GUNDERSON DETTMER

SILICON VALLEY
ANN ARBOR
BEIJING
BOSTON
LOS ANGELES
NEW YORK
SAN DIEGO
SAN FRANCISCO
SINGAPORE

December 6, 2019

By email to privacyregulations@doj.ca.gov

With a copy to:
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Re: Comments to the Attorney General's CCPA Implementing Regulations

Dear Sir/Madam:

On behalf of a working group of California and national in-house and law firm attorneys, organized by Smithline PC, we thank you for the opportunity to submit comments regarding the Attorney General's CCPA Implementing Regulations (California Consumer Privacy Act Regulations (Stats. 2018, Ch.55 [AB 375], as amended by Stats. 2018, Ch. 735 [SB1121])) (the "Implementing Regulations").

We support the Attorney General's stated goal of providing clarity and specificity to assist in the implementation of the CCPA. For the reasons set forth below, we believe that in their current form, the draft Implementing Regulations will not achieve the stated goal, and in many cases risk introducing additional uncertainty for businesses and service providers seeking to comply with the CCPA.

Further, we believe that, while this uncertainty will hamper companies of all sizes, it will disproportionately impede (and create barriers to entry for) innovative smaller companies vis-à-vis their larger incumbent competitors who already have the money, legal resources, and legacy databases necessary to move forward despite the uncertainty.

With this in mind, we have outlined below our proposed revisions to the Implementing Regulations. These clarifications address ambiguities in the CCPA and the draft Implementing Regulations, and aim to provide more concrete guidance to companies on how to comply with the CCPA.

I. TABLE OF CONTENTS

	Issue	Para. Ref.
A.	Opt-In Consent for New Purpose	11 CCR § 999.305(a)(3)
B.	Service Providers	11 CCR § 999.314
C.	Compliance with Browser Opt-Out Signals	11 CCR § 999.315(c)
D.	Responding to Consumer and Agent Requests	11 CCR §§ 999.313 and Article 4
E.	Compliance Concerns Not Addressed in Current Draft of Implementing Regulations	N/A

II. PROPOSED AMENDMENTS AND REQUESTS FOR CLARIFICATION

A. Opt-In Consent for New Purpose - 11 CCR § 999.305(a)(3)

§ ***999.305(a)(3)*: [Comment: AG should not introduce new requirements exceeding the scope of the CCPA]**

1. Background: § 999.305(a)(3) provides that explicit consent is required for a business to use a consumer's personal information for any purpose other than those disclosed in the notice at collection.

2. Comment: This provision creates a new consent requirement for certain processing of personal information that a business initially performed legally on a notice basis (*with no consent required*). § 1798.100 of the CCPA expressly states that "A business shall not … use personal information collected for additional purposes without providing the consumer with notice consistent with this section." As such, this provision in the Implementing Regulations is in direct conflict with, and significantly exceeds the scope of, the CCPA, even though it was not introduced through the appropriate legislative process.

   Additionally, this provision does not increase privacy protections for California consumers. Instead, it incentivizes businesses to create over-broad, lengthy privacy notices covering every potential "purpose" and use of personal information they may consider in the future, leaving California consumers without meaningful and readable disclosures about how businesses use their personal information. This directly conflicts with the requirement in § 999.305(a)(2) to have a notice at collection that is "easy to read and understandable to an average consumer."

3. Request: We request the Attorney General reverse this material expansion of the scope of the CCPA and remove subsection (a)(3), or, alternatively, clarify that the express consent to a different purpose only applies when the initial processing was consent-based. To the extent the Attorney General believes there needs to be a requirement for consent-based processing of personal information in certain circumstances, that change should be made directly through the legislative process.

