

December 6, 2019

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 Proposed Text of the CCPA Regulations

On behalf of the Software & Information Industry Association (SIIA), thank you for the opportunity to submit comments regarding the proposed text for the regulations implementing the California Consumer Privacy Act Regulations (CCPA). SIIA and our member companies support the CCPA's intention to provide consumers with more awareness, control, and choice over the dissemination of their personal information. We thank the Office of the Attorney General for its leadership and diligence in developing proposed regulations that are measured, sensible, and provide industry with needed guidance on how to implement the CCPA.

As background, SIIA is the principal trade association of the software and digital content industry. We represent over 800 companies that develop and market software and digital content for business, education, consumers, the Internet, and entertainment. Our members include software publishers, financial trading and investment services, and specialized and business-to-business publishers. A number of our member companies also provide services to children online and to schools to develop and deliver software applications, digital instructional content, online learning services, and related technologies. These members, often referred to as "edtech companies," work to support teachers and instruction, improve student learning, carry out various administrative operations, and improve school productivity.

The proposed regulations are particularly useful where they clarify the CCPA's legislative intent to provide consumers with meaningful notice, choice, and control over the collection and use of their personal information. For example, the proposed regulations provide a critical clarification regarding the obligations of service providers in section 999.314(a), by making it clear that a person or entity qualifies as a "service provider" if it "provides services to a person or organization that is not a business, and would otherwise meet the requirements of a 'service provider'" under the CCPA.

With this clarification, businesses that provide services to schools or other government agencies will be subject to the CCPA's service provider requirements. This includes edtech companies, which provide services critical to modern learning

in the classroom. For edtech companies, this proposed clarification appropriately alleviates the conflicting compliance obligations imposed by existing student privacy laws, including California's Student Online Personal Information Protection Act (SOPIPA). For more information on the compliance conflicts created by the CCPA on edtech companies without this clarification, please see our [December 26, 2018 letter to the Attorney General](#).

Nevertheless, we have a number of concerns with the proposed regulations, which we are grateful for the opportunity to bring to your attention. As a general matter, we are concerned about the constitutional issues raised by the statute and the proposed regulations. More specifically, we note that the proposed regulations run afoul of First Amendment principles in three important respects:

- First, the underlying statute has fatal constitutional defects that we urge the Attorney General to remedy in this proceeding. The CCPA unconstitutionally regulates information in the public domain including information sourced from research databases, directories, registries, news articles, books, unrestricted social media feeds, and any number of other general interest, media, or business-to-business publications available to the general public. The Attorney General has an opportunity to correct this constitutional defect using his authority granted by Cal Civ. Code 1798-185(a)(3) to promulgate regulations to "[e]stablish[] any exceptions necessary to comply with state or federal law. . . ." **To comply with federal constitutional law, we respectfully urge the Attorney General to use this statutory authority to draft an exemption for all publicly available information, whether made available by a government agency or a non-government source.**
- Second, section 999.305(d), which sets forth requirements for businesses that do not collect information directly from consumers, increases the burdens imposed by an already problematic statute in a particularly overbroad way. **To cure this constitutional infirmity, we recommend that the Attorney General strike section 999.305(d) from the proposed regulations.**
- Third, the proposed regulations do not adopt the CCPA's amended treatment of information contained in public records, which the legislature enacted pursuant to AB 874 in order to resolve significant First Amendment defects with respect to the CCPA's regulation of information in the public domain. **To account for this legislative change, which the Governor signed into law after the proposed regulations were released, the Attorney General should amend the definitions at section 999.301(d) and (e) to strike or clarify references to public records and government entities that could run afoul of the exemption for public records set forth in AB 874.**

Finally, our members have practical, operational concerns with several sections of the proposed regulations that impose unintentional compliance outcomes and difficulties without meaningfully advancing the CCPA's intention to expand

consumer choice and control. Our focus here is on sections 999.313(c)(4), .314(d), .315(c) and (f), and .316(a). As explained in more detail in Section II, below, we generally recommend line-item edits to these proposed provisions to clarify that they do not require overly burdensome compliance requirements.

