December 6, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring Street
Los Angeles, CA 90013
Via email: privacyregulations@doj.ca.gov
Re: Internet Association Comments on California Consumer Privacy Act of 2018 Proposed Regulations

To Whom It May Concern:

Internet Association ("IA") appreciates the opportunity to provide the Attorney General's Office ("AGO") feedback on the Text of Proposed Regulations for the California Consumer Privacy Act ("CCPA") Regulations ("Proposed Regulations"). IA is the only trade association that exclusively represents leading global internet companies on matters of public policy.[1] Our mission is to foster innovation, promote economic growth, and empower people through the free and open internet. We believe the internet creates unprecedented benefits for society, and as the voice of the world's leading internet companies, IA works to ensure legislators, consumers, and other stakeholders understand these benefits.

IA members are committed to providing consumers with strong privacy protections and control over personal information, as well as to compliance with applicable laws, and advocates for a modern privacy framework in the IA Privacy Principles.[2] Internet companies believe individuals should have the ability to access, correct, delete, and download data they provide to companies both online and offline. It is essential that the U.S. enact a comprehensive, federal privacy law that provides Americans consistent protections and controls regardless of where they live, work, or travel.

As expressed in IA's comments submitted to the Attorney General during the drafting period for these regulations,[3] IA hoped that the AGO would use the regulations as an opportunity to clarify the CCPA in ways that would promote strong consumer privacy protections and businesses' ability to comply with the statute's legal requirements. IA is concerned that the proposed regulations place confusing and unnecessary burdens on businesses without providing meaningful privacy protections for consumers. The Proposed Regulations require significant new actions that go beyond the Legislature's original intent for CCPA. It will result in a confusing barrage of notices and disclosures that frustrate consumers and fail to provide stronger protections. Modern privacy controls emphasize contextual cues to help consumers make real time decisions about how their information is used. The Proposed Regulations

[1] IA's full list of members is available at: https://internetassociation.org/our-members/.
[2] IA Privacy Principles for a Modern National Regulatory Framework, available at: https://internetassociation.org/files/ia_privacy-principles-for-a-modern-national-regulatory-framework_full-doc/ (last accessed November 25, 2019).
[3] IA Comments on CCPA Initial Rulemaking begin at p. 857 of the CCPA Public Comments available at: https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-public-comments.pdf (last accessed November 25, 2019).

represent a leap backwards with new disclosure and notice requirements that don't provide consumers strong protections or controls and harm businesses.

IA urges the AGO to use the remaining time available to amend the regulations in a manner consistent with the CCPA's provisions and that facilitates implementation and compliance with its terms.

Section I. General Comments

IA would like to share a few high level concerns that apply to the Proposed Regulations as a whole, before providing our comments on specific provisions:

1. **The Proposed Regulations introduce new requirements too close to the effective date of CCPA.**

The CCPA's provisions become operative on January 1, 2020 pursuant to Cal. Civil Code Section 1798.198(a). The Attorney General is able to bring enforcement actions beginning on July 1, 2020 (or sooner if the final regulations are published six months prior to July 1, 2020, which is also the date on which the regulations required by the CCPA are due to be final).[4] The AGO may bring enforcement actions for non-compliance with CCPA for actions going back to the January 1, 2020 effective date, regardless of whether the final regulations were available at the time the violation occurred. The comment period for the Proposed Regulations closes December 6, 2019. It is clear that final regulations will not be ready before the January 1, 2020 effective date of CCPA, and it seems unlikely that the final regulations will be ready much before the enforcement date of July 1, 2020.

Putting aside the wisdom of the implementation schedule in CCPA,[5] the reality is that businesses subject to CCPA began assessing compliance needs and developing the required new tools, such as the capability to opt-out of sale, months ago to work toward the January 1, 2020 effective date. Significant resources have already been put against understanding the legal requirements of the statute as they apply to a given business; hiring and training necessary staff across functional areas; and designing and coding a complex set of new capabilities. The implementation schedule in CCPA only makes sense to the extent that the AGO reads the requirements for regulations narrowly, as providing clarifications and detail consistent with the existing requirement as necessary to implement the requirements of the law.[6] Such an approach would also be most consistent with the rulemaking mandate in the

[4] Cal. Civ. Code § Section 1798.185(c). The August 2018 amendments (S.B. 1121) to CCPA revised the original time frame in the statute by giving the AGO more time to prepare the regulations, at the AGO's urging, thus creating a framework where the CCPA law would become operative before the AGO would be required to deliver final regulations.

[5] Though by comparison, it is notable that the EU General Data Protection Regulation ("GDPR"), which built on the requirements of its predecessor, the EU Data Protection Directive (adopted in 1995), allowed covered entities two years from publication of the final text of the Regulation to the effective date.

[6] This approach to drafting the implementing regulations for CCPA would also be most consistent with the expectations of the California Legislature which expected that the CCPA would set the deadlines and core provisions for compliance with CCPA. The

CCPA (as originally passed and as amended by A.B. 1355) which only allows "additional regulations as necessary to further the purposes of th[e] title"[7] and California law governing the rulemaking process.[8]

In the Proposed Regulations, the AG has taken a far broader approach than what is called for and creates new obligations beyond those contemplated in the text of the CCPA.[9] Even assuming that the AG has the appropriate legal authority to do so,[10] sound public policy dictates that the AG should not at this late date introduce new requirements that will be finalized *after* CCPA has already become operative on January 1, 2020. There is even the potential that certain CCPA regulations will not be finalized much before the date on which enforcement must begin, July 1, 2020.[11] Not only does this raise questions of fair warning and due process, but it also creates harms for consumers and businesses. For consumers, it makes understanding their rights and protections under CCPA a moving target and significantly harder to understand. For businesses, it adds uncertainty, increases legal costs, and punishes the responsible actors who began compliance efforts early by moving the goalposts, rendering prior work moot, and necessitating further investment. There is already a significant price tag for CCPA compliance efforts estimated at an initial cost of up to $55 billion, according to the AGO's Standardized Regulatory Impact Assessment ("SRIA"),[12] these regulations will be a cost-multiplier that makes the initial numbers seem reasonable by comparison.

IA Recommendation: The AGO should take a fair and reasonable approach to regulations by only adopting rules that are provided for in CCPA's rulemaking mandate, reasonably necessary, [13] and for which CCPA has already provided businesses with fair warning of the potential requirements in order to make the current implementation schedule for CCPA as beneficial to consumers as possible. IA provides detailed recommendations and proposed changes in *Section II: Specific Provision*s of these comments.

