy Rights Act (CPRA) and update existing regulations under the California Consumer Privacy Act (CCPA).

SIIA is the principal trade association for the software and digital information industries worldwide. Our members include over 450 companies and associations reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide and companies specializing in data analytics and information services.

SIIA supports privacy as a fundamental value, one essential to individual autonomy and a functioning democracy. We believe that data privacy standards that harmonize meaningful consumer safeguards with appropriate business compliance will ensure smooth implementation of uniform data privacy practices. We have previously provided stakeholder input on CCPA and CPRA, as the law sets an important milestone for companies engaging in interstate commerce both within and outside of California.

We commend the CPPA on taking SIIA's (and other stakeholders') constructive feedback into consideration. For example, we were pleased to see the CPPA's decision to: streamline notice at collection for first and third parties, as well as streamlined practices for the information shared with consumers in the privacy policy (§ 7012); expand the types of entities that can claim "disproportionate effort" to fulfill consumer requests (§ 7023 and § 7001); allow businesses the option to display whether the company processed an opt out preference signal (§ 7025); and the decision to add clarity with regard to the business purposes for which service providers can use data (including when the business purpose is not specified in the written

contract required by the CCPA). The substantive changes in the modified regulations will greatly reduce consent fatigue and support harmonized business processes.

We provide recommendations intended to better align the CPRA regulations with the letter and spirit of the statute. Our suggested edits to the proposed regulations are reflected in **purple, bolded** text. We do so to avoid confusion across earlier drafts of the proposed regulations.

The following are outstanding recommendations that require additional consideration:

- Issue 1: Clarify the considerations for businesses to meet the expectations of the "average consumer", to streamline business compliance. (§ 7002)
- Issue 2: Remove the example that implies businesses are prohibited from leveraging advertising based on email addresses, which diverges from statute. (§ 7050)

Issue 1: Clarify considerations for businesses to meet the expectations of the "average consumer", to streamline business compliance. (§ 7002)

We appreciate that the CPPA incorporates our recommendation to modify language in § 7002 in an effort to clarify the reasonable expectations of the average consumer that the business should consider as it determines whether to process the consumer's personal information without consent. The CPPA Statement of Reasons further clarifies the section, explaining that the "purpose for which the personal information was collected or processed must be consistent with the reasonable expectations of the consumer and enumerates factors that establish the reasonable expectations of the consumer."[1]

We recommend clarifying the section to ensure practical, streamlined business compliance, as follows.

Therefore, SIIA recommends the following edits:

§ 7002. Restrictions on the Collection and Use of Personal Information.

(b) The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed. The consumer's reasonable expectations concerning the purpose for which their personal information will be collected or processed shall be based on the following:

(1) The relationship between the consumer(s) and the business. For example, if the consumer is intentionally interacting with the business on its website to purchase a good or service, the consumer likely expects that the purpose for collecting or processing the personal information is to provide that good or service **or another related product or service within the same industry**. By

[1]CPPA. Page 3. Explanation of Modified Text of Proposed Regulations.

contrast, for example, the consumer of a business's mobile flashlight application would not expect the business to collect the consumer's geolocation information to provide the flashlight service.

[...]

(3) The source of the personal information and the business's method for collecting or processing it. For example, if the consumer is providing their personal information directly to the business while using the business's product or service, the consumer likely expects that the business will use the personal information to provide that product or service **or another related product or service within the same industry**. ~~**However, the consumer may not expect that the business will use that same personal information for a different product or service offered by the business or the business's subsidiary.**~~

~~**(5) The degree to which the involvement of service providers, contractors, third parties, or other entities in the collecting or processing of personal information is apparent to the consumer(s). For example, the consumer likely expects an online retailer's disclosure of the consumer's name and address to a delivery service provider in order for that service provider to deliver a purchased product, because that service provider's involvement is apparent to the consumer. By contrast, the consumer may not expect the disclosure of personal information to a service provider if the consumer is not directly interacting with the service provider or the service provider's role in the processing is not apparent to the consumer.**~~

(c) ~~To be reasonably necessary and proportionate, the business's collection, use, retention, and/or sharing must be consistent with what an average consumer would expect when the personal information was collected. A business's collection, use, retention, and/or sharing of a consumer's personal information may also be for other disclosed purpose(s) if they are compatible with what is reasonably expected by the average consumer.~~ Whether another disclosed purpose is compatible with the context in which the personal information was collected shall be based on the following:

(1) At the time of collection of the personal information, the reasonable expectations of the consumer(s) whose personal information is collected or processed concerning the purpose for which their personal information will be collected or processed, based on the factors set forth in subsection (b).

(2) The other disclosed purpose for which the business seeks to further collect or process the consumer's personal information, including whether it is a Business Purpose listed in Civil Code section 1798.140, subdivisions (e)(1) through (e)(8).