B. Service Providers - 11 CCR § 999.314

***Subsection (a)*: [Comment: Vast Expansion of Scope of Service Providers]**

1. Background: § 999.314(a) provides that a "person or entity" is still a "service provider" if it (1) provides services to a "person or organization" that is not a business and (2) otherwise meets the "service provider" definition. The Initial Statement of Reasons for these changes focuses on non-profit and government entities as potential non-business service recipients. For context, under the statute a "business" or "service provider" must be an *entity* ("sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity …") and an entity is a service provider only if it provides services to a "business" as defined by the statute. (§§ 1798.140(c)(1) and (v))

   Comment: The Attorney General's proposed regulations raise two important issues. First, this provision expands the definitions of "service provider" and "business" to include individuals in addition to legal entities. Second, in addition to non-profits and government entities, this would capture for-profit companies that do not meet the CCPA's criteria for a business. The proposal exceeds the scope of the statute and imposes contractual obligations and potential liability on service providers for whom there is no corresponding "business". The effects would fall especially on service providers to small businesses (who are likely small businesses themselves).

2. Request: We request the Attorney General reverse this material expansion of the scope of entities that qualify as service providers. To the extent the Attorney General believes other for-profit entities should be covered as businesses, that change should be made directly through the legislative process.

***Subsection (c)*: [Comment: AG Should Not Overrule Statute's "Reasonably Necessary and Proportionate" Standard]**

1. Background: § 999.314(c) prohibits a service provider from using one customer's personal information "for the purpose of providing services to another person or entity." The sole exceptions relate to security, fraud and illegal activity. In explaining this new rule, the Attorney General states that other uses across businesses would be "outside the bounds of a 'necessary and proportionate' use of personal information" under the statute's standards for a permitted business purpose. (See § 1798.140(d))

2. Comment:

   a. General. We support the Attorney General's goal of providing clear guidance for a complex statute. We are concerned, however, that the proposed regulation exceeds the scope of the statute and could have serious unintended consequences for California technology companies and consumers.

   b. Standard Industry Practice. Enterprise businesses frequently authorize service providers to use personal information to build, support and improve the services they provide. These activities are essential to technology development and benefit businesses, service providers and consumers. For instance, a service provider might use personal information provided by a business internally for feature optimization, troubleshooting bugs, or training algorithms that benefit all customers. (In modern product architecture, using only de-identified information for these purposes may be insufficient.)

   c. Part of the Service. These activities are expected as *part of the service provider providing its service as requested by customers*. Under the CCPA, they may certainly constitute "reasonably necessary and proportionate" business purposes within the service context. (§ 1798.140(d)) By way of analogy, the GDPR uses a balancing test of "legitimate interest" rather than predetermining all permitted uses of personal information.

   d. Respect for Private Contract. Businesses are sophisticated parties and the data rights they grant service providers depend on the services involved. Their private contracts should be respected, provided the contracts otherwise comply with the CCPA and businesses meet the CCPA's requirements in collecting personal information. The proposed regulation could void existing contracts and cause many enterprise SaaS services to become arguably "non-compliant" overnight under a rule that, by definition, refuses to even allow consideration of the nature of the parties, data or services involved. Note further in this context that most SaaS providers operate on a "single build" model, so any product changes implemented in response to this proposed regulation would likely de facto be extended to all users in all jurisdictions.

   e. Unneeded Change. Subsection (c) is unnecessary and appears to conflict with the statute. The statute already prohibits the service provider's use of personal information for "commercial purposes" outside of the service context, while also expressly allowing use for the service provider's "business purposes." This fact-based standard accommodates a variety of service types and relationships. (§ 1798.140(d) and (v))

   f. Exceeds Statutory Authority. The proposed regulation upsets that statutory balance, introducing a vague rule that certain uses of data could *never* be

"reasonably necessary and proportionate", regardless of circumstances. No authority is cited for this sweeping change and none is evident.

g. Unintended Consequences. The scope of subsection (c) is unclear. However, a blanket prohibition on using personal information for service improvement (if that is the regulation's intent or effect) would have no precedent at law, would disrupt technological and economic development, and runs contrary to industry practice and freedom of contract. While sector-specific statutes may impose restrictions on specific regulated information (e.g., financial, health or student data), the CCPA applies broadly to all personal information. It must remain flexible enough to apply across all industries and over time.

3. Request: We request that the Attorney General modify subsection (c) as follows:

   a. Clarify that, when authorized by the business, a service provider may internally use personal information provided by a business to build, support or improve the service provider's services and for other permitted business purposes.

   b. Alternatively, remove subsection (c).

