December 6, 2019

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

**RE: Proposed Text of Regulations to Implement the California Consumer Privacy Act**

Dear Attorney General Becerra:

BSA | The Software Alliance appreciates the opportunity to submit comments on 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 submits these comments to address the unique role of service providers, which create the products and services that other businesses rely on. Service providers have important obligations to safeguard the privacy of data they process and maintain. The CCPA recognizes this role, including by requiring service providers to act on behalf of businesses and at their direction. A broad reading of the draft regulations risks upsetting the business-service provider relationship set out in statute. We urge three revisions to the draft regulations to avoid that result:

- *First*, to ensure that service providers can meet the specific requests of their customers, the regulations should expressly state that a service provider may use personal information received from a business or consumer to serve another entity—*when a business or consumer directs it to do so.*

- *Second*, and for the same reason, the regulations should also expressly state that a service provider may combine information received from one or more businesses,

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

*when doing so is needed to provide and maintain the services and related services provided to those businesses.*

- *Third*, the regulations should clarify that a service provider should only respond to consumer requests sent to it *by a business*—to help avoid the privacy and security risks associated with requiring service providers to respond directly to consumers, with whom they generally lack a direct relationship.

These changes will together help to ensure the business-service provider relationship established by the CCPA is not inadvertently altered by the draft regulations.

## I. The Unique Role of Service Providers.

As enterprise software companies, BSA members develop and deliver the technology products and services on which other businesses rely. In this role, they 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 financial transactions all over the world. And it drives the growth of new technologies like artificial intelligence ("AI"), which have helped companies of all sizes enter new markets and compete on a global scale.

Businesses entrust some of their most sensitive data—including personal information—with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations. Indeed, many businesses depend on BSA members to help them better protect privacy. For example, our members offer cloud computing services that allow customers to compartmentalize datasets, which can prevent a breach in one location from impacting a full dataset. Other BSA members provide privacy-enhancing technologies that use, for example, data masking, which help companies to reduce the sensitivity of data they hold, and thereby reduce privacy and security threats.

## II. The Difference Between "Businesses" and "Service Providers" Under the CCPA.

The CCPA recognizes the distinct role of service providers. While the statute focuses primarily on businesses, which "determine[] the purposes and means of the processing of consumers' personal information"[3] it recognizes that businesses may engage service providers to

[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. While these comments focus on issues relevant to service providers, we recognize there are a number of issues important to companies acting as "businesses" under the CCPA that are likewise important to BSA. Those include providing more clarity on how businesses can comply with requests to delete, including ensuring a reasonable timeline for deletion of personal information in backup systems, supporting use of security measures like multi-factor authentication in connection with user verification, and providing additional guidance on how businesses are to honor opt-out requests in connection with consumer browser plugins or privacy settings.

[3] *See* Cal. Civil Code § 1798.140(d).

"process[] information on behalf of a business."[4] The CCPA requires service providers to enter into written contracts with businesses they serve, limiting how the service provider can retain, use, and disclose personal information provided to them by a business.[5]

The CCPA also assigns businesses and service providers different obligations, in line with their different roles in handling consumers' data. Since businesses decide why and how to collect a consumer's personal information, they must provide consumers certain rights, including the ability to opt-out of sales of their information. Businesses must therefore direct service providers to help implement certain rights, including the right to delete personal information.[6] But service providers do not decide why a consumer's information is collected or used. Rather, they process the personal information on behalf of a business, pursuant to their written contract.

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). Voluntary frameworks that promote data privacy and cross-border transfers also reflect the distinct roles that different types of companies have in handling consumers' data.[7]

## III. The Draft Regulations Should be Clarified to Avoid Altering the Business-Service Provider Relationship Established in the CCPA.

The draft regulations should not be read to upset the business-service provider relationship created by the text of the CCPA. We encourage three revisions to avoid that result.

### A. Service Providers' Role in Processing Personal Information

Our first two recommendations focus on the portions of the draft regulations addressing how service providers process data provided to them by a business.

*Text of Proposed Regulations*. Section 999.314(c) states that a service provider "shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for the purpose of providing services to another person or entity." However, "[a] service provider may . . . combine personal information received from one or more entities . . . on behalf of such businesses, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity."

*Negative Consequences of Reading Proposed Regulations Broadly*. If this provision were read broadly, it would risk upsetting the business-service provider relationship created in the CCPA.

[4] *See* Cal. Civil Code § 1798.140(v).

[5] *Id*.

[6] *See* Cal. Civil Code § 1798.105(d).

