Before the
CALIFORNIA DEPARTMENT OF JUSTICE
Los Angeles, CA 90013

In the Matter of	)
	)
Revised California Consumer Privacy Act	)
Implementing Regulations	)

COMMENTS OF THE COMPUTING TECHNOLOGY INDUSTRY ASSOCATION

Dileep Srihari
Vice President and Senior Counsel

Alexi Madon
Vice President, State Government Affairs

COMPUTING TECHNOLOGY
INDUSTRY ASSOCIATION
3500 Lacey Road, Suite 100
Downers Grove, IL 60515

February 25, 2020

INTRODUCTION

The Computing Technology Industry Association (CompTIA),[1] the leading association for the global information technology (IT) industry, respectfully submits these comments in response to the Department of Justice's revised California Consumer Privacy Act (CCPA) regulations. CompTIA's member companies encompass a wide cross-section of the IT sector, including software, technology services, telecommunications services, and device and infrastructure companies. Our members are committed to ensuring the privacy and security of customer data through well-crafted protections that achieve meaningful benefits, while avoiding unnecessary restrictions that would limit innovation and/or impose significant costs that would ultimately harm competition and consumers.

In these comments, we offer additional guidance to address concerns that remain in the revised version of the regulations. CompTIA appreciates the changes the Department made to the prior version in response to stakeholder feedback. While a number of these changes represent an improvement to the regulations, we believe that additional edits to the proposed regulations should be made. These edits are addressed below.[2]

DISCUSSION

I. § 999.301(a). Authorization Should Not Include Multiple Steps

The draft rules define "affirmative authorization" as:

> an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a child under 13, it means that the parent or guardian has provided

[1] CompTIA supports policies that enable the information technology industry to thrive in the global marketplace. We work to promote investment and innovation, market access, robust cybersecurity solutions, commonsense privacy policies, streamlined procurement, and a skilled IT workforce. Visit www.comptia.org to learn more.

[2] The proposed edits in these comments do not necessarily represent the only areas for improvement in the proposed regulations.

> consent to the sale of the child's personal information in accordance with the methods set forth in section 999.330. For consumers 13 years and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.

CCPA requires detailed notice concerning consumers' right to opt in to the sale of their information. This requirement, along with consumers having to affirmatively and "clearly request to opt-in," works to ensure that consumers are making informed choices.

It is therefore unclear why consumers would need to undertake an extra step concerning their affirmative and clear choice. Multiple pop-ups and other prominent notices can interrupt consumers' experiences and lead to confusion. The more notifications presented to consumers, the less likely consumers can comprehend or absorb any one particular notice and make informed choices about their data.

The more notices that companies display, the greater the chance of creating "click fatigue," whereby consumers skip over the words and click through to continue using the service. To address this issue, we suggest striking the language mandating a two-step process.

II. § 999.305(d). The Indirect Collection Exception Should Apply Beyond Data Brokers.

As § 999.305(d) was previously written, businesses did not need to provide notice at collection if they did not collect information directly from consumers. The revised language now states that only registered data brokers do not need to provide notice at collection in instances of indirect collection:

> If a ~~A~~ business that does not collect information directly from consumers is registered with the Attorney General as a data broker pursuant to Civil Code section 1798.99.80, *et seq.* it does not need to provide a notice at collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out. ~~to the consumer,~~

We do not believe notice at collection should be required when any business, and not just a registered data broker, indirectly collects publicly available data. For that reason, the prior exception should be reinstated to apply to all businesses.

III. § 999.305(a)(4). The Just-In-Time Notification Obligation Should Be Removed.

The just-in-time requirement for mobile devices proposed in § 999.305(a)(4) does not exist in the CCPA and goes well beyond the obligations for notice at collection in the CCPA. Additionally, the proposed standard – a "purpose that the consumer would not reasonably expect" – is too vague. Facing such a vague requirement, companies may provide more just-in-time notices than is warranted or necessary. The resulting over-notification, depending upon the nature of the app, could negatively impact user privacy and experience. For these reasons, this proposed requirement should be removed.