Senate Judiciary Bill Analysis stated, "[t]hese provisions provide clear guidance on the basics for ensuring compliance." Senate Judiciary Committee Bill Analysis, p. 19 (June 25, 2018). Available at: https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375 (last accessed November 19, 2019).

[7] Cal. Civ. Code § 1798.185(b)(2)(as amended by A.B. 1355).

[8] Rulemaking is governed by the California Administrative Procedure Act ("APA"), Government Code § 11340 *et seq*. Rulemaking must also comply with regulations adopted by the Office of Administrative Law ("OAL"), California Code of Regulations, Title 1, §§ 1-120.

[9] *See* Section II, *infra*, for a further discussion of the manner in which the AGO conflicts with and/or enlarges the requirements of the CPPA in the Proposed Regulations.

[10] *See* Section II, *infra*, for arguments that new requirements exceed the AGO's authority.

[11] IA notes that CCPA, Cal. Civ. Code § 1798.185(a), requires specific regulations be issued "on or before July 1, 2020," but that it also provides a more general rulemaking authorization that is not time bound in subsection (b). To the extent that the Proposed Regulations include provisions which exceed the rulemaking mandate in Section 1798.185(a), there does not appear to be any required due date for such regulatory provisions.

[12] Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, available at: http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

[13] Cal. Gov. Code § 11349(a).

2. **The Proposed Regulations exceed the legal authority of the AGO by altering, amending, or enlarging the CCPA, and failing to meet other requirements of California administrative procedure.**

As more fully detailed below in *Section II: Specific Provisions*, the AGO exceeds its mandate to draft regulations to implement, interpret, or make specific the requirements of the CCPA by including provisions that directly contradict the language of CCPA, introduce new requirements not encompassed within the scope of CCPA and for which there is no reasonable necessity, and/or fails to meet other requirements of California's statutes and regulations for administrative procedure.[14]

Background on California's Rules for Promulgating Regulations

For the benefit of members of the public who may review these comments, we offer the following basic background on the APA.[15] The California Government Code and its implementing regulations require that regulations adopted by agencies in the state meet procedural and substantive specifications. These specifications apply to the Proposed Regulations, the Initial Statement of Reasons ("ISOR"), and the SRIA. For example, the ISOR must explain how the Proposed Regulation is "reasonably necessary to carry out the purpose and address the problem for which it is proposed" and describe "reasonable alternatives to the regulation and the agency's reasons for rejecting those alternatives."[16] The required financial analysis is intended to inform the agency and the public about whether the Proposed Regulation "is an efficient and effective means of implementing the policy decisions enacted in statute …in the least burdensome manner."[17] The Office of Administrative Law ("OAL") is tasked with reviewing Proposed Regulations, prior to enactment, for compliance with procedural requirements and substantive requirements including: (1) Necessity; (2) Authority; (3) Clarity; (4) Consistency; (5) Reference; and (6) Nonduplication.[18]

Where the Proposed Regulations create new requirements, such as the requirement to treat a browser signal as a valid opt-out of sale,[19] the AGO fails to show sufficient authority or necessity to meet the requirements of California law. For example, with regard to browser signals the ISOR states,

[14] Cal. Gov. Code § 11340 *et seq*. California Code of Regulations, Title 1, §§ 1-120. Cal. Gov. Code § 11342.2 states, "Whenever by the express or implied terms of any statute a state agency has authority to adopt regulations to implement, interpret, make specific or otherwise carry out the provisions of the statute, no regulation adopted is valid or effective unless consistent and not in conflict with the statute and reasonably necessary to effectuate the purpose of the statute."
[15] Resources for additional background are available on the website of the Office of Administrative Law, available at: oal.ca.gov. The California Architects Board website hosts a report titled "How to Participate in the Rulemaking Process" which also offers background on state requirements for promulgating regulations, available at: https://www.cab.ca.gov/docs/misc/rulemaking_process.pdf (last accessed November 25, 2019).
[16] Cal. Gov. Code § 11346.2(b).
[17] Cal. Gov. Code§ 11346.3(e).
[18] Cal. Gov. Code § 11341.1(a).
[19] Proposed Regulation § 999.315.

> *This subdivision is intended to support innovation for privacy services that facilitate the exercise of consumer rights in furtherance of the purposes of the CCPA. This subdivision is necessary because, without it, businesses are likely to reject or ignore consumer tools.*[20]

This is ironic, because in the drafting of CPPA, reliance on existing consumer controls was rejected because of the view that having a uniform button or logo was too important to forgo. As a result the CCPA provides only one mechanism for consumer opt-out to sale - the "Do Not Sell My Personal Information" link on the business' internet homepage.[21] The authority provided by CCPA specifically tasked the AGO with creating rules for, "development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness."[22] Thus, it is clearly not within the rulemaking mandate from the Legislature. Nor is it consistent with the general rulemaking authorization in CCPA, allowing the AGO to "adopt additional regulations as necessary to further the purposes of this title."[23]

The record provided in the ISOR does not satisfy California law's definition of necessity in this context. California Government Code Section 11349(a) defines "necessity" as requiring that the rulemaking record,

> *demonstrates by substantial evidence the need for a regulation to effectuate the purpose of the statute ... that the regulation implements, interprets, or makes specific, taking into account the totality of the record. For purposes of this standard, evidence includes, but is not limited to, facts, studies, and expert opinion.*

Other than speculation in the ISOR that businesses "will likely ignore" other methods, no reasoning is offered for rejecting the approach adopted by the Legislature of having a uniform mechanism to signal to consumers how to opt-out from sale of their personal information. In addition, the ISOR provides no explanation for the adoption of browser signals and other technology as required by the APA, Cal. Gov. Code § 11346.2(b)(1), which states that,

> *Where the adoption or amendment of a regulation would mandate the use of specific technologies or equipment, a statement of the reasons why the agency believes these mandates or prescriptive standards are required.*

Furthermore, the AGO did not include this new requirement in the discussion of reasonable alternatives in the ISOR. California Government Code Section 11346.2(b)(4) mandates consideration of reasonable alternatives. In light of readily available alternatives including following the legislative mandate of CCPA, using the "designated methods" available for access and deletion requests, or allowing companies to rely on existing opt-out programs that achieve similar goals, as well as the likelihood that such alternatives would impose substantially less burden on business, including small business, it is not clear why the AGO

[20] ISOR, p. 24.
[21] Cal. Civ. Code § 1798.135(a)(1).
[22] Cal. Civ. Code § 1798.185(a)(4)(C).
[23] Cal. Civ. Code § 1798.185(b)(2).

thought this was an area where reasonable alternatives did need need to be given consideration and the rejection of less burdensome alternatives justified. IA also believes that, given the technical nature of the mandates around "browser plug-ins" and other user-enabled technologies, the AGO should be required to consider performance-based alternatives under the APA.[24]

This provision will be further discussed below in *Section II*'s analysis of Section 999.315, but it is offered here as *but one* example of how the AGO has exceeded its authority and the Proposed Regulations conflict with the requirements of California's APA.