I. The First Amendment and Privacy Regulation

A. The CCPA's Regulation of Public Domain Information Constitutes a First Amendment Violation that The Attorney General Can Cure by Exempting Information From Non-Government Sources

SIIA's members amass public domain information to provide research tools for a variety of socially valuable uses, such as law enforcement investigations, investigative journalism, identity verification, scientific and medical research, corporate due diligence, and finding missing witnesses, among other uses. The collection and publication of public domain information is protected by the First Amendment, which requires statutes and regulations to be carefully tailored so that they do not infringe freedom of speech guarantees. Such guarantees extend to a private company that, for example, creates databases of publicly available factual information. *See IMS Health v. Ayotte*, 564, U.S. 552, 570 (2011) (“the creation and dissemination of information are speech within the meaning of the First Amendment”), citing *Bartnicki v. Vopper*, 532 U.S. 514, 527 (2001) (“If the acts of disclosing and publishing information do not constitute speech, it is hard to imagine what does fall within that category, as distinct from the category of expressive conduct.”) (other citations omitted).

During California's 2018-19 legislative session, SIIA shared with legislators a [memorandum from its outside counsel](#) regarding First Amendment problems raised by the CCPA as originally enacted. The memo detailed the way in which the statute was vague, overbroad, and content-discriminatory by regulating information in the public domain. In response to those First Amendment concerns, Rep. Irwin introduced AB 874, which unanimously passed both houses and was signed into law on October 11, 2019 – a day after the Attorney General released the proposed regulations.¹

¹ *See* Senate Judiciary Committee, [Bill Analysis](#) at 5-6 (recognizing “very real concerns” raised by the Mayer Brown memorandum); Assembly Committee on Privacy and Consumer Protection, [Bill Analysis](#) at 5 (“The concern that this bill seeks to address is that the CCPA's limitations on the use of publicly available information are vague and could run afoul of the First Amendment, which protects the right of individuals to disseminate information.”).

AB 874 amended the provision specifying the “publicly available information” exempted from the definition of “personal information.”² Following the enactment of AB 874, the relevant portion of the CCPA exempting “publicly available information” states:

“Personal information” does not include publicly available information. For purposes of this paragraph, “publicly available” means information that is lawfully made available from federal, state, or local government records. “Publicly available” does not mean biometric information collected by a business about a consumer without the consumer’s knowledge.

Cal. Civ. Code 1748.140(o)(2).

AB 874 cures the CCPA’s First Amendment defect with respect to public domain information derived from public records. But the amended CCPA (and by extension the proposed regulations as currently drafted) still contain fatal First Amendment flaws because they regulate public domain information derived from widely available non-government sources, such as professional contact, credential and licensing details, biographical data, and other information drawn from registries, directories, websites, and news and social media channels.

However, the CCPA gives the Attorney General the authority to establish exemptions necessary to “comply with state or federal law.” *See* Cal. Civ. Code. 1798.185(a)(3). **SIIA, therefore, respectfully urges the Attorney General to use that authority to promulgate a regulation that places the scope of the CCPA’s regulations within the bounds of the First Amendment. This can be done by expressly excluding from the regulation’s scope public domain information that is widely available from non-government sources.**

Unfortunately, in some instances, the proposed regulations take the existing constitutional problems with the CCPA and make them worse. In the absence of legislative action, these constitutional problems require regulatory adjustment even if the Attorney General uses his authority to exempt widely distributed media to cure the larger First Amendment issues created by the CCPA. We turn to these problems in the following subsections.

² AB 874, Bill History, available at https://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml?bill_id=201920200AB874.

B. The Attorney General Should Strike Section 999.305(d) in its Entirety In Order to Conform with the First Amendment

As proposed, section 999.305(d) of the regulations requires that a business that does not collect “information directly from consumers” must, *before* disseminating personal information, fulfill one of two conditions. First, the business may contact consumers directly and inform them that the business has personal information about them and provide them with a notice of their right to opt-out of the sale of their personal information. *See* Section 999.305(d)(1). Alternatively, the business must contact the source of the information to confirm that the source provided the consumers with a notice as required by the CCPA *and* obtain signed attestations from the “source of the consumer information” describing how the source gave the notice required by CCPA at the time of collection and including an example of the notice.” Failure to satisfy one of these two proposed requirements makes publication of the information unlawful, whether the CCPA would have otherwise permitted its dissemination or not.

