State Privacy and Security Coalition, Inc.

COMMENTS TO THE ATTORNEY GENERAL

February 25, 2020

California Department of Justice
Attn: Privacy Regulations Coordinator
300 Spring Street
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

Re: Comments Regarding Title 11(1)(20): CCPA Revised Proposed Text of Regulations

I. Introduction

The State Privacy & Security Coalition is a coalition of 30 companies and 8 trade associations across the retail, payments, communications, technology, fraud prevention, tax preparation, automotive and health sectors. We work for laws and regulations at the state level that provide strong protection for consumer privacy and cybersecurity in a consistent and workable matter that reduces consumer confusion and unnecessary compliance burdens and costs.

Our Coalition worked with Californians for Consumer Privacy and other consumer privacy groups on amendments to clarify confusing language in the CCPA, to reduce the risk of fraudulent consumer requests that would create risks to the security of consumer data, and to focus CCPA requirements on consumer data, consistent with the title of the law.

We appreciate that the revised draft Regulations address and resolve a number of the outstanding confusing features of the law. We focus these comments only on clarifications to new proposals in the revised proposed rules, with the exception of the "do not sell" signal component, which we urge the Attorney General's Office to suspend pending resolution of the California Privacy Rights Act Initiative ("CPRA"), No. 19-0021, filed Nov. 13, 2019.

As we noted in our opening comments, the CCPA has already been amended and changed twice. The rules will change CCPA requirements *a third time* (after two drafts).

If approved by the voters in 2020 (as appears likely), the CPRA will make further changes in 2023 and will move authority over this area of the law to a new agency, and will require rulemakings by that new agency in 14 more areas. These repeated changes make the CCPA a "moving target" and create needless and wasteful uncertainty. We urge your office to give weight to this concern as it finalizes its CCPA rules.

500 8th Street, NW
Washington, DC 20004
202.799.4000 Tel
202.799.5000 Fax

II. AG's Office should not issue rules, such as the Do Not Sell Signals Rules, that differ from both the statute and CPRA

By way of example, the proposed "do not sell" signal or browser or device settings are mentioned nowhere in the CCPA, including in Civ. Code § 1798.185(a)(4), which authorizes an AG rulemaking on the do not sell icon, but not on a technical setting expressing a do not sell request.

But leaving aside the question of whether the Attorney General's Office has the statutory authority on this issue, moving forward *at this juncture* with a rule on this question is unwise public policy because the CPRA would address the issue very specifically. If the CPRA is approved, it would establish different requirements regarding providing consumers with the ability to opt out of selling or sharing personal information. Honoring an opt-out preference is one of the options provided, and including the required hyperlink to limit sharing of personal information and secondary use of sensitive personal information is another compliance option. What is more, websites would be able to present on a landing page reasons why the Internet user should agree to a CCPA data "sale." CPRA, § 1798.135(b)(2). The CPRA would provide for two rulemakings to clarify the requirement. CPRA, § 1798.185(a)(19)-(20). It would also make this requirement effective in 2023, only after the rulemakings regarding practical implication issues. CRPRA, § 31. This is a more nuanced approach than the one in the proposed rule, and one that is arguably more narrowly tailored for purposes of a challenge in a 1st Amendment action that may be brought by smaller Internet advertising firms that lose access to personal information under a "do not sell" technical settings system in which individuals are not making case-by-case choices about use of their personal information.

The AG's Office will know in a matter of months whether the CPRA Initiative has enough valid signatures to appear on the November 2020 ballot, and in November 2020, whether the CPRA has been approved by the voters. It would be far more sensible to defer consideration of this aspect of the proposed rules until after the outcome of the CPRA is known.

It would be needlessly confusing to issue a do not sell rule that would change significantly three years later. This aspect of the proposed rules would serve no purpose because the new agency is called upon to issue these rules in 2023. The proposed rule contains no process at all for clarifying the system and how it would be implemented technically. Because there is no such signal today, these questions are very important. The CPRA requires two further rulemakings to develop real rules on this issue, then time for the development of a technical standard, and then deployment of technology to make the privacy control effective. Because it would take time for the technical signal mentioned in the proposed rule to be implemented, there is no interest in rushing to finalize this aspect of the proposed rules. The far wiser course is to hold this aspect of the rule in abeyance until November 2020, once the outcome of the CPRA Initiative is known.

500 8th Street, NW
Washington, DC 20004
202.799.4000 Tel
202.799.5000 Fax

III. The Final Rules Should Restore the Risk Exception in § 999.313(c)(3) from Disclosing Specific Pieces of Personal Information where there is "a Substantial, Articulable, and Unreasonable Risk to the Security of that Personal Information"

The latest version of the proposed rules would strike a critical fraud exception in the previous version of § 999.313(c)(3) against disclosing specific pieces of personal information where there is a substantial, articulable and unreasonable risk to the security of that personal information. This exception should be restored in the final rules.

The exception was tightly drafted and addressed the very real risk of "pretexting" requests for personal information. This risk is heightened because other parts of the proposed rules would allow third party authorized agents to obtain access to and delete personal information of individuals. In this environment, fraudsters and even foreign intelligence services may attempt to abuse the CCPA access right to obtain personal information about California residents. If they are sophisticated, they may well be able to phish or otherwise obtain the requisite number of verifying data elements and falsify an authorization request.