IA Recommendation: The AGO should substantially revise the Proposed Regulations to bring them more clearly within the authority of the rulemaking powers granted by the CCPA, to ensure consistency with the clear terms of the CCPA, and to abide by the APA and its regulations. This should include another notice and comment period due to the substantial changes to the Proposed Regulations,[25] a new ISOR that appropriately considers reasonable alternatives,[26] and a new SRIA based on accurate understandings of the business impact of the regulations where they deviate from the requirements of the CCPA.[27]

3. The Proposed Regulations place unnecessary burdens on consumers and businesses.

The Proposed Regulations impose new requirements, beyond those required by the CCPA, which will impose unnecessary burdens on consumers and businesses. These unnecessary burdens undermine the statutory intent of the CCPA, by making it more difficult for consumers to understand and exercise rights over their data created by CCPA. The unnecessary burdens to business introduce new requirements without justification, require duplicative processes, enlarge obligations contained in the CCPA, make it more difficult for businesses to comply with the requirements of the CCPA, and expand the costs of compliance far beyond what was contemplated in the SRIA prepared in connection with this rulemaking process.

Numerous examples are explained below in *Section II*'s discussion of specific provisions of the Proposed Regulations, but one notable example that harms both consumers and businesses is the Proposed Regulation's provisions on notices to consumers. Transparency regarding

[24] Cal. Gov. Code § 11346.2(b)(4)(A).
[25] Cal. Gov. Code § 11346.8(c)(restricting the ability of an agency to adopt regulations with "nonsubstantial changes" from those noticed to the public. Title 1, Section 40 of the California Code of Regulations defines "nonsubstantial changes" to mean those that "clarify without materially altering the requirements, rights, responsibilities, conditions, or prescriptions contained in the original text." 1 C.C.R. § 40).
[26] Cal. Gov. Code § 11346.2(b)(4).
[27] Cal. Gov. Code §§ 11346.3 & 11346.36 set forth the requirements for the financial analysis for a Proposed Regulation. Due to the substantial deviations from CCPA and the baseline regulatory measures that purported to form the basis of the SRIA that was conducted, a new SRIA should be prepared that satisfies the requirement that "[t]he baseline for the regulatory analysis shall be the most cost-effective set of regulatory measures that are equally effective in achieving the purpose of the regulation in a manner that ensures full compliance with the authorizing statute or other law being implemented or made specific by the Proposed Regulation." Cal. Gov. Code § 11346.3(e).

business practices for handling personal information is widely regarded as a core element of a strong privacy regulatory regime and is a privacy principle that IA member companies support.[28] California has been a leader in the U.S. in adopting transparency requirements for personal information. However, privacy regulators and privacy researchers across the globe have also noted that *more* information is not necessarily the hallmark of effective transparency, rather that effective transparency requires the communication of the most important information to inform consumer choices. The Proposed Regulations introduce numerous new required disclosures for various notices and for privacy policies that exceed the requirements of CCPA and add significantly more detail and complexity to such disclosures. While the Proposed Regulations also talk of notices needing to be in "plain language" and easily understood by consumers, any notice comprised of all the required elements in the regulations will span innumerable small screens (like those on a mobile phone) and is unlikely to attract the full attention, if any, of consumers. This conflicts with the AGO's performance-based standards for privacy policies articulated in the regulations and with weight of concerns expressed by regulators and other privacy experts.[29] In fact, it arguably fails to understand that the concept of "plain language," as used in the studies and reports the AGO cites, means more than the selection of words that are understandable to the average consumer, it means—

> *A communication is in plain language if its wording, structure, and design are so clear that the intended readers can easily find what they need, understand what they find, and use that information.*[30]

IA Recommendation: The AGO should substantially revise the requirements of the Proposed Regulations to remove unnecessary burdens on business and to ensure that consumers benefit from clear, meaningful disclosures of privacy practices and methods for exercising their data rights, such that consumer can easily find the information they need and are able to use such information, as further explained in *Section II*.

Section II. Specific Provisions of Proposed Regulations

§ 999.301 Definitions

[28] *See* IA Privacy Principles, fn. 2, *supra*.
[29] *See, e.g.*, Center for Plain Language, *Privacy-policy Analysis* (2015), p. 1 (noting that a privacy policy that no one reads provides no protections), available at: https://centerforplainlanguage.org/wp-content/uploads/2016/11/TIME-privacy-policy-analysis-report.pdf (last accessed December 4, 2019); Norton, *The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Mode*l, 27 Fordham Intell. Prop. Media & Ent. L.J. 181 (2016), pp. 188-89 (discussing the difficulty of being concise in privacy policies and how long it would take a consumer to read all relevant privacy notices); Schaub, et al., *A Design Space for Effective Privacy Notices*, Symposium on Usable Privacy and Security (SOUPS) 2015 at Ottawa, Canada, p. 2 (July 22-24, 2015) (explaining that requirements regulatory compliance impact the length and complexity of notices stating "privacy notices often take the shape of long privacy policies or terms of service that are necessarily complex because the respective laws, regulations, and business practices are complex" and that privacy policy typically read like contracts because regulators seek to enforce them like contracts), available at: https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf; See also, European Union's Article 29 Working Party, Guidance on Transparency, para. 4, "The concept of transparency in the GDPR is user-centric rather than legalistic …[T]he quality, accessibility and comprehensibility of the information is as important as the actual content of the transparency information, which must be provided to data subjects" "succinctly in order to avoid information fatigue."
[30] Center for Plain Language, Privacy-policy Analysis, p. 1.

- **(a) "Affirmative Authorization"** requires that consumers undergo a two-step process to indicate and then confirm their request to opt-in to sale. Elsewhere in the Proposed Regulations, a two-step process is outlined for the exercise of additional consumer rights, such as the right to delete.[31] This two-step process introduces unnecessary friction to consumers, as well as potential risks. For example, a consumer may believe that after completing step one of the process that they have successfully performed the task and leave the process. This will result in the consumer's intent going unfulfilled without their knowledge, and create a potential limbo state for the business which may be unsure how to treat a consumer who has initiated but not completed a process. It is important that consumers understand the significance of the action they intend to undertake, which is why CCPA requires clear consumer notices and the Proposed Regulations define "affirmative authorization" as "an action that demonstrates the intentional decision by the consumer." This performance-based standard is preferable to a strict technical mandate to use two-steps. A business should not be able to rely on satisfying a technical requirement to have two steps, rather than satisfying an obligation to design a process that is clear to consumers and ensures they are intentionally exercising their rights. In addition, more "clicks" can be obstacles to the exercise of consumer rights and has the potential to numb consumers to the processes required to accomplish tasks associated with exercising their privacy rights.[32] To avoid these results, the Proposed Regulations should establish a definition of "affirmative authorization" that is not dependent on a two-step process and then use the definition where appropriate to describe the process for a consumer to exercise a right regarding their personal information, rather than prescribing a specific two-step process in each regulatory provision addressing methods for exercise of consumer rights.

