March 27, 2020

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

RE: Second Set of Modifications to Proposed Regulations to Implement the California Consumer Privacy Act

Dear Attorney General Becerra:

BSA | The Software Alliance appreciates the opportunity to submit comments on the second set of modifications to the proposed regulations to implement the California Consumer Privacy Act ("CCPA").

BSA is the leading advocate for the global software industry before governments and in the international marketplace.[1] Our members are enterprise software companies that create the technology products and services that power other businesses. They offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, and collaboration software. Our companies compete on privacy—and their business models do not depend on monetizing users' data. BSA members recognize that companies must earn consumers' trust and act responsibly with their data. We appreciate California's leadership on these important issues.

BSA's comments focus on the unique role of service providers, which create the products and services on which other businesses rely. As enterprise software companies, BSA members generally act as service providers under the CCPA.[2] Service providers are critical in today's economy, as more companies across a range of industries become technology companies—and depend on service providers for the tools and services that fuel their growth. Software is the backbone of shipping and transportation logistics. It enables remote workplaces and financial transactions all over the world. And it drives the growth of new

[1] BSA's members include: Adobe, Atlassian, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] Of course, when BSA members collect data for their own business purposes, they take on responsibility for complying with the provisions of the CCPA that apply to "businesses" that "determine[] the purposes and means of the processing of consumers' personal information." For instance, a company that operates principally as a service provider will nonetheless be treated as a business when it collects data for the purposes of providing services directly to consumers.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

technologies like artificial intelligence, which have helped companies of all sizes enter new markets and compete on a global scale.

I. The Proposed Regulations Should be Modified to Reflect the Role of Service Providers

The CCPA already recognizes the unique role of service providers, which act on behalf of businesses that determine the purposes and means of collecting personal information from consumers.[3] We encourage the Attorney General to modify the draft regulations in two ways to avoid altering the service provider-business relationship set out in the CCPA:

1. ***Restore the language from the February revisions to Section 999.314(c)(1)***. Under the text of the revised draft regulations released in February, Section 999.314(c)(1) recognized that a service provider may retain, use, or disclose personal information to "perform the services specified in the written contract with the business that provided the personal information." That clear statement reflects the fundamental role of service providers as defined by the CCPA's legislative text: to process information "on behalf of a business" pursuant to a written contract.[4] The newly-revised text is less clear, and instead states that a service provider may "process or maintain personal information on behalf of the business that provided the information . . . and in compliance with the written contract for services required by the CCPA." This language creates uncertainty for service providers that serve joint ventures, or other situations in which multiple businesses seek to jointly engage a service provider.

   We recommend restoring the language from the February text of Section 999.314(c)(1). Alternatively, if the current language is retained, we suggest modifying it to recognize that multiple businesses may jointly engage a service provider, by adding the following italicized/underlined language: "To process or maintain personal information on behalf of the business*(es)* that provided the personal information, or that directed the service provider to collect the personal information, and in compliance with the written contract for services required by the CCPA."

2. ***Revise Section 999.314(c)(3), to clarify that service providers may appropriately augment and correct data for internal uses, but not for building or modifying consumer or household profiles.*** As currently written, Section 999.314(c)(3) may inadvertently reduce the ability of service providers to augment and correct data used for internal purposes, including to train machine learning algorithms. The current language states that a service provider may retain, use or disclose personal information "[f]or internal use by the service provider to build or improve the quality of its services, provided that the use does not include . . . correcting or augmenting data acquired from another source." Read broadly, this could prevent service providers from combining data from multiple sources, if combining the data sets may be viewed as "augmenting" one of the relevant data sets. That raises crucial concerns for

[3] Distinguishing between businesses and service providers is important from a privacy perspective, because adopting this type of role-based responsibility improves privacy protection. Indeed, the distinction is pervasive in the privacy ecosystem. For example, the EU's General Data Protection Regulation ("GDPR") applies to "controllers" that determine the means and purpose for which consumers' data is collected (similar to businesses under the CCPA), and "processors" that process data on their behalf (similar to service providers under the CCPA).