For these reasons, it is very important that this exception be restored in order to avoid undermining the privacy of Californians' personal information in ways that can be very damaging.

IV. The Clarification in § 999.302 Regarding the Status of IP Addresses Is Helpful But Should Be Clarified Further to Address the Status of Deidentified Data and Aggregate Data

The guidance inserted in new § 999.302 regarding the status of IP addresses is generally helpful, but is incomplete and not yet accurate because it does not account for IP addresses that are de-identified or aggregated and thereby fall outside the definition of "personal information."

The Civ. Code § 1798.140(o)(2) was amended in 2019 to clarify that: "'Personal information' does not include consumer information that is deidentified or aggregate consumer information." This clarification should be reflected in § 999.302 by inserting the following text in revision marks:

> (a) Whether information is "personal information," as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that "identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household," in aggregate form, or in de-identified form with safeguards so that "they cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer." For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, ~~and could not reasonably link the~~

500 8th Street, NW
Washington, DC 20004
202.799.4000 Tel
202.799.5000 Fax

~~IP address with a particular consumer or household,~~ then the IP address would not be "personal information."

These revisions would accurately reflect the de-identification and aggregate data definitions and avoid needless confusion.

V. The Proposal in § 999.305(a)(3)(a) to require links to "at or before collection" notices "on all webpages where personal information is collected" Should be Revised

This subparagraph changes from an "or" to an "and" the requirements to provide a conspicuous link to the "at collection" notice "on the introductory page of the business's website *and* on all webpages where personal information is collected notice." This language is inconsistent with the statute, which requires notice "at *or* before collection", not "at *and* before."

It is true that, in a drafting error, the definition of "homepage" includes "any Internet web page where personal information is collected." § 1798.140(l). However, this is highly counter-intuitive and contradicts the statutory obligation to provide notice either at or before the point of collection. For this reason, as in the previous version of this proposed rule, the final rules should state that link may be placed on the home page *or* at each point of collection.

This change would both align with common understanding of the term "home page" and would be less likely to make consumers tune out by seeing the same link on every web page.

VI. The Clarifications to Service Provider Uses of Personal Data in § 999.314(c) Align the Provision with Statute, But the Reference to "Cleaning and Augmenting Data" Does Not and Is Unclear

The CCPA expressly allows service providers to use personal data "for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title." § 1798.140(v). This text fully supports the changes to § 999.314(c).

However, the reference to "cleaning" and augmenting other data is undefined and unclear and should be either removed or clarified by adding at the end "unless performed as part the services specified in the written contract". This clarification is important to avoid confusion as to whether service providers do not lose their status as service providers if they are engaged to and perform analytics functions while acting in a service provider role.

VII. The Requirement in § 999.305(a)(5) to Obtain Opt-in Consent for Specific Data Uses Is Inconsistent with the Statute.

500 8th Street, NW
Washington, DC 20004
202.799.4000 Tel
202.799.5000 Fax

We appreciate that the explicit consent requirement in this section has been cabined somewhat through a "materially different" standard. However, the requirement that an entity must "directly notify" and "obtain explicit consent" from consumers in order to use a consumer's personal information for a purpose materially different than what was disclosed in the notice at the time of collection goes beyond the scope of what the underlying statute provides. Civ. Code §1798.100 (b) clearly states that use of collected personal information for additional purposes should be subject to further *notice* requirements only.

The drafters of the CCPA required the further step of obtaining explicit consent from a consumer only for the sale of a minor consumer's personal information,[1] participation in an entity's financial incentive program,[2] and retention of a consumer's personal information for the purposes of peer-reviewed scientific, historical, or statistical research in the public interest.[3]

Requiring explicit consent beyond these well-defined and clearly cabined use cases in the statute is contrary to the text of the CCPA.

VIII. The New Requirement in § 999.323(d) Preventing Businesses from Charging Consumers for Identity Verification Should be Clarified.

The new requirement in § 999.323(d) that businesses not charge consumers for proper identity verification should be clarified to make clear that *authorized agents* can be charged for identity verification, including powers of attorney, which are specifically envisioned by § 999.326(b) and require notarization. Experience thus far with CCPA requests suggests that entities are building for-profit authorized agent businesses. They can afford identity verification. At the same time, there is risk that fraudsters may pose as authorized agents and obtain access to specific pieces of personal information or delete accounts. It makes sense as a matter of public policy to require that authorized agents verify the identity and legitimacy of their business, as well as their authority to act on behalf of the consumers they are purporting to represent. At least as to access to specific pieces of personal information and data deletion, § 999.323(d) should be clarified specifically to allow this in order to reduce potential risk to Californians' privacy.

The same risk applies to fraudsters who pose as a California consumer. In this context, the final rules should also clarify that while a business should not require that consumers pay for a new power of attorney, it may require consumers that already have a power of attorney submit it.

Respectfully submitted,

Alan F. Hoyt

[1] § 1798.120(d).
[2] § 1798.125(b)(3).
[3] § 1798.105(d)(6).

500 8th Street, NW
Washington, DC 20004
202.799.4000 Tel
202.799.5000 Fax

Jim Halpert, Counsel
State Privacy & Security Coalition

500 8th Street, NW
Washington, DC 20004
202.799.4000 Tel
202.799.5000 Fax