  IA Recommendation: Revise the definition of "affirmative authorization" to read, "means an action that demonstrates the intentional decision by the consumer to exercise a consumer right provided by the CCPA. ~~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 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 two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.~~" Additionally, Sections 999.316(a), 999.312(d), and 999.313(d)(7) should be revised to require "affirmative authorization" rather than a "two-step process."

- **(g) "Financial Incentive"** please see discussion of this definition and IA's recommendations for Sections 999.307 and 999.337, *infra*.

[31] *See*, § 999.312(d).
[32] *See, e.g.*, Schaub, A Design Space for Effective Privacy Notices (discussing risks of notice fatigue and habituitzation in response to consumer notices and choices and alternatives for increasing consumer engagement in making choices).

- **(h) "Household"** as defined, whether alone or in combination with Section 999.318, does not resolve concerns about risks to the physical safety of consumers that may result from allowing individual members of a household to obtain data that pertains to the entire household, as is discussed in detail, *infra,* in connection with Section 999.318.
- **(j), (p), and (q) "Notice of right to opt-out"; "Request to opt-out"; "Request to opt-in"** are defined in the Proposed Regulations as abbreviated terms for the longer statutory terms of "right to opt-out of sale"; "request to opt-out of sale;" and "request to opt-in to financial incentive." While IA appreciates that adopting shorthand for these lengthy phrases is useful, we are also concerned that defaulting to these more general monikers may result in consumer confusion. First, CCPA uses the term "opt-in" in two different contexts — sales of personal information and financial incentive programs — but the definition for "request to opt-in" refers only to the sale of personal information. Presumably, a request to opt-in to a financial incentive would need to be referenced by its full description. However, consumers may be easily confused and not aware at any given time that there are different types of "opt-ins" implicated by CCPA. Likewise, requests and notices related to opt-out could apply across a range of scenarios in CCPA. In addition to the opt-out from sale referenced in the regulatory definition, "opt-out" could also apply to a withdrawal of consent following an opt-in to a financial incentive or opt-in to sale of personal information by a parent of a consumer under the age of 13. In addition, confusion over these terms may also result from the use of the terms "opt-in" and "opt-out" in other privacy laws[33] or privacy controls[34] that may be applicable to a consumer. Given the varying definitions and scope of the potential range of "opt-opt" and "opt-in" choices a consumer will be presented with in the course of managing the privacy of his/her personal information, the AGO should be more specific in adopting any shorthand for the rights provided by the CCPA.

  IA Recommendation: Revise definitions to adopt more specific references to each type of opt-out or opt-in, such as "Sale Opt-Out/In" and "Incentive Opt-Out/In."

- **(l) "Price or service difference"** please see discussion of this definition and IA's recommendation for Section 999.337.
- **(s) "Typical Consumer"** is defined as "mean[ing] a natural person residing in the United States." It is not clear from this definition how defining the term by reference to a single person leads to an understanding of what is "typical." The Merriam-Webster Dictionary defines "typical" as "combining or exhibiting the essential characteristics of

[33] *See, e.g.*, Privacy of Consumer Financial Information Rule, 16 C.F.R. Part 313, Subpart A (Privacy and Opt-Out Notice)(May 24, 2000); *See also*, HHS.gov FAQ, *Can a covered entity use existing aspects of the HIPAA Privacy Rule to give individuals the right to Opt-In or Opt-Out of electronic health information exchange?*, available at: https://www.hhs.gov/hipaa/for-professionals/faq/555/can-a-covered-entity-use-hipaa-to-give-individuals-opt-in-or-opt-out-rights/index.html (discussing opt-in and opt-out options under the HIPPA Statute and Rule)(last accessed November 19, 2019).
[34] *See*, *e.g.*, the Digital Advertising Alliance's "Your AdChoices" Opt-out), available at: https://youradchoices.com/choices-faq (last accessed November 19, 2019).

a group (ex: typical suburban houses)."[35] This definition is further confused by referencing a resident of the United States, when the CCPA defines "consumer" to mean a resident of California.[36] The ISOR seems to suggest that this definition is necessary for the Proposed Regulations Section 999.337(b) for purposes of determining the value of consumer data.[37]

IA Recommendation: Incorporate a definition for "typical" drawn from standard dictionary definitions, such as "means the most usual characteristics of a natural person,"[38] and replace the term "average consumer" (an undefined term used within the Proposed Regulations) with the defined term "typical consumer." Or make "average consumer" the defined term, adopting a dictionary definition such "as a level typical of a group, class, or series,"[39] and replace "typical consumer" throughout the Proposed Regulations. Remove reference to residency.

- **Add new subdivision (v) "Signed attestation"** should be defined to specifically allow an electronically signed attestation to be acceptable.

IA Recommendation: Add new subdivision (v) to read, "Signed attestation" means an attestation that has been signed in writing or electronically.

999.305 Notice at collection

- **Proposed regulations contradict and enlarge CCPA provisions regarding new purposes for processing personal information.** Proposed Regulation Section 999.305(a)(3) introduces a new requirement for a business to obtain "explicit consent" from a consumer before processing personal information for a new purpose beyond those disclosed in prior consumer notices. This language contradicts the clear language of CCPA which requires notice to consumers of new purposes for processing personal information in Section 1798.100(b). Notably, the CCPA does not contain any consent requirements related to collection or processing of personal information, absent the singular example where the legal guardian of a minor must "opt-in" to the sale of personal information related to the child, as provided in Section 1798.120(c).

The sole justification cited for the new explicit consent requirement states,

> *The purpose of these subdivisions is to implement Civil Code Section 1798.100, subdivision (b). The subdivisions make clear that a business cannot change their practices after giving the notice at collection because the consumer could have*

[35] Available at: https://www.merriam-webster.com/dictionary/typical (last accessed November 19, 2019).
[36] Cal. Civ. Code § 1798.140(g).
[37] ISOR, p. 7.
[38] Drawn from Collins Dictionary definition of "typical," available at: https://www.collinsdictionary.com/us/dictionary/english/typical (last accessed November 19. 2019).
[39] Merriam-Webster Dictionary, available at: https://www.merriam-webster.com/dictionary/average (last accessed November 21, 2019).