SIIA’s members have a constitutional right to publish directories, registries and other important works that contain public domain information, whether that information comes from public records or publicly available non-government sources. For example, some of SIIA’s members sell online databases that index millions of articles covering subjects ranging from science and medicine to law and finance. These kinds of databases contain the author’s names and other information about the authors sourced from works published by different publishing houses.

The proposed regulation makes the publication and sale of the above information illegal – and exposes publishers to massive potential liability – in all circumstances unless they comply with section 999.305(d) by either contacting all of these authors to give a privacy notice required by the CCPA or obtain attestations that such notice was provided from the original source of the articles. This neither advances a compelling privacy interest, nor does it comport with our First Amendment guarantees to freedom of speech. Indeed, proposed section 999.305(d) goes even further than the statute, rendering *all* publication illegal, even if the CCPA’s substantive requirements would have otherwise permitted it. Section 999.305(d) exacerbates the CCPA’s First Amendment infirmities.

Finally, the conditions imposed by proposed section 999.305(d) will in many cases be impossible to satisfy. Take, for example, the situation in which a publishing house from which a library of journals is acquired has been absorbed or gone out of business or when the author of a work that is thirty or fifty years old cannot be found. This problem repeats itself across a variety of media, including directories of films, literary agents, or newspaper articles. If section 999.305(d) is promulgated as proposed, the State will, in effect, ban the publication of information in these

circumstances despite an obvious lack of tailoring to a colorable privacy interest. Although the State may in certain circumstances punish the publication of some information after its release, the state may not curtail First Amendment speech by a blanket ban on publication. **Section 999.305(d) should be stricken in its entirety.**

C. The Attorney General Should Revise the Definitions for “Categories of Sources” and “Categories of Third Parties” to Conform with AB 874 and the First Amendment.

The Attorney General’s proposed regulations were released to the public one day before AB 874 was signed into law by the Governor. Once AB 874 became law, information derived from lawfully made available records was exempted from the CCPA’s scope and, by extension, from any resulting regulations. While on balance, this does not affect the vast majority of the proposed regulations, it does call into question two definitions that could be interpreted to capture public record information that the legislature expressly excluded from the CCPA’s scope.

First, “Categories of sources” in section 999.301(d) is defined to include “government entities from which public records are obtained” as a type of entity “from which a business collects personal information about consumers.” As a result of AB 874, however, information derived from public records is not regulated by the CCPA. It is inappropriate both under the strictures of AB 874 and the First Amendment concerns that prompted it, for the proposed regulations to capture public record information by including government entities that publish such records in this definition. **We respectfully request that the Attorney General strike the reference to “government entities from which public records are obtained” from this definition.**

Second, the proposed regulation defines “Categories of third parties” to include “government entities” as a type of entity that does “not collect personal information directly from consumers.” **To avoid any confusion that this definition results in the proposed regulations drawing in government entities with respect to public records, it should either be stricken or clarified to conform to AB 874.**

We note that both of these definitions include the qualifier “personal information,” which technically constrains the extension of those definitions to account for the amended CCPA’s exemption of public records information. Nevertheless, both definitions can be interpreted to work around this exemption to draw in government entities with respect to public records for the proposed obligations elsewhere in the proposed regulations. This result is likely not intentional, but underlies why our recommendations to strike and/or clarify these aspects of the two defined terms is important to bring the proposed regulations

within the ambit of AB 874 and the First Amendment concerns it was passed to address.

II. The Attorney General Should Revise Several Proposed Provisions to Avoid Unintentional and Overly Burdensome Compliance Outcomes

Setting the above-described constitutional concerns aside, SIIA generally supports the proposed regulations, which update, establish, and govern the CCPA's standards. We have concerns with five proposed provisions, however, because they create overly burdensome operational problems for businesses and service providers subject to the CCPA. Those proposed provisions are: Sections 999.313(c)(4), .314(d), .315(c) and (f), and .316(a). Our comments below explain the compliance issues presented by these provisions and suggest revisions or clarifications that the Attorney General can make to avoid unintentional but burdensome compliance outcomes.