[7] For example, privacy laws in Hong Kong, Malaysia, and Argentina distinguish between "data users" that control the collection or use of data and companies that only process data on behalf of others. In Mexico, the Philippines, and Switzerland, privacy laws adopt the "controller" and "processor" terminology. Likewise, the APEC Cross Border Privacy Rules, which the US Department of Commerce has strongly supported and promoted, apply only to controllers and are complemented by the APEC Privacy Recognition for Processors, which help companies that process data demonstrate adherence to privacy obligations and help controllers identify qualified and accountable processors.

Under the statute, if a business asks a service provider to use personal information to serve multiple businesses, or to combine that information with other data sets, the service provider is obligated to do so. The draft regulations should not be read so broadly to prevent that result.

If Section 999.314(c) were read to prevent these actions, it would have several negative consequences:

- *First*, it would risk placing new obligations on service providers that are inconsistent with their role under the CCPA. In particular, if the draft regulations were read to require a service provider to refuse to process data when a business specifically asks for the data to be provided to multiple businesses, it would effectively require the service provider to decide when it can and cannot process information. Yet the CCPA makes businesses—not service providers—responsible for those decisions.

  By definition, a business "determines the purposes and means of the processing of consumers' personal information."[8] Service providers have no such authority, which is fundamental to the distinction between businesses and service providers under the statute. Moreover, the CCPA prescribes specific contractual and other requirements that entities must observe if they wish to establish and maintain a business-service provider relationship.[9] The draft regulations should not be read to upset this careful balance.

- *Second*, it would risk limiting the ability of businesses to combine information in ways that benefit consumers. Indeed, businesses may ask service providers to combine information with other data sets, or to serve multiple businesses, for a range of purposes that benefit consumers and support responsible innovation—without monetizing consumers' data or using it for advertising. These include:

  - *Serving businesses that enter into a joint venture*. When two businesses want a service provider to act on their behalf, the CCPA allows the service provider to do so, as long as a written contract is in place. Similarly, a business may choose to engage two service providers, and direct them to share data on its behalf. The draft regulations should not be read to prohibit such arrangements.

  - *Providing and improving services.* Businesses may direct service providers to use personal information they disclose to the service provider to improve services offered to multiple businesses. For example, a service provider may use personal information provided by one business to improve an algorithm that powers a service provided to multiple businesses, even without combining the underlying data. Similarly, a business may direct a service provider to combine metadata that is personal information under the CCPA from its

[8] *See* Cal. Civ. Code § 1798.140(c)(1).

[9] *See generally* Cal. Civ. Code §§ 1798.140(v), (d) and (f) (defining "service provider," "business purpose," and "commercial purpose," respectively). A broad reading of the draft regulations would limit the actions of service providers in new ways, not contained in the statutory text of CCPA. Even under the broadest grant of rulemaking authority in the CCPA, *see* Cal. Civ. Code § 1798.185(b), that broad reading of subdivision 999.314(c) would not "fill in the details" of the statutory scheme, *See Ford Dealers Ass'n v. Dep't of Motor Vehicles*, 32 Cal. 3d 347, 362-63 (1982). The broad reading would also conflict with the CCPA's consent requirements, which subjects certain actions to opt-out consent and others to opt-in consent. Reading subdivision 999.314(c) broadly to disallow these actions would also ignore the role of consent in the statutory scheme, and create a ban on processing to which no consent could be given.

business and from other businesses to better provide a service, such as to prepare to handle peak traffic times across geographies.

- *Facilitating research*. Service providers can help entities conducting scientific research by combining multiple sets of data, at the direction of those entities and in line with privacy safeguards they have established. The resulting data could then be used to serve each of the participating entities.

- *Providing benchmarking services to both consumers and businesses*. These services can provide context to a consumer or business seeking to understand how it fits into broader trends. For example, a consumer may want to opt-in to a program that allows her health care provider to use a service provider to combine her information with other data sets, to better understand potential health risk factors. While such a service would depend on the service provider's ability to combine several sets of personal information in order to identify those risk factors, it may limit the information shared with consumers to aggregated or de-identified information about how that consumer fits into these broader trends. Similarly, businesses may use benchmarking services to understand industry trends in hiring and human resources management, and to identify areas in which they may need to invest additional resources.

- *Developing and testing AI systems*. AI systems are trained with large volumes of data. Their accuracy—and benefits—depend on access to large amounts of high-quality data, which service providers may process at the direction of businesses. For example, cities are optimizing medical emergency response processes using AI-based systems, enabling them to more strategically position personnel and reduce both response times and the overall number of emergency trips. The draft regulations should not prohibit service providers from using or combining information for such purposes, at the direction of a business.

