SIIA Accelerating Innovation in Technology, Data & Media

1090 Vermont Ave NW Sixth Floor
Washington DC 20005-4905
www.siia.net

February 25, 2020

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, California 90013
Via Email: PrivacyRegulations@doj.ca.gov

Re: SIIA Comments on the Modifications to the Proposed Text of the CCPA Regulations

The Software & Information Industry Association (SIIA) appreciates the opportunity to submit additional comments on the modifications to proposed regulations implementing the California Consumer Privacy Act (CCPA). These comments, like our prior submission, highlight the constitutional defects raised by the CCPA and, by extension, any implementing regulation.[1] We also identify discrete compliance issues raised by the proposed text in several provisions.

SIIA is the principal trade association for the software and digital content industry. We provide global services in government relations, business development, corporate education, and intellectual property protection to the leading companies that are setting the pace for the digital age. With over 800 members spread over eight specialized divisions, SIIA provides a voice for its membership on the importance of information to promote a competitive, fair, and innovative digital economy. Our members include software publishers, financial trading and investment services, specialized and B2B publishers, and education technology service providers.

We submit these comments to reiterate our concern that the CCPA, and the implementing regulation, will be vulnerable to a First Amendment challenge unless the Attorney General uses the authority granted by Cal Civ. Code 1798.185(a)(3) to cure the unconstitutional regulation of information in the public domain. In addition, our comments identify several proposed provisions that could benefit from edits to avoid unintentional compliance outcomes. The identified provisions are not an exhaustive list, but represent key concerns based on SIIA's members.

---

[1] SIIA Comments on the Proposed Text of the CCPA Regulations (Dec. 6, 2019), available at https://www.siia.net/Portals/0/pdf/Policy/Privacy%20and%20Data%20Security/SIIA%20Comments%20re%20CCPA%20regs%206%20DEC%20FNL%20%20FILED.pdf?ver=2019-12-06-172925-923.

I. The Attorney General Should Cure the CCPA's First Amendment Defects

We appreciate the Attorney General's partial response to the constitutional concerns we previously raised. First, we were glad to see Section 999.305(d), which would have required attestations before disseminating public domain information, stricken from the draft regulations. As we noted in our comments, the draft language raised a number of significant First Amendment and policy concerns by imposing impossible compliance obstacles that would render the publication of information unlawful even when the CCPA would otherwise permit its dissemination. The Attorney General's decision to strike this provision was correct as a matter of law and policy.

Second, we thank the Attorney General for curing a similar problem with the definition of "categories of sources" to exclude the reference to public records. As our comments flagged, the capture of public records by this definition was in contravention of AB 874, which amended the CCPA to entirely exclude public records information from its regulatory scope. Moreover, it raised significant First Amendment concerns because it regulated the public domain without advancing a compelling interest or tailoring the regulation to meet that interest. Again, the decision to strike this reference is the right choice as a matter of law and policy.

Although we welcome these revisions, they are insufficient to address the statute's core First Amendment problems. The statute defines "personal information" to exclude "publicly available information."[2] The CCPA, however, limits "publicly available information" to "information that is lawfully available from federal, state, or local government records." It does not exclude a second and considerably larger category of public domain information, which is information that is widely available in private hands. This second category of public domain information includes professional contact details, credential and licensing details, biographical data, and other information drawn from registries, directories, websites, and news and social medial channels.

The broad and untailored regulation of this second category of the public domain raises significant constitutional and policy concerns. As a constitutional matter, the CCPA's regulation of the non-governmentally sourced public domain impedes protected speech without advancing a compelling government interest or

[2] The CCPA's treatment of publicly available information has been a concern of SIIA's through this entire legislative process, and we have documented the statute's constitutional defects in several filings. For additional resources, please refer to our December 6, 2019 written comments (*see* fn. 1, *supra*), which cites to a memorandum from our outside counsel, our December 26, 2019 letter to the Attorney General, and the Senate and Assembly's Bill Analyses for AB 874 (which was enacted in response to the concerns outlined in our outside counsel memo).

engaging in the tailoring to meet that interest as required by the First Amendment. *See IMS Health v. Sorrell*, 564 U.S. 552 (2011); *Bartnicki v. Vopper*, 532 U.S. 514 (2001). Moreover, the CCPA discriminates among speakers and on the basis of speech content, which separately violates the First Amendment.

As a policy matter, the regulation of the non-government public domain will result in poor policy outcomes, including the suppression of information for use in law enforcement investigations, investigative journalism, identity verification, scientific and medical research, corporate due diligence, and finding missing persons. SIIA's members provide the tools necessary to achieve these socially valuable uses. The value of these tools depends on their completeness and accuracy, and consists in large part of information that is publicly available from both governmental and non-governmental sources. If the CCPA and its implementing regulation do not exclude the non-governmental public domain from their scope, these socially valuable uses will be impeded through efforts to obfuscate the ability to collect, disseminate, and publish information in the public domain.