[4] Cal. Civil Code § 1798.140(v).

service providers that use machine learning algorithms – since improving the accuracy of an algorithm and reducing its potential bias may require a provider to combine training data from multiple sources. For example, an algorithm used to detect spam emails is more likely to be accurate if it is trained on data that includes spam emails received by multiple customers of a service provider. Moreover, the algorithm will be even more accurate if the provider specifies, for each spam email in the training data set, how many customers received it. That may be viewed as "augmenting" the underlying data set of spam emails — but is crucial to ensure the algorithm is accurate. Indeed, in this context reading Section 999.314(c)(3) to prohibit such activity may also inadvertently limit the scope of Section 999.314(c)(4), which recognizes that service providers may retain, use, or disclose personal information to detect cybersecurity incidents, or protect against fraud or illegal activity.

To avoid that result, and to ensure Section 999.314(c) does not inadvertently limit the ability of service providers to improve the accuracy and reduce the bias of machine learning algorithms, we recommend revising this clause of Section 999.314(c)(3), to focus more narrowly on prohibiting internal uses that involve augmenting or cleaning data for purposes relating to building or modifying consumer profiles. Narrowing the language in this way is consistent with the overall goal of this provision, while reducing concerns that arise from the current broad language.

Specifically, we recommend revising Section 999.314(c)(3) to delete the following language in strikethrough and add the language in italics/underline: "For internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles to use in providing services to another business, ~~or~~ *including* correcting or augmenting data from another source *for use in such household or consumer profiles*."

II. The Proposed Regulations Should be Modified to Ensure Consumer Rights Are Not Exercised in a Manner that Undermines Consumer Security

Beyond the issues above that are specific to service providers, we also encourage Section 999.313(c)(3) be revised, to ensure that the new consumer rights created by the CCPA are not exercised in a manner that ultimately creates new security risks for consumers. We recommend the following change:

1. ***Restore the original language in Section 999.313(c)(3), and fold it into a revised version of the current four-part test.*** The original language of this section recognized that a business may decline to *provide* a consumer with specific pieces of information in response to a request to know if doing so "creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks." That is critical to ensuring that a consumer's right to access information is not implemented in a manner that creates security risks.

   In February, that language was removed from the draft regulations and replaced by a four-part test setting out instances in which business are not required to *search* for information. As an initial matter, the test should not require that all four parts be met, as the current draft would do. More concerning, though, none of those four parts clearly allow a business to deny a right to know request if compliance would create a security risk. For example, a bad actor could use access requests to try and better understand the business' server network structure and identify weak points in the system. Similarly, an individual involved in criminal activity may seek access to

information that would show whether the company has identified the criminal acts occurring on their platform, such as the successful or unsuccessful use of compromised credentials to access a protected environment. Disclosure of that information could thwart efforts by the company or even law enforcement to address such acts.

We recommend: (1) restoring the original language recognizing that businesses may deny requests to know that raise specific security risks, and (2) merging that language into a revised version of the current four-part test, so that not all parts of the test must be met in order to deny a request to know.

We recommend revising Section 999.313(c)(3) to state:

(3) In responding to a request to know, a business is not required to search for personal information if:

(a) *Disclosure of the specific pieces of personal information creates a substantial, articulable, and unreasonable risks to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks;*
(b) *The business does not maintain the personal data in a searchable or reasonably accessible format, provided that the business: (1) does not sell the information, and (2) describes to the consumer the categories of records that may contain personal information that it did not search under this provision; or*
(c) *The business maintains the personal information solely for legal or compliance purposes, provided that the business: (1) does not sell the information, and (2) describes to the consumer the categories of records that may contain personal information that it did not search under this provision.*

* * *

BSA supports strong privacy protections for consumers, and we appreciate the opportunity to provide these comments. We welcome an opportunity to further engage with the Attorney General's Office on these important issues.

Sincerely,

Kate Goodloe
Director, Policy
BSA | The Software Alliance