> *reasonably relied on the information provided in the notice at collection when interacting with the business.*[40]

This explanation fails to explain why the AGO applied different treatment to changes in the categories of information collected and changes for purposes of collection in the Proposed Regulations when CCPA sets the same requirement for both changes - new notice to the consumer. The Proposed Regulations require a new notice for the collection of additional categories of information, but require explicit consent for any new purposes of processing.[41] The AGO has not provided an explanation of why explicit consent for new purposes of processing is required, when notice without explicit consent is sufficient for the original purposes of processing under the CCPA. Regardless of the objective, the AGO has not established that this significant new burden on business is justified, or even authorized.

IA Recommendation: This unsupported and burdensome requirement clearly exceeds the AGO's rulemaking mandate and authority and should be struck from the Proposed Regulations. Specifically, IA recommends that the second sentence of 999.305(a)(3) be revised to, "If the business intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use ~~and obtain explicit consent from the consumer to use it for this new purpose~~.

- **Confusing language in the Proposed Regulations seem to require notice *before* collection of any personal information, contradicting the clear language of the CCPA.** Section 1798.100(b) says that notice to consumers shall be provided "at or before the point of collection." Section 999.305(a)(2)(e) of the Proposed Regulations state that notice must, "be visible or accessible where a consumer will see it *before* any personal information is collected." (*emphasis added*). However, Section 999.305(a)(1) states "at or before." This could potentially be an oversight given that the Proposed Regulations and the ISOR also uses the "at or before" formulation in other areas as well.[42] The ISOR, however, explains that,

> *[t]he subdivision makes clear that businesses that collect personal information without first giving notice to the consumer are in violation of Civil Code Section 1798.100 and these corresponding regulations. It clearly prohibits the surreptitious collection of personal information.*[43]

Given the operation of the internet, there are instances where it is impossible to provide notice before collection of personal information, particularly as that term is defined in

[40] ISOR, p. 8.
[41] *Id.*
[42] *See*, §§ 999.305(a)(1) & (a)(5), 999.301(i)(specifically defining "notice of collection" to be notice "at or before" time of collection); ISOR, pp. 5, 8-9, 43, 54.
[43] ISOR, p. 9.

the CCPA Section 1798.140(o)(1)(A) including "internet protocol address" and unique identifiers.[44] Even robust privacy regulations, such as the European Union's General Data Protection Regulation ("GDPR"), provides:

> *As regards timing of the provision of this information, providing it in a timely manner is a vital element of the transparency obligation and the obligation to process data fairly. Where Article 13 applies, under Article 13.1 the information must be provided "at the time when personal data are obtained."*[45]

The difficulty entities subject to the GDPR have faced trying to comply with the requirements for data collection via cookies on websites demonstrates the importance of creating clear rules that create privacy benefits for consumers. Basic internet functions require that certain technical data is transferred from a client to server in order for a user to be able to view a website and some of this data in encompassed within CCPA's definition of personal information.[46]

IA Recommendation: Amend Proposed Regulations to ensure consistent use of "at or before" language, including inserting "at or" in front of "before" in Section 999.305(a)(2)(e) of the Proposed Regulations so that it states that, "notice must be visible or accessible where a consumer will see it at or before any personal information is collected."

- **Section 999.305 should clarify that a "notice of collection" can be satisfied by providing a link to the appropriate Section of a business' privacy policy.** Section 999.305 requires a separate "notice of collection" in addition to the information provided in a privacy policy. The Notice can take the form of either a link to a specific section of the policy, or a discrete notice. Some legal practitioners are interpreting the Proposed Regulations to require a second notice. IA believes this is not in consumers' best interest because it only introduces more clutter and an associated increased likelihood of confusion. The AGO should make clear that the notice of collection requirement can be satisfied via a link to the corresponding section of the privacy policy, to avoid any further confusion.

999.306 Notice of right to opt-out of sale

- **Subdivision 999.306(d)(2) adds a new requirement to treat consumers as having opted-out of sale, if their personal information is collected during a period when a**

[44] *See*, Lea Kessner, Building With Respect, CCPA Bugs and Engineering Commentary on the CCCPA, available at: https://buildwithrespect.com/2019/11/16/ccpa-bugs-and-engineering-commentary-on-the-california-consumer-privacy-act-regs/amp/?__twitter_impression=true (last accessed November 19, 2019); *See also*, https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information/#when-notification-is-to-occur (last accessed November 15, 2019).
[45] Article 29 Working Party Guidance on Transparency Principles of GDPR, para. 27, available at: https://iapp.org/media/pdf/resource_center/20180413_Article29WPTransparencyGuidelinespdf.pdf
[46] https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/How_the_Web_works

business states that it does not sell data (and/or does not provide an opt-out from sale link) is unnecessary due to existing requirements for notifying consumers of changes in business practices for personal information, and creates confusion. As discussed, *supra*, with regard to Section 999.305(a)(3), CCPA and the Proposed Regulations adequately address what notice should be provided to a consumer when a business collects new information or changes the purposes of processing information. The notice requirement under Section 999.305(a)(3) would be triggered by a change to purposes of processing such as beginning to sell personal information that has not previously been sold. This notice would, like the notice at the point of collection, allow consumers the opportunity to opt-out. This meets the stated purpose for subdivision (d) in the AGO's ISOR, to avoid "selling a consumer's personal information without giving them notice and the opportunity opt-out."[47] Thus the requirement in Section 999.306(d)(2) to treat all consumers whose information was collected while a business was not selling consumer information as having exercised the right to opt-out is unnecessary for the protection of consumers.[48]

Treating consumers who provide personal information as having opt-out of sale without using a trackable opt-out measure is a confusing and difficult to implement. CCPA Section 1798.120(a) requires that a business who has received a consumer opt-out of sale to wait 12 months before asking the consumer for authorization to sell their personal data.[49] The interaction of this provision with Proposed Regulation Section 999.306(d)(2) creates confusion about when the 12-month wait period would begin. Specifically whether it would it be the first date of collection or the most recent date of collection. It is also not clear whether it is consistent with the intent of the wait period in CCPA, where it ensures that a consumer who has clearly indicated a desire to opt-out from sale will not be regularly asked by a business to reconsider the opt-out. If the consumer has not been presented with a decision of whether or not opt-out previously, there is no benefit to artificially postponing the ability of a business to notify the consumer of the change in policy and the newly available opt-out mechanism.[50] If in response to notice of new purposes for personal information a consumer chooses to exercise the right to opt-out of sale, the 12 month period will begin from that date and protect the consumer from repeated requests to reverse that decision.