A. The Attorney General Should Clarify Proposed Provision 999.313(c)(4) To Meet Consumer Expectations for Data Portability

Proposed provision 999.313(c) clarifies the parameters for how a business must respond to a request to know from a consumer, including obligations for disclosures when a business cannot verify an individual and prohibitions on disclosing sensitive data. The latter point is addressed by proposed provision 999.313(c)(4), which outright bans a business from disclosing “a consumer’s Social Security number, driver’s license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or security questions and answers.”

We agree that this provision is generally sensible given the sensitivity of the data, particularly if the business has not been able to verify the identity of the person making the request to know. We also note that it is sensible to outright prohibit the disclosure of passwords and security questions and answers. However, this prohibition is unlikely to align with some consumer’s expectations. For example, medical, tax, and other forms that contain government identifiers may be sought by consumers to port such forms from one provider to use for another purpose (including to port to another provider). **Taking into account consumer expectations and that the CCPA does not expressly prohibit such disclosure, we recommend modifying the proposed provision to allow, subject to a verified request, an entity to consider the context and intent of the consumer’s request, including portability, when determining whether to provide such data.**

A. The Attorney General Should Revised Proposed Provision 999.314(d) to either remove or clarify the word “maintains” and to clarify the meaning of “feasible”

Proposed section 999.315(d) clarifies the obligations of a service provider that receives a request from a consumer to know or delete personal information. The proposed provision requires a service provider in receipt of such requests to explain the basis for a denial, if one is made, and to inform requesting consumers that they should submit the request directly to the business that controls the data at issue. In addition, the service provider must, *when feasible*, provide the consumer with the contact information for the business. The obligations under this section are triggered when the service provider receives a qualifying consumer request regarding personal information that the provider “collects, *maintains*, or sells on behalf of the business it services.” (emphasis added)

The provision attempts to balance obligations between the service provider and the business while ensuring that consumers receive sufficient information to resubmit requests to know or delete to the appropriate entity (i.e. the business). We are concerned, however, that inclusion of the word “maintains” is vague and may capture situations in which a service provider “maintains” data on behalf of a business but does not have a right to access the data. A common example would be a cloud service provider, which likely maintains personal information on behalf of businesses that it is contractually obligated not to access. In these circumstances, it would be contractually impossible for the service provider to access the data to respond to a request to know or delete in order to assess a reason for the denial or to redirect the consumer to the appropriate business to which to submit the request.

To address these situations (and avoid forcing service providers to access data in contravention of contractual obligations), we recommend that the Attorney General revise this proposed section to clarify that service providers who “maintain” personal information on behalf of a business but do not have a right to access the data are not subject to this provision. This can be done by either striking the word “maintains” from this provision or by clarifying that the term is not intended to reach situations where personal information is maintained without a right of access by a service provider. The latter fix can be achieved by revising 999.314(d) to state:

- If a service provider receives a request to know or a request to delete from a consumer regarding personal information that the service provider collects, ***maintains with a right to access***, or sells on behalf of the business it services, and does not comply with the request, it shall explain the basis for the denial.

In addition, the proposed provision requires a service provider to give the requesting consumer the contact information for the relevant business when it is feasible to do so, but the proposal leaves it unclear when it may be infeasible to do so. For instance, would a feasibility determination rest on whether a service provider

would have to deploy significant resources to identify the business? Or would a feasibility determination come down to a technical ability to identify the business? What if the business is prohibited by a court order or a legal obligation from identifying the business? **To help businesses make these determinations, we respectfully suggest that the Attorney General revise this provision to clarify the meaning of feasibility and to ensure that businesses can rely on an infeasibility determination when identifying a business requires them to deploy significant and disproportionate resources or they are otherwise legally barred from doing so.**

B. The Attorney General Should Strike Proposed Section 999.315(c)

Proposed section 999.315(c) addresses consumer requests to opt-out of the sale of their personal information by obligating businesses that collect such information online to treat user-enabled privacy controls as a valid request to opt-out for the browser or device from which the request is sent, or from the consumer (if known). It is unclear if this provision is intended as a *de facto* amendment to the California Online Privacy Protection Act to export that law's Do Not Track requirements into the CCPA, or if it is merely intended to incentivize the development of new technological solutions to facilitate these requests. We respectfully suggest that if it is the former, it would be helpful for the Attorney General, at a minimum, to explicitly reference the Do Not Track to facilitate compliance. But even with this fix, large scale operational concerns remain that render this proposed provision harmful to consumer choice and unduly disruptive to business without a concomitant benefit to consumers.