IV. § 999.306(f). The Opt-Out Button Graphic Should Be Deleted.

The draft rules have proposed an optional "Do Not Sell My Personal Information" and "Do Not Sell My Info" toggle button. We urge the Department to remove this toggle button as an option due to its unclear design, which inadvertently suggests it is an actual control, whereas it is intended to serve as a link so that consumers can obtain additional information. The button omits important nuances that each business might need to convey based on specific practices. Moreover, excessive standardization could lead to consumers ignoring notifications altogether. The draft requires privacy notices to be "reasonably accessible to consumers with disabilities," yet standardized notification requirements like the envisioned toggle button can fail consumers with disabilities and diverse needs. Businesses will be in the best position to craft notices appropriately tailored to help inform consumers with specific needs and abilities, as they are continuously conducting user interface (UI) and user experience (UX) research.

V. § 999.307. The Value of Consumer Data Disclosure Requirements Should Be Deleted.

The section requires "[a]n explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including: a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and a description of the method the business used to calculate the value of the consumer's data."

We recommend removing any requirements for providing an estimate of the value of consumer data. We propose:

> "[a]n explanation of how the financial incentive or price or service difference reasonably related to the value of the consumer's data~~, including: a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and a description of the method the business used to calculate the value of the consumer's data~~."

We also propose striking 999.37, which describes the methods in calculating the value of consumer data.

The perceived value of data is subjective, in flux, and depends on context. It does not have independent value. Because data lacks clear, objective value, academics have come up with various methods for estimating the value of certain services to people. Regarding free, ads-based, personalized services, people do not give up or exchange data for their experience. Rather, the experience is made possible by data. This distinction is important. Data enables ads-based services to provide the core of the service itself, which is personalized content. The reason certain businesses can offer their services for free is ***not*** that they are being compensated for an individual's data. They make money selling advertisements. These businesses sell advertisers the opportunity to present their messages to people. And advertisers pay the businesses based on

objective metrics such as the number of people who see their ads or the number of people who click on their ads.

VI. § 999.308(c)(1)(e). The New Notification Requirement for Categories of Third Parties Should Be Removed.

The revised proposed regulations would require businesses to disclose "the categories of third parties to whom the information was disclosed or sold" for "each category of personal information identified." The requirement is needlessly burdensome. Disclosing additional categories of third parties will make the privacy policies less consumer-friendly and complicated, and will be burdensome for businesses. As a result, we suggest that this provision be removed.

VII. § 999.312(b). The "Exclusively Online" Exception Should Be Extended to Deletion Requests.

We agree that business operating online should have an exception from the requirement to provide two methods for right to know requests. This same exception should be extended to deletion requests. A single email point of contact aligns with international standards for rights requests, would be simpler for consumers, and makes it easier for online businesses to comply with the CCPA.

VIII. § 999.313(c)(1). Obligations for Unverified Requests Should Be Removed.

The obligations under § 999.313 for *unverified* requests conflicts with the CCPA. Understandably, the CCPA contemplates that unverified requests should be *discarded* because they are unverified: "A business is not obligated to provide information to the consumer pursuant to Sections … 1798.105 … if the business cannot verify … that the consumer making the request is the consumer about whom the business has collected information …" This approach protects the consumer, as a business should discard an unverified request. If a business is unable to verify the individual's identity, it should not act on requests related to that

consumer's personal information. Additionally, the CCPA already has a mechanism for opting-out of the sale of information. Combining verification and opt-out procedures is contrary to the statute and creates the potential for abuse. As such, we recommend making the following edits:

> For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the consumer that it cannot verify their identity. ~~If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subSection (c)(2).~~

IX. § 999.313(c)(3). The Security Risk Exception Should Be Reinstated.

We request that the eliminated language on "security risks" be reinstated. This language would have enabled a business to not provide specific pieces of information if it met a particular security risk threshold. It was intended to ensure that businesses would not have to compromise security to comply with the law. Accordingly, we request that this language be restored:

> 999.313(c)(3) A business shall not provide a consumer with specific pieces of personal information if the disclosure 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.

X. § 999.313(c)(3). Additional Clarification Should Be Provided on When Businesses Should Not Be Required to Search for Personal Information in Response to a Right to Know Request.