[47] ISOR, p. 11.
[48] IA also notes that the change in whether a business "sells" personal information could result from a change in the law, rather than a change in business practices. This is not hypothetical— the definition of "sale" proposed by the new CCPA initiative expected for the November 2020 ballot would likely require many businesses who do not sell personal information under CCPA 2018 to add an opt-out of sale mechanism. It is also unclear how an "implied" opt-out would be computed for purposes of the 12-month wait period. *See* "A Letter from Alistair MacTaggart," posted September 25, 2019 to Californians for Consumer Privacy's website linking to initial proposed text of ballot initiative to amend CCPA 2018, available at: https://www.caprivacy.org/post/a-letter-from-alastair-mactaggart-board-chair-and-founder-of-californians-for-consumer-privacy (last accessed November 25, 2019).
[49] This is implemented in Proposed Regulation Section 999.315.
[50] Clearly, once a consumer opts-out, whether in response to notice at the original point of collection or subsequent notice of a change in purposes of processing to include sale, the 12 month wait period will apply.

- **Subdivision(d)(2) also purports to apply to future activities of a business in a way that appears to restrict the ability of businesses to change their practices.** However, the CCPA does not govern a business's future potential to sell personal information, but instead governs the practices of businesses that sell personal information at the time of processing the personal information. The proposed regulation references not only businesses that actually sell personal information but that may in the future, which exceeds the current statutory language.

  IA Recommendation: Strike language in Section 999.306(d)(2) stating that consumers are to be treated as having opted out of sale if they provide personal information to a business that, at that time, states that they do not sell personal information, as follows:
  (d) A business is exempt from providing a notice of right to opt-out if~~:~~
  ~~(1) I~~it does not~~, and will not,~~ sell personal information collected during the time period during which the notice of right to opt-out is not posted.~~; and~~
  ~~(2) It states in its privacy policy that that it does not and will not sell personal information.A consumer whose personal information is collected while a notice of right to opt-out notice is not posted shall be deemed to have validly submitted a request to opt-out.~~

999.307 Notice of financial incentive

- **The manner in which this Section implements the requirements of CCPA's "non-discrimination" provision, Section 1798.125, is unclear as to its intent.** Clarity is needed as to whether Section 999.307 is intended to only apply: (1) where consumers receive a financial incentive or price or service difference in connection with the exercise of their rights of access, deletion, and opt-out of sale under CCPA; or (2) to any financial incentive or price or service difference offered by businesses in connection with simply the collection of personal information. The Proposed Regulations define a "financial incentive" by reference to these activities, stating in the ISOR that it,

  > *means a program, benefit, or other offering, including payments to consumers as compensation, for the disclosure, deletion, or sale of personal information. Civil Code Section 1798.185, subdivision (a)(6), directs the Attorney General to establish rules and guidelines regarding financial incentive offerings, but does not define the term. The purpose of defining this term is to provide clarity to the regulations and avoid any confusion that may result from different understandings of the term.*[51]

  This clearly ties the term "financial incentive" to the concept of discrimination against a consumer for exercising rights provided by the CCPA. This is consistent with the CCPA,

[51] ISOR, p. 5. "Financial incentive" is defined in Section 999.301(g). IA notes that the proposed definition includes the term "disclosure" which is not a defined term in CCPA or the Proposed Regulations and it is unclear to which consumer right created by the CCPA it correlates or what activities it would be intended to cover.

which bars "discriminat[ion] against a consumer because the consumer exercised any of the consumer rights under this title,"[52] by taking actions such as "denying goods or services," "charging different prices or rates for goods or services," "providing a different level of quality of goods or services," or "suggesting that the consumer will receive a different price or rate."[53] The CCPA does provide for exemptions from the ban on these types of price or service differentials in Section 1798.125(a)(1) in subparagraph (a)(2) where the differential is "reasonably related to the value" of the consumer's data. Section 1798.125(b) regulates "financial incentives" by mandating notice and consumer opt-in. The ISOR goes on to connect "financial incentives" to the exercise of consumer rights over their personal information by stating,

> *The definition is intended to help businesses implement the regulations by giving a name to the notice required by Civil Code Section 1798.125, subdivision (b)(2), regarding the prohibition on discrimination based on a consumer's exercise of rights under the CCPA.*[54]

The ISOR also explains that a financial incentive or price or service difference is "discriminatory" if it treats consumers differently because they "exercised a right conferred by the CCPA or these regulations."[55] For the sake of clarity, the consumer rights granted by CCPA, and for which any discrimination is barred, are understood to be the consumer right to know (encompassing both transparency regarding business practices and access to the consumer's specific pieces of personal information), right to delete, and right to opt-out of sale.[56] If a consumer has not exercised one of these rights, then a business, by definition, could not engage in prohibited discrimination under CCPA.

However, in other areas of the Proposed Regulations and ISOR the text is less clear that financial incentives are differences in terms resulting from the exercise of consumer rights under the CCPA, or even in regard to the processing of personal information. For example, the ISOR states without any mention of discrimination or retaliation,

> *that "price or service difference" means any difference in the price or rate charged for any goods or services to any consumer, including through the use of discounts, financial payments, or other benefits or penalties; or any difference in*

[52] Cal. Civ. Code § 1798.125(a)(1).
[53] *Id.*
[54] ISOR, p. 5.; *see also* ISOR, p. 36.
[55] *Id.*, p. 36. IA notes that CCPA does not reference any new rights for consumers that may be created by regulation and that would provide a grounds for arguing a business has engaged in unlawful discrimination under Section 1798.125. The inclusion of "these regulations" in the Proposed Regulations Section 999.336(a), and in the explanatory text of the ISOR, likely exceeds the authority of the AGO.
[56] *See*, Proposed Regulation § 999.308(b) which lists these as the rights which must be disclosed in a privacy policy, in addition to the right not to be discriminated against for exercising these three rights.

> *the level or quality of any goods or services offered to any consumer, including denial of goods or services to the consumer.*[57]

This language is broad and in no way tied to discrimination against consumers who exercise rights under the CCPA. In subdivision(b) of Section 999.307, the Proposed Regulations add new requirements for offering financial incentives which speak to service and price differences without any connection to exercise of consumer rights under CCPA. The ISOR however makes the conclusory statement that, these new requirements are "essential to further the CCPA's purpose of prohibiting discrimination based on a consumer's exercise of privacy rights." This is clearly overreaching to the extent it purports to regulate a business that offers differing levels of service or pricing based on factors *other than* the exercise of consumer rights under the CCPA. Much like a restaurant charges different prices to consumers depending on whether they order bread and water versus lobster and Champagne, there are any number of business or market factors which may justify price or quality differentials. In some cases these may relate to processing of personal information, but the fact that personal information is processed does not mean that the consumer will *by necessity* face discrimination if they exercise one of the three consumer rights provided by the CCPA.