(3) The strength of the link between subsection (c)(1) and subsection (c)(2). For example, a strong link exists between the consumer's expectations that the personal information will be used to provide them with a requested service at the time of collection, and the use of the information to repair errors that impair the intended functionality of that requested service **or another related product or service within the same industry**. This would weigh in favor of compatibility. By contrast, for example, a weak link exists between the consumer's reasonable expectations that the personal information will be collected to provide a requested cloud storage service at the time of collection, and the use of the information to research and develop an unrelated facial recognition service.

(d) For each purpose identified in subsection (a)(1) or (a)(2), the collection, use, retention, and/or sharing of a consumer's personal information to achieve that purpose shall be reasonably necessary and proportionate. The business's collection, use, retention, and/or sharing of a consumer's personal information shall also be reasonably necessary and proportionate to achieve any purpose for which the business obtains the consumer's consent in compliance with subsection (e). Whether a business's collection, use, retention, and/or sharing of a consumer's personal information is reasonably necessary and proportionate to achieve the purpose identified in subsection (a)(1) or (a)(2), or any purpose for which the business obtains consent, shall be based on the following:

(1) The minimum personal information that is necessary to achieve the purpose identified in subsection (a)(1) or (a)(2), or any purpose for which the business obtains consent. For example, to complete an online purchase and send an email confirmation of the purchase to the consumer, an online retailer may need the consumer's order information, payment and shipping information, and email address.

(2) The possible ~~**negative**~~ impacts on consumers posed by the **unauthorized disclosure of the** business's collection or processing of the personal information. For example, a possible negative impact of collecting precise geolocation information is that it may reveal other sensitive personal information about the consumer, such as health information based on visits to healthcare providers.

(3) The existence of additional safeguards for the personal information ~~**to specifically address the possible negative impacts on consumers considered by the business**~~ **in subsection (d)(2)**. For example, a business may consider encryption or automatic deletion of personal information within a specific window of time as potential safeguards.

SIIA Comments:

Section 7002 (b)(1) would not permit the processing of personal information for multiple products or services, within the same industry, by one business. Businesses engage in data analytics, product development and testing on a variety of related products and services within a related industry/vertical on a fairly routine basis, so this section would hamstring and curtail innovation. We want to underscore the importance of information collection to support product development within the same industry.

We also recommend revising § 7002 (b)(3) by clarifying the expectation and deleting the example in the last sentence. The section focuses on how a business can determine whether processing a consumer's personal information is in line with the reasonable expectations of the consumer. The expectation and example in § 7002 (b)(3) states that a business would not be able to "use personal information for a different product or service offered by the business or the business's subsidiary." This is a critical restriction that places burdensome limitations on a fairly routine part of the business life cycle, used to support product development, market research, and basic data security practices – without a meaningful benefit to consumers. By restricting the use of consumer data for companies and their supporting entities (conglomerates and their service providers and contractors) for an overly specific purpose, restricted to only one specific product or service, businesses are subject to obtaining consent for every individual update or analytical test they run on similar products within the same vertical or industry (including preliminary/ early stage design tests), which will likely result in consent fatigue. As well-established research[2] suggests, overly restrictive practices reminiscent of the data minimization and purpose limitation principles in GDPR may hamstring the potential of an innovative digital marketplace.

Section 7002 (b)(1), (b)(3), and the example in § 7002 (c)(3) conflict with the new language that supports and streamlines business compliance under § 7050(a)(3)[3]. Section 7050(a)(3) was intentionally added to the regulations to ensure that businesses *can* use consumer personal information for internal use "to build or improve the quality of services." As noted previously, and in line with § 7050(a)(3), businesses, service providers and contractors should be able to use consumer personal information for the purposes of product development, security compliance and investigations, and a range of other purposes that would be beneficial for multiple products in the product life cycle that support research and development. Thus, revising § 7002 (b)(1), deleting the section in § 7002 (b)(3), and revising the example in § 7002 (c)(3) would align with the intent of § 7050(a)(3).

In addition, we recommend striking § 7002 (b)(5). Section § 7002 (b)(5) places the expectation on businesses to base the reasonable consumer standard on the consumer's

---

[2] Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data," Seton Hall Law Review 47 no. 995 (2017).

[3] In the Statement of Reasons, CPPA notes: "7050(a)(3): Revised this subsection to clarify that the service provider or contractor may use personal information collected pursuant to the contract with the business to build or improve the quality of the services that the service provider or contractor is providing, even if this business purpose is not specified in the written contract required by the CCPA and these regulations, provided that they are not using the personal information to perform services on behalf of another person."

understanding of the vast number of service providers or other downstream providers that the business works with. It seems impractical to expect the business to align the expectations to a standard that rationalizes the consumers' understanding of the potentially vast and excessive range of entities working with the business, including all service providers and third parties. From a compliance perspective, it would be better to remove this language and instead, rely on the expectations of the business to share the information about all downstream providers that is already included in the privacy policy (in line with § 7011).