To cure these constitutional and policy flaws, SIIA again urges the Attorney General to use his authority in Section 1798.185(a)(3) to promulgate a regulation that makes the CCPA constitutional. This can be done by expressly excluding public domain information that is widely available from non-governmental sources from the regulation's scope.

II. The Regulations Should be Amended to Define "Data Broker" and Clarify When Non-Data Broker Third Parties Must Provide Notices. *See* Sections 999.301(d)-(e); 999.304; 999.305(a)(7) and (d).

The modifications add references to "data brokers" in the definitions for "categories of sources" and "categories of third parties." *See* Section 999.301(d) and (e). The proposed modifications, however, do not incorporate a corresponding definition for "data broker" to explain the use of the term in .301(d) and (e). This is in contrast to Section 999.305, which also refers to "data broker," but expressly ties the use of the term in that provision to the data broker registry law (*see* Cal Civ. Code 1798.99.80 *et seq.*), which in turn defines a "data broker." To cure any resulting regulatory ambiguity, we respectfully urge the Attorney General to promulgate a regulation that adopts the definition of "data broker" from Cal Civ. Code 1798.99.80(d).[3]

Relatedly, we note that the modification to Section 999.305(d) to address "data brokers" leaves continued ambiguity regarding the obligations of non-data brokers that collect information indirectly from consumers with respect to the

[3] We note that the "data broker" definition in Section 1798.99.80 is ambiguous on its own with respect to which businesses qualify as data brokers.

notices required at the time of collection. As we noted above, Section 999.305(d) applies only to businesses that register as data brokers in compliance with Cal Civ. Code 1798.99.80. That law defines a "data broker" to exclude several categories of businesses to the extent they are covered by another sectoral federal privacy law (i.e. consumer reporting agencies, financial institutions, and insurance companies). Thus, an entity like a consumer reporting agency, will not be subject to the proposed modifications in Section 999.305(d).

To cure this, the Attorney General should amend the modifications at Sections 999.304 and 999.305(a)(7) and (d) to clearly state that businesses that are not data brokers and that do not collect information directly from consumers are not required to provide a notice at the time of collection to the consumer. Doing so will permit businesses that are excluded from the "data broker" definition to continue to engage in data collection while bound by existing federal sectoral privacy laws.

III. Affirmative Authorization Should Not Be Defined to Require a Two-Step Verification Process. *See* Sections 999.301(a); 999.316(a).

In our prior comments, we objected to the CCPA's proposal to require a two-step process for consumers 13 years and older to opt-in to the sale of their personal information. As we noted then, and reiterate now, the de facto double opt-in fails to meaningfully advance consumer choice. Indeed, it risks unduly interfering with consumer choice by calling into question the informed decision the consumer already made with respect to their request to opt-in. Consumers should be free to exercise their choices without barriers designed to signal that such choice is wrong or risky. Moreover, consumers should be able to exercise a meaningful and intentional opt-in without a barrage of repeat notifications that realistically only interrupt the consumer's online experience and risk notification fatigue.

The baseline definition for "affirmative authorization" accomplishes what is the appropriate and necessary consent for consumers 13 years and older who request to opt-in to the sale of their information. By the terms of the proposed definition, that authorization "means an action that demonstrates the ***intentional decision*** by the consumer to opt-in to the sale of personal information." The strength of this provision lies in its requirement of a demonstrated intentional decision to opt-in, which can and should be accomplished in one notice. **To accomplish this, we urge the Attorney General to modify the definition at Section 999.301(a) to strike the two-step requirement. Then, to fully capture the spirit of this change, the Attorney General should also modify Section 999.316(a) to remove the requirement for a second step in the opt-in process.**[4]

[4] We also note that if the Attorney General does not take our suggested modification for Section 999.301(a), then a modification of Section 999.316(a) is absolutely necessary. As

IV. Data Does Not Have an Independent Value and the Regulations Should Not Require a Misleading Disclosure of a Value that Cannot be Quantified. *See* Sections 999.307(b)(5); 999.337).

We recommend that the Attorney General revise the proposed modifications to remove any requirement for businesses that offer financial incentives to provide estimates of the value of the consumer's data. **To accomplish this, we suggest the Attorney General strike subsections (a) and (b) of 999.307(b)(5) and strike Section 999.337 entirely. The revised Section 999.307(b)(5) would read: "An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data."**

The purpose of our recommendation is to avoid value disclosures that are impossible to calculate. As a general matter, data does not have independent value. Its value, if any, is subjective, in flux, and depends on the context in which it is collected and processed. Because of data's lack of a clear and objective value, even academics are flummoxed when estimating its value, often arriving at wildly different estimates for the same services.