Thus, the Proposed Regulations and any explanatory text should be clear that simply offering differing services or prices is not within the scope of regulated "financial incentives" under CCPA Section 1798.125(b), *unless* such differences are triggered by a consumer's exercise of the rights provided under the CCPA. Non-discriminatory service and price differences fall outside of the notice and opt-in requirements that apply to financial incentive programs regulated by CCPA specifically because they potentially retaliate against consumers exercising their data rights.

IA Recommendation: The Proposed Regulations should be clarified to ensure that regulated "financial incentives" and other price or service differences are clearly connected to the exercise of consumer rights under CCPA, by revising subdivision (a)(1) to read, "The purpose of the notice of financial incentive is to explain to the consumer each financial incentive or price or service difference a business may offer in exchange for ~~the retention or sale of~~ a consumer~~'s personal information~~ refraining from exercising a right created by the CCPA so that the consumer may make an informed decision on whether to participate."

- **Required notices of financial incentives, like other privacy disclosure requirements discussed in these comments, are overly-detailed and may be ineffective as a result of being ignored by consumers.**[58] Deleting certain Sections requiring detailed information would make it more likely that companies can succinctly describe financial

[57] *Id.*, p. 5.
[58] *See*, fn. 29, *supra*.

incentives and differences in price and service in their online privacy notices, which is permitted under §999.307 (a)(3). Detailed recommendations for information that may be duplicative and unnecessary, include:

- The portion of subdivision (b)(2) requiring businesses to point out specific categories of personal information that are implicated, as requiring such a specific disclosure could make it much more difficult for companies to direct customers to online privacy notices.
- Subdivision (b)(5) requires inclusion of data that is likely to be proprietary information of companies.

IA Recommendation:

- Revise subdivision (b)(2) as follows: A description of the material terms of the financial incentive or price of service difference~~, including the categories of personal information that are implicated by the financial incentive or price or service difference~~;
- Revise subdivision (b)(5) by striking "b. A description of the method the business used to calculate the value of the consumer's data" in its entirety.[59]

- **Subdivision (b)(5) creates a new obligation, not present in CCPA, to provide consumers with a specific monetary value of their data despite a lack of consensus on reliable methodology for determining such value and dubious value to consumers in using such unreliable figures as a basis for making privacy choices.** See, *infra*, IA's comments on the requirement to provide an estimate of the value of a consumer's data (§ 999.336) and how that value is calculated (§ 999.337).

999.308 Privacy policy

- **The Proposed Regulations expand and enlarge the required notices and privacy policies under the CCPA, creating significant challenges for consumers to parse the notices for the information needed to make informed choices.**[60] The additional requirements make meeting the "performance-based standard" set out in the Proposed Regulations more difficult for businesses. The proposed Section 999.308 expands and enlarges the requirements of the CCPA in two ways: 1) it adds new and duplicative disclosures that must be provided in "notices" and in "privacy policies"; and 2) it creates, for the first time, a requirement that "information helpful for consumers," but not required by the CCPA, be included in privacy policies. These new requirements cause problems for consumers and businesses alike, including:

    1. **The sheer volume of information required to be provided to consumers makes it nearly impossible for businesses to meet the performance-based**

[59] *See also*, IA comments, *infra*, of Sections 999.336-37 as pertains to Section 999.307(b)(5)(a) which IA also believes should be substantially revised, however for different reasons.
[60] *See also*, IA's comments, *supra*, in Section I.3 on this topic generally.

approach in subdivision (a)(2). The performance-based approach in subdivision (a)(2) requires a privacy policy to be "easy to read and understandable to an average consumer" by complying with the following requirements:

a. Use plain, straightforward language and avoid technical or legal jargon.
b. Use a format that makes the policy readable, including on smaller screens, if applicable.
c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers.
d. Be accessible to consumers with disabilities. At a minimum, provide information on how a consumer with a disability may access the policy in an alternative format.
e. Be available in an additional format that allows a consumer to print it out as a separate document.

Subdivision (b) requires a privacy policy contain the following information:

(1) Right to Know About Personal Information Collected, Disclosed, or Sold

a. Explain that a consumer has the right to request that the business disclose what personal information it collects, uses, discloses, and sells.
b. Provide instructions for submitting a verifiable consumer request to know and provide links to an online request form or portal for making the request, if offered by the business.
c. Describe the process the business will use to verify the consumer request, including any information the consumer must provide.
d. Collection of Personal Information

1. List the categories of consumers' personal information the business has collected about consumers in the preceding 12 months. The notice shall be written in a manner that provides consumers a meaningful understanding of the information being collected.
2. For each category of personal information collected, provide the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties with whom the business shares personal information. The notice shall be written in a manner that provides consumers a meaningful understanding of the categories listed.

e. Disclosure or Sale of Personal Information

1. State whether or not the business has disclosed or sold any personal information to third parties for a business or commercial purpose in the preceding 12 months.

2. List the categories of personal information, if any, that it disclosed or sold to third parties for a business or commercial purpose in the preceding 12 months.
3. State whether or not the business sells the personal information of minors under 16 years of age without affirmative authorization.

(2) Right to Request Deletion of Personal Information
a. Explain that the consumer has a right to request the deletion of their personal information collected or maintained by the business.
b. Provide instructions for submitting a verifiable consumer request to delete and provide links to an online request form or portal for making the request, if offered by the business.
c. Describe the process the business will use to verify the consumer request,including any information the consumer must provide.

(3) Right to Opt-Out of the Sale of Personal Information
a. Explain that the consumer has a right to opt-out of the sale of their personal information by a business.
b. Include the contents of the notice of right to opt-out or a link to it in accordance with Section 999.306.

(4) Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights
a. Explain that the consumer has a right not to receive discriminatory treatment by the business for the exercise of the privacy rights conferred by the CCPA.

(5) Authorized Agent
a. Explain how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf.

(6) Contact for More Information: Provide consumers with a contact for questions or concerns about the business's privacy policies and practices using a method reflecting the manner in which the business primarily interacts with the consumer.

(7) Date the privacy policy was last updated.

(8) If subject to the requirements set forth Section 999.317(g), the information compiled in Section 999.317(g)(1) or a link to it.