We suggest clarifications on conditions under which businesses should not be required to search for personal information in response to a right to know request. As currently written, the draft requires a business to meet enumerated conditions to excuse the business from conducting a search. However, operationally, the exceptions do not work together. For example, when a business maintains personal information solely for legal or compliance purposes (subsection b) it must maintain that information in a searchable or reasonably accessible format (subsection a) so that it can undertake its legal or compliance purposes.

Further, the statute and draft regulations currently lack sufficient clarity regarding how far the access right extends. A clear regulation is necessary to draw outer lines around the information a business must make available. Many businesses possess data that may technically fall within the CCPA's broad definition of "personal information," but that is not used in the ordinary course of business, such as log data, is not readily accessible, or has not been "collected." This is particularly true with data that the business has derived, rather than collected, the data. Requiring a business to identify, compile, and then make accessible such information has the adverse effects of forcing a business to create new or more robust consumer profiles. This creates privacy and security concerns for consumers by associating more data with them than otherwise would be, as businesses will be required to build systems with more detailed consumer profiles and then send those profiles outside of the business. Accordingly, we recommend the following edits:

> A business shall not provide a consumer with specific pieces of personal information if the disclosure 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, networks, or consumers. In responding to a request to know, a business is not required to 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 it did not provide because it meets one of the conditions stated ~~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 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.

~~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.~~

XI. § 999.313(c)(4). Payment Card Numbers Should Be Included.

We agree that highly sensitive personal information, such as a consumer's Social Security number, driver's license number, and financial account number, should not be disclosed in response to a request to know. We recommend that § 999.313(c)(4) also include payment card numbers on the list of personal information that should not be disclosed in response to a rights request.

XII. § 999.315(d)(1). An Opt-Out Inherently Includes Defaults.

The language in § 999.315(d)(1) is confusing because "shall not be designed with any pre-selected settings" suggests that there can be no default, when it is quite clear that the default would allow for sale of personal information. A consumer is required to select the "opt-out" and an opt-out inherently includes defaults. Accordingly, the language should be modified as follows:

> 999.315(d)(1). Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a customer intends to opt-out of the sale of personal information. The privacy control shall require that the consumer affirmatively select their choice to opt-out and shall not be designed in a manner that would prevent the sale of personal information unless the customer affirmatively selects their choice to opt-out. ~~with any pre-selected settings~~.

XIII. § 999.316. The Two-Step Process for Opt-In Should Be Removed

The draft continues to envision a two-step process to opt in to the sale of data, where the consumer requests to opt in to the sale of data and then confirms the opt-in. Multiple pop-ups and other prominent notices are highly likely to be noticed, but can interrupt consumers'

experiences. The more notifications presented to consumers, the less likely consumers are to comprehend or absorb any one particular notice and make informed choices about their data. The more notices that companies display, the greater the chance of creating "click fatigue," whereby consumers just skip over the words and click through to continue using the service. We therefore suggest striking the reference to a required "two-step" process.

XIV. § 999.317(g). The Recordkeeping Requirements Should Be Deleted

The reporting and recordkeeping requirement presented in §999.317(g) does not exist in the statute itself and therefore has no support in the law. Additionally, the requirement is burdensome and provides little value to consumers. We believe this requirement should be deleted altogether, or at the very least, the requirement to have the metrics posted on the privacy policy should be removed. The percentages of approvals compared to denials for requests under the CCPA, for various reasons, could be very different for different organizations. These differences could be based upon legitimate reasons. However, the differences in these numbers could be misleading to consumers and needlessly cause reputational damages to businesses.

CONCLUSION

CompTIA and our member companies continue to take consumer privacy issues very seriously, and well-crafted privacy protections must achieve meaningful benefits while avoiding unnecessary restrictions that would harm innovation, hurt competition, drive up costs, or violate the statutory scheme established by the Legislature. While we believe the Department has made progress between its initial draft and most recent draft of the regulations, we believe additional changes should be made. We urge the Department to adopt the changes described above, and we look forward to reviewing feedback from others on the draft regulations.

Sincerely,

/s/ Alexi Madon

Dileep Srihari
Vice President and Senior Counsel

Alexi Madon
Vice President, State Government Affairs

COMPUTING TECHNOLOGY
INDUSTRY ASSOCIATION
3500 Lacey Road, Suite 100
Downers Grove, IL 60515