- *Supporting open data initiatives*. More broadly, there is increasing recognition among governments and companies of the benefits of sharing data—subject to appropriate privacy protections. For example, in January the United States enacted the OPEN Government Data Act, which makes non-sensitive government data more readily available so that they can be leveraged to improve the delivery of public services and enhance the development of AI.[10] Companies have also supported voluntary information-sharing arrangements, including seeking to develop common terms so that companies that want to share data can more readily do so.[11]

<u>Proposed Revision to Regulations</u>*.* To ensure the draft regulations are not read so broadly as to prohibit service providers from processing personal information at the direction of and on behalf of businesses—we suggest adding the italicized language to Section 999.314(c):

> "A service provider shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for

[10] *See* Public Law No. 115-435, Title II (Jan. 14, 2019).

[11] *See* Microsoft, The Open Use of Data Agreement, *available at* https://github.com/microsoft/Open-Use-of-Data-Agreement; The Linux Foundation Projects, Community Data License Agreement, *available at* https://cdla.io/.

> the purpose of providing services to another person or entity, *except at the direction and on behalf of the business providing the personal information*. A service provider may, however, combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity*, or for purposes compatible with providing the services*."

### B. Role of Service Providers in Responding to Consumer Requests

Our third recommendation addresses the role service providers play in responding to consumer requests under the CCPA.

*Text of Proposed Regulations*. Section 999.314(d) states: "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, or sells on behalf of the business it services, and does not comply with the request, it shall explain the basis for the denial. The service provider shall also inform the consumer that it should submit the request directly to the business on whose behalf the service provider processes the information and, when feasible, provide the consumer with contact information for that business."

*Negative Consequences of Proposed Regulations*. This provision also risks upsetting the business-service provider relationship established in the CCPA. In particular, Section 999.314(d) could be read to require service providers to evaluate and respond to consumer requests to know or delete personal information—an obligation not placed on them by the CCPA.

Under the text of the CCPA, service providers merely play a supporting role in executing deletion requests on behalf of businesses.[12] Notably, the statute requires *businesses* to delete personal information pursuant to a verifiable consumer request and to "direct any service providers" to do the same.[13] The statute thus anticipates that service providers act *at the direction of businesses*—and not at the direction of consumers, with whom they lack a direct relationship. The connection between right to know requests and service providers is even more attenuated; the text of the law does not refer explicitly to service providers in connection with the right to know.[14] As a result, "neither the CCPA nor the regulations require service providers to comply with such requests."[15]

This arrangement is for good reason. Requiring service providers to respond directly to consumer requests invites a host of security and privacy risks, which arise because service providers generally do not interact with consumers. In the ordinary course, a service provider may not maintain information about the consumers its business customers serve—and thus would not ordinarily review records containing their names, services provided, or other information needed to respond to a request. Service providers should not be encouraged to seek out that information, if they would not otherwise have access to it. For example, a service provider that works with multiple businesses may not be able to identify the business relevant to a consumer's request without combing through personal information it provides on a host of businesses, to identify the relevant one. That result should be avoided, because it would invade consumers' privacy, not protect it. Likewise, service providers may not have sufficient

[12] *See* Cal. Civ. Code §§ 1798.105(c), (d).

[13] *See* Cal. Civ. Code § 1798.105(c).

[14] *See generally* Cal. Civ. Code §§ 1798.100 and 1798.110.

[15] *Initial Statement of Reasons*, at 22-23.

information to verify a consumer’s request, and thus could create security risks in responding directly to a consumer without verifying her identity.

Instead, the CCPA recognizes that businesses should respond to consumer requests—since they have the most complete understanding of what data they control about a particular consumer. Section 999.314(d) should be revised to ensure it does not alter this process.

*Proposed Revision*. We suggest revising Section 999.314(d) to more clearly reflect the existing statutory scheme, by deleting the language in strikethrough below and adding the language in italics.

> “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, or sells on behalf of the business it services~~, and does not comply with the request, it shall explain the basis for the denial. The service provider shall also~~ *then the service provider shall* inform the consumer that it should submit the request directly to the business ~~on whose behalf the service provider processes the information, and when feasible, provide the consumer with contact information for that business.~~ *with which the consumer interacted*.”

* * *

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

Kate Goodloe
Director, Policy
BSA | The Software Alliance