These clarifications would protect consumers' privacy interests and provide much-needed clarity in the marketplace, while enabling the continued technology development on which California companies and millions of consumers rely.

§ ***1798.140 of Statute*: *Definition of "Service Provider" vs. "Third Party"*** **[Comment: Need to Separate Service Provider and Third Party]**

1. Background: The CCPA creates two types of parties that process personal information under contract with a business: "service providers" and persons who are *not* "third parties" (to whom we refer as exempt third parties). While similar, each has different rights and obligations, creating confusion in the marketplace as to what contractual terms are required. (§ 1798.140(v) and (w))

2. Request: We request clarification of the relationship between service providers and exempt third parties, and specifically, confirmation that those who are "service providers" need not also be characterized as exempt third parties.

§ ***1798.155(a) of Statute*: *Seeking Opinion of Attorney General*** **[Comment: Service Providers May Also Seek Opinion]**

1. Background: The CCPA provides that "Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title." (§ 1798.155(a)) Service providers are not expressly mentioned, but also have legitimate reasons to seek the Attorney General's opinion regarding compliance.

2. Request: Add service providers to the parties that may seek the Attorney General's opinion under § 1798.155(a). The ability of a service provider to clarify its compliance obligations will benefit it, the businesses it deals with and consumers.

C. Compliance with Browser Opt-Out Signals – 11 CCR § 999.315(c)

§ ***999.315(c)*: [Comment: AG should not introduce new requirements exceeding the scope of the CCPA]**

1. Background: § 999.315(c) states that a business shall treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request for that browser or device, or, if known, for the consumer.

2. Comment: Pursuant to the California Online Privacy Protection Act ("CalOPPA"), website operators are required to state how they respond to "Do Not Track" browser signals, but are not required to implement technology changes to recognize and honor such signals. The requirement in the Implementing Regulations for businesses to be technically able to recognize and comply with "Do Not Sell" browser plugins or other browser privacy settings is a new, onerous requirement that exceeds the scope of the CCPA and existing California law. There is currently no standardized protocol for "Do Not Sell" browser requests or controls that businesses can reasonably identify and comply with, and any new requirement for businesses to recognize and honor browser signals and plugins needs to be addressed through the California legislative process.

3. Request: Amend § 999.315(c) to state that businesses are required to state in their privacy policy if and how they respond to "Do Not Sell" browser signals or settings, and if a business is unable to comply with such signals, it shall specify other available methods of submitting a "Do Not Sell" request as set forth in § 999.315(a).

D. Responding to Consumer and Agent Requests – 11 CCR §§ 999.313 and Article 4

§§ ***999.313 and Article 4*: [Comment: Need certainty on a business' liability when responding to consumer requests, including when dealing with an "authorized agent"]:**

1. Background: The Implementing Regulations provide general guidance regarding a business' response to consumer requests in a variety of circumstances, depending on the type of request, the sensitivity of information involved, the degree of certainty required for verification and whether the request is made by a consumer, household member or authorized agent.

2. Comment: These guidelines inherently require a business to undertake a fact-based inquiry and exercise good-faith discretion. This leaves open the question of whether a business acting in good faith could be exposed to liability if it discloses or deletes

information in response to a request that is later determined to be fraudulent. The concern is heightened for requests from putative authorized agents. Even if the Secretary of State maintains a registry of authorized agents, it may be difficult for businesses to validate that *a particular agent* is truly authorized by *a particular consumer*, considering that consumer permissions or agent communications each may be forged. Since the GDPR took effect, EU businesses have been overwhelmed by automated, large-scale data subject requests through third party agents, often including fraudulent requests seeking to obtain data subjects' identity information or introduce phishing malware via suspicious links. Given technical limits and the sophistication of online crime, there is no fail-safe guarantee against fraud.

Businesses may reasonably be concerned about potential exposure under the CCPA or other laws based on their mistaken response to a consumer request. Without further clarity, businesses are left with a Hobson's choice: they will either tend *not* to disclose or delete the requested information without complete certainty of the request's validity (frustrating the consumer interests the CCPA is designed to protect) *or* they will risk potential liability for good faith disclosures in response to requests later determined to be fraudulent.