This is because the proposed provision creates several unintended policy outcomes. First, it weakens rather than strengthens consumer choice and control by creating a legal assumption that the browser-based user-enabled privacy controls, like do not track, are equivalent to an opt-out. Second, because the proposed regulations do not require businesses to verify the identity of a consumer making an opt-out request, it will be incredibly difficult, if not impossible, for businesses to ascertain the identity of a consumer for purposes of operationalizing these requests as an opt-out request. The proposed provision's requirements for business to exercise the opt-out at the browser or device level do not help because it will result in overinclusive opt-outs. Take, for instance, a large company that uses a single IP address across the devices used by its thousands of employees. Under proposed provision section 999.315(c), business will have to opt-out all information associated with the IP address of that company if even one personal within the company utilizes a user-enabled privacy control.

These outcomes are unduly and wrongly disruptive to businesses subject to this regulation. Worse, these outcomes vitiate consumer control and choice, a key

tenant of the CCPA. **To avoid this, the Attorney General should strike this provision.**

C. The Attorney General Should Clarify Section 999.315(f)

Proposed section 999.315(f) seeks to ensure that consumer opt-outs are fulfilled downstream by requiring businesses to notify all third parties to whom they have sold the information within 90 days prior to the receipt of the consumer request to opt-out. Businesses are required to instruct third parties to not further sell the information, and to inform the consumer when this obligation has been fulfilled. We have several concerns with this provision.

First, the proposed provision imposes a significant and unfair compliance risk on businesses by requiring downstream notifications while mandating opt-outs without requiring verifiable consumer requests. Because businesses must honor an opt-out request even when they cannot verify a consumer's identity, it will be difficult in many situations to execute a meaningful downstream opt-out consistent with the obligations imposed by this proposed provision. **This risk can be alleviated by modifying the proposed provision to clarify that businesses are only obligated to follow its strictures when the consumer making the opt-out request can be identified.**

Second, the proposed provision requires businesses to notify "third parties" and instruct them to not further sell the personal information. The CCPA, however, defines third parties to mean persons with whom the business does not have a written contract. In other words, third parties in the CCPA context are not subject to the instructions of the business. It is unclear, therefore, how a business's instruction to a third party could be considered mandatory. Additionally, this ignores the "use" contexts of data that consumers will want to preserve even when opting-out with respect to one use. For example, a consumer's opt-out to stop the sale of information for marketing purposes does not mean the consumer wants their information to be removed for other non-marketing uses. For example, many sole proprietorships have built a web presence across the internet in the form of positive reviews, a positive financial history and other reputational benefits. Such information is personally identifiable as it can be traced back to a specific individual. The sole proprietor may wish to have their contact information removed from marketing lists but that does not mean they want their online reputation to disappear. **These unintended outcomes can be alleviated by modifying the proposed provision to refer to "service providers" instead of "third parties" and to clarify that the downstream notification obligations are limited to the same or similar use contexts that generated the opt-out.**

D. The Attorney General Should Revise Section 999.316(a) to Require a Single Opt-In

Proposed section 999.316(a) requires a double opt-in when a consumer is requesting to opt-in to the sale of information after exercising their opt-out right. While we agree that opt-in is the appropriate standard, we are concerned that the double opt-in may override consumer choice by signaling that they are doing something wrong by exercising an opt-in. A consumer should be free to exercise their opt-in without barriers designed to signal that their choice is wrong or risky, when that is not the case. **We, therefore, respectfully suggest that the Attorney General revise this provision to require a single affirmative opt-in consent for consumers who wish to opt-in to the sale of their information following an opt-out.**

III. 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, Vice President 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.siiia.net