One of the fundamental misunderstandings in the debate over the value of data is the assumption that its usefulness to advertising corresponds to its value. It is not possible, however, to derive a value estimate from data solely by looking at ad revenue. With respect to ad-supported and free online services, the consumer value rests in the experience, which is made possible by the data that supports the ad model. Consumers do not exchange their data for the experience. Rather, the experience is made possible by the data. The data, in turn, enables the ads so that the service can provide its core service – the personalized content. The business model isn't compensated by consumer's data, but rather through the selling of ads. The data may influence the delivery of the ads, but it does not drive the value of the ad sales, which are influenced by external metrics relating to delivery, views, and clicks.

---

currently drafted, Section 999.316(a) sets out the requirements for a "request to opt-in" as requiring two steps: (1) a clear "request to opt-in" and (2) a separate confirmation of the consumer's choice to opt-in. The problem, however, is that "request to opt-in" is a defined term. As defined in Section 999.301(t) it means "the ***affirmative authorization*** that the business may sell personal information about the consumer. . ." "Affirmative authorization," as we discuss above is currently defined to mean a two-step process for obtaining consent and then confirming that consent. The explicit inclusion of a two-step process in Section 999.316(a), therefore, is superfluous because by its terms it incorporates the "affirmative authorization" requirement of a two-step process. If the Attoreny General keeps both provisions as currently proposed, then Section 999.316(a) could be interpreted to actually require a three step process for an opt-in: First, the request to opt-in and the two-step process it requires by its very terms; and secondly, the .316(a) confirmation of the request to opt-in.

V. Businesses that Operate Online Should Not Be Required to Maintain Toll-Free Numbers for Receiving Requests to Know. *See* Section 999.312(a).

We are concerned that the proposed modification to Section 999.312(a) would require businesses that do not have a direct relationship with consumers to maintain a toll-free telephone number for receiving requests to know even if the business operates online. The requirement to maintain a toll-free telephone number is expensive and burdensome, and it is not clear how mandating its upkeep and availability materially improves a consumer's ability to submit a request to know to an online business with which she does not have a direct relationship. **We respectfully request that the Attorney General modify the proposed text to permit online businesses that do not have direct relationships with consumers to provide two or more designated methods, which can include a toll-free number, an interactive webform, a designated email address, or a form submitted via the mail.**

VI. Businesses Should Not be Burdened With Obligations to Respond to Unverified Requests to Know. *See* Section 999.313(c)(1) and (3).

Both the initial proposal and the current modifications contemplate obligations for businesses with respect to *unverified* requests to know in Section 999.313(c)(1). This is inconsistent and contrary to the CCPA, which expressly contemplates the discarding of unverified requests precisely because they are unverified. *See* Section 1798.105. As a practical matter, the CCPA's direction that business can and should discard unverified requests operates for the protection of the consumer, which Section 999.313(c)(1) undermines. **To address this, we suggest the Attorney General strike the last sentence of Section 999.313(c)(1)**.

We are also concerned that the modifications to the proposed text include the deletion of Section 999.313(c)(3), which would have prohibited a business from providing a consumer with specific pieces of personal information when the disclosure created a substantial, articulable, and unreasonable security risk. The modifications replace this text with a four-part test. We are concerned, however, that this new test is too restrictive, overly burdensome, and completely fails to address the key security concerns addressed by the original language.

The security standard originally set forth in Section 999.313(c)(3) was high. A business could not merely identify a potential security risk and withhold the information when responding to a request to know. To be a valid withholding, the business had to be able to show that the disclosure would create a "substantial, articulable, and unreasonable risk to the security of [the] personal information, the consumer's account with the business, or the security of the business's systems or networks." When this standard is met, a business should not be compelled to turnover personal information in response to a request to know.

We respectfully urge the Attorney General to amend the modification to re-insert the original Section 999.313(c)(3). With respect to the four-part test, we urge the Attorney General to largely retain it, but draw a clearer line by making any of the enumerated conditions sufficient on their own to limit access rights in a manner that balances individual privacy and operational burdens. We suggest the following language:

In responding to a request to know, a business is not required to search for or provide personal information ~~if all~~ that meets any of the following conditions ~~are met~~, provided the business describes to the consumer the categories of records that may contain personal information that it did not provide because it meets one of the conditions state ~~above~~ below

(a) The business does not maintain the personal information in a searchable or reasonably accessible format;
(b) The business maintains the personal information solely for legal or compliance purposes;
(c) The business does not sell the personal information and does not use it for any commercial purpose
(d) ~~The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above~~. The business does not associate the personal information with a consumer in the ordinary course of business; or
(e) The personal information was not collected from the consumer or a third party, but was instead derived internally by the business.

VII. Conclusion

We thank the Attorney General for this opportunity to provide our comments and suggested edits, and for considering our concerns as you work toward finalizing these proposed regulations. If you have any questions or concerns regarding our comments, please contact us at your convenience.

Respectfully submitted,

Christopher A. Mohr, VP for Intellectual Property and General Counsel
Sara C. DePaul, Senior Director, Technology Policy
Software & Information Industry Association
1090 Vermont Avenue NW, 6th Floor
Washington D.C. 20005
www.siia.net