3. Request: We request that the Attorney General create a liability safe harbor for businesses: a business shall not be liable if, in response to a consumer or authorized agent request, it discloses or deletes information in good faith in accordance with a documented verification method reasonably designed to comply with the Implementing Regulations. We also request that the Attorney General provide further guidance regarding the proof a business is required to seek in order to verify that a particular agent is authorized by a particular consumer.

E. Compliance Concerns Not Addressed in Current Draft of Implementing Regulations

***Website Cookies Shared with Third Parties*:**

1. Background: A common practice for businesses engaged in behavioral or interest-based advertising is the use of cookies placed on website visitors' devices and subsequently sent to third parties in exchange for information about such website visitor. Neither the CCPA nor the Implementing Regulations provide guidance on how to ensure compliance with respect to this common practice.

2. Request: We ask that the Attorney General provide clarity on whether the use of website cookies shared with third parties constitutes a "sale" of personal information pursuant to the CCPA.

***Personal Information in User-Generated Content*:**

1. Background: Many websites and mobile applications allow for the uploading of significant amounts of user-generated content, which content is provided at the

discretion of the user. Sometimes the uploaded content includes personal information of consumers other than such user; however, the business (a) may have no way of knowing that such personal information has been included in uploaded content and (b) in any case, has no contact information or relationship with a consumer whose personal information may be so included in the content of uploading user.

2. Request: We ask that the Attorney General provides clarity on how to comply with the CCPA with respect to personal information that may be included in user-generated content. The business typically will not have contact information for the consumer whose personal information may be included in the content of a user (and may not be aware that such personal information is included in uploaded content), and, accordingly, the business cannot provide a privacy notice or notice at collection directly to such consumer.

   In particular, we would welcome clarification from the Attorney General that having the required notice and privacy policy prominently posted or referenced on the business' website or mobile application, as applicable, is sufficient for this common use case.

Thank you for your consideration of these comments. We appreciate the opportunity to provide ideas and information to assist in the process of clarifying the CCPA compliance obligations.

Note: **The opinions and views expressed in these comments are those of the individual attorney authors and do not necessarily reflect the opinions or views of any such attorney's employer or client. Affiliations are provided for identification purposes only.**

Very truly yours,

Anna Westfelt

Anna Westfelt
Of Counsel
Gunderson Dettmer Stough Villeneuve Franklin & Hachigian, LLP

Derek Schwede

Derek Schwede
Principal
Smithline PC

Todd Smithline

Todd Smithline
Managing Principal
Smithline PC

Amanda Weare
Associate General Counsel – IP, Product and Privacy
Collibra Inc.

Jeffrey L. Poston
Partner
Crowell & Moring LLP

Gabriel M. Ramsey
Partner
Crowell & Moring LLP

Lee Matheson
Associate
Crowell & Moring LLP

David Mitchell
VP, Legal
Demandbase, Inc.

Elaine Tan
Sr. Manager, Compliance
Demandbase, Inc.

Vikki Nguyen
Associate
Gunderson Dettmer Stough Villeneuve Franklin & Hachigian, LLP

Xavier Le Hericy
Chief Privacy Officer
New Relic, Inc.

Diane Nahm
Head of Legal
RealtimeBoard, Inc. dba Miro

Mark Kahn
General Counsel and VP of Policy
Segment.io, Inc.

Brandon Wiebe
Senior Corporate Counsel
Segment.io, Inc.

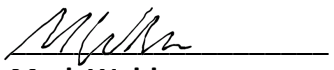
Audrey Kittock
Corporate Counsel
Segment.io, Inc.

Lisa Babel
General Counsel
StreamSets, Inc.

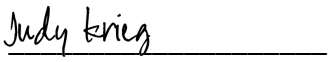
Diana Olin
Assistant General Counsel
Sumo Logic, Inc.

Eric Lambert
Division Counsel
Trimble Inc.

Annie Sun
In-house Attorney



Mark Webber
U.S. Managing Partner, Technology and Privacy
Fieldfisher (Silicon Valley) LLP



Judy Krieg
Partner, Privacy, Security and Information
Fieldfisher LLP