Next, we are concerned with unwieldy and concerning requirements in § 7002 (d)(2) and § 7002 (d)(3). Section § 7002 (d) notes that "whether a business's collection, use, retention, and/or sharing of a consumer's personal information is reasonably necessary and proportionate to achieve the purpose identified in subsection (a)(1) or (a)(2)" and other valid methods to obtain consent is to be based on specific data minimization principles that the business must apply before processing the data. As written, the expectation is overbroad, and would require businesses to gauge *all* the possible negative impacts of processing personal information, for potentially *all* consumers. This burdensome requirement places an expectation on businesses to gauge all possible harms to a consumer, whether they include a lack of technical safeguards, or much broader consumer harms that are not based on injury-in-fact. The lack of clarity regarding the "possible negative impacts on consumers" was also noted by CPPA Board Member de la Torre at the recent board meetings[4] in October. We believe that modifications will bring the language in line with reasonable business compliance.

To clarify § 7002 (d)(2) and § 7002 (d)(3), we recommend the business be expected to gauge the *unauthorized disclosure* of the business's collection or processing of the personal information and its impact on the consumer. This would place an inherent expectation on the business to implement and maintain technical safeguards for consumers' personal information, which is part of § 7002 (d)(3).

Issue 2: Remove the example that implies businesses are prohibited from leveraging advertising based on email addresses, which diverges from statute. (§ 7050)

Section § 7050, which focuses on service provider restrictions, includes an example that restricts service providers from fulfilling their obligations to their respective businesses and, in doing so, diverges from statute. The example conflates the role of service providers and third parties. The example suggests that the service provider should not fulfill its duty to the business to use email addresses granted by the business to serve the business's customers with ads – even if the email addresses are directly obtained by the business and strictly used on the business's own customers.

Therefore, we suggest the following edits:

[4] CPPA. Discussion from October 28 and 29th Board Meeting.

§ 7050. ~~§ 7051.~~ Service Providers and Contractors.

(b) ~~(c)~~ A service provider or contractor cannot contract with a business to provide cross- contextual behavioral advertising. Per Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but the service provider or contractor ~~those services~~ shall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or collects from its own interaction with consumers. A person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor with respect to cross-contextual behavioral advertising services. Illustrative examples follow.

(1) Business S, a clothing company, hires a social media company as a service provider for the purpose of providing Business S's advertisements on the social media company's platform. The social media company can serve Business S by providing non-personalized advertising services on its platform based on aggregated or demographic information (*e.g.*, advertisements to women, 18-30 years old, that live in Los Angeles). **~~However, it cannot use a list of customer email addresses provided by Business S to identify users on the social media company's platform to serve advertisements to them.~~ The social media company can also use a customer list provided by Business S to serve Business S's advertisements to Business S's customers. However, it cannot use a list of customer email addresses provided by Business S to then target those customers with advertisements based on information obtained from other third party businesses's websites, applications, or services.**

SIIA Comments:

We suggest clarifying the example with the suggested sentence (noted above) that authorizes the service provider to fulfill its fiduciary duty in using the list of customer email addresses provided by its business (Business S) to serve Business S's customers with ads. We also recommend adding a sentence to further clarify the prohibition on cross-contextual advertising, which would prevent the service provider from using the same email addresses to target Business S's customers with ads that are grounded in third party sources of information (i.e., information obtained from other third party business websites, applications, or services). This clarification would align the example to how it reads in the statute[5].

[5] California Privacy Rights Act. § 1798.140 (k) "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

Conclusion

As noted, after reviewing the most recent draft of the modified regulations, we have identified additional areas where the regulations significantly diverge from the statute. We believe that the draft regulations should be further clarified and aligned to the statute, so that companies are not left with additional outstanding questions, onerous requirements that result in negligible privacy protective benefits to consumers, and high costs to comply, on the heels of the CPRA compliance date: January 1, 2023.

Furthermore, we make two recommendations that require procedural changes. First, we recommend that additional guidance be provided to a) exempt employee and business to business (B2B) data from compliance with CCPA and CPRA, as well as the modified regulations; and b) ensure businesses are provided further support on the appropriate treatment of employee and B2B data with regard to CPRA, including how to mitigate the uncertainty and conflicting requirements imposed on treating employee data and B2B data in the same breath as consumer data.

The CPRA draft rules were required to be finalized by July 1, 2022 and become enforceable on July 1, 2023. To ensure consistency with the intent of the statute, which provides for one year between the date when the rules are finalized and the enforcement date, we recommend the enforcement date be shifted to one year from the date of when the rules are finalized. Providing sufficient time for compliance with the regulations will help to mitigate confusion across the business and consumer community.

* * *

Thank you for considering our suggested revisions to the proposed regulations to the CPRA. We are happy to discuss in further detail, as appropriate. For further information, please contact Divya Sridhar, at dsridhar@siia.net.

Respectfully submitted,

Divya Sridhar, Ph.D.,
Senior Director, Data Policy
Software and Information Industry Association (SIIA)