It is a monumental task to make this vast amount of information easily understood, in plain language, and user-friendly across devices (including the small screens of the mobile environment). The ISOR discusses privacy policy design and performance standards to ensure that consumers understand policies. This appears in tension with the substantial amount of information required to be contained in policies which will make them long, time-consuming to review, and unwieldy for different types of platforms where they will be required to be made available.

2. **There should be a difference between a privacy policy and a privacy resource center.** Proposed Regulation Section 999.308(b)(1)(c) requires that the process for account verification, including information needed for verification, be included in the privacy policy. Including process descriptions in the privacy policy will have adverse consequences because of the importance of avoiding unnecessary changes to the privacy policy. Descriptions of processes are frequently subject to change, particularly in the light of the CCPA implementation schedule. Because the operative date of the statute is January 1, 2020 and the regulations governing the verification process will not be finalized until some time after, it is likely that most businesses will have to make changes in the processes that will be rolled out for January 1 after the regulations are final. In addition, CCPA requires that companies review and update their privacy policies at least every 12 months.[61] Furthermore, CCPA and the Proposed Regulations also require that privacy policies be available in appropriate languages and available to those with disabilities. Any policy changes thus need to be translated and appropriate updates made to ensure accessibility.

   Updating privacy policies is a time-consuming process that cannot happen frequently or quickly. If a company needs to change its verification practice because it has learned about security vulnerability that impacts its current practice, it will need to act quickly to change the verification process description. For this reason, this type of process-oriented information is more appropriately *linked to* from the privacy policy, but considered outside the formal policy to allow changes according to business needs, to address emerging security threats, to enhance consumer experience, or to comply with changed legal requirements. Similar arguments apply to the requirement to place metrics in the privacy policy in subdivision (b)(8).

   In addition, any descriptions of information used for verification of consumer account ownership and authentication processes should not disclose details that would allow a bad actor to obtain advance notice of how they might impersonate the account holder. Failed attempts to authenticate are useful indicators of potential fraud and would justify heightened scrutiny by a business. This would also enable businesses to maintain a sufficient level of flexibility so that they can accommodate consumers who may have forgotten or changed account information. For example, consumers may no longer have access to a specific email account or phone number that they used at the time of account registration and thus may need the business to work with them to find alternate verification options.

[61] Cal. Civ. Code § 1798.130(a)(5).

CCPA does not require that this information to be in the privacy policy, nor is it information that is mandated to be disclosed pursuant to CCPA's notice provisions. In fact, the most relevant language in CCPA regarding this proposed language is contained the grant of rulemaking authority to the Attorney General, Section 1798.185(a)(7) which provides authority for the AGO to establish rules to "facilitate" access "taking into account available technology, security concerns."

There is no enforcement benefit to requiring a business to detail this process information in the privacy policy as required by the Proposed Regulation since a failure to comply with consumer requests is a statutory or regulatory violation and can be enforced as such regardless of the language of a specific company privacy policy. Consumers benefit most from being able to find such information easily to facilitate the exercise of their rights under the CCPA.

IA Recommendations:

- Revise (b)(1)(b), (b)(2)(b) by striking it in its entirety or revise to reference providing only a link to instructions or webforms for submitting requests.
- Revise (b)(1)(c), (b)(2)(c) to state: ~~Describe~~ Link to the process the business will use to verify the consumer request, ~~including any~~ which shall include a general description of the information the consumer ~~must~~ may be asked to provide.
- Revise (b)(8) by striking it in its entirety. *See also* discussion of Section 999.317(g), *infra*.

3. **Attempts to consolidate disclosure requirements, which are spread out in the CCPA, create confusing new obligations which will inundated consumers with repetitive information not required by law.** The Proposed Regulations require extensive information to be provided in the "notices" (e.g. at collection, right to know, delete, financial incentives, etc.) and privacy policy which goes beyond the information required by CCPA and will result in redundant disclosures to consumers making notices and Privacy Policies even more difficult for consumers to parse for the information that need to make informed decisions about the privacy of their personal information. For example, subdivision (b)(1)(d)(2) requires that a privacy policy disclose *for each* category of personal information, the categories of sources, business or commercial purposes for collection, and the categories of third parties with whom information is shared. This may seem similar to the requirements of Section 1798.130(a)(5) of CCPA which specifies information to be disclosed in privacy policies, but there are notable differences. Section 1798.130(a)(5) requires: 1) a

description of consumer rights provided by the CCPA; 2) a list of categories of personal information collected in the preceding 12 months; 3) categories of personal information sold in the preceding 12 months (or a statement that personal information has not been sold); and 4) a list of categories of personal information disclosed for business purposes in the preceding 12 months. Providing each of these individual lists required by the CCPA is very different than providing listing of sources, purposes of processing, and categories of recipients for each category of personal information collected (with is to be done in a manner consistent with the categories of information in the CCPA's definition of personal information which includes 11 broad categories of information and numerous more detailed categories).[62] For some businesses, these categories could be the same for every category of personal information and after wading through pages of disclosures consumers will have obtained little additional helpful information. For consumers who want more nuanced information, it is available from other sources such as the "Notice at Collection" which describes the purposes of processing categories of personal information or by submitting a consumer request to obtain, for example, detailed information on the categories of personal information sold and the types of entities to whom it was sold.[63] Essentially, the proposed regulations convert information that CCPA mandated to be available only in response to verifiable consumer requests into information disclosed generally in privacy policies.

These types of additional disclosures are inconsistent with the text of the CCPA and not justified by reasonable necessity given the availability of the information through other means that are specifically provided for by the CCPA.

IA Recommendation: Revise subdivision (b)(1)(d)(2) to conform to Cal. Civ. Code Section 1798.120(a)(5).

- **Subdivision (b)(5) does not make adequately clear that a company may still require the use of an online account to process a request, regardless of whether or not an authorized agent is used**. Please see IA comments regarding Section 999.313(c)(7), *infra*.

- **Subdivision (b) requires that a privacy policy explain "the procedure for a consumer to designate an authorized agent," a role better filled by the AGO.** This requirement would charge businesses with explaining legal processes including how to execute a power of attorney or to name an authorized representative according to the regulations promulgated by the AGO. As explained above, a business privacy policy is not the appropriate place for consumer privacy resources generally, nor for company-specific

[62] Cal. Civ. Code § 1798.140(o).
[63] Cal. Civ. Code § 1798.115(a).

business processes. A business should not be put in the position of providing legal advice on the appropriate manner for designating an authorized agent. For certain types of consumer explanatory material, it may be more appropriate for the AGO to house resources for consumers that explain how best to satisfy the requirements established by the CCPA regulations.

As discussed above, IA recommends that the AGO avoid confusing the privacy policy with a privacy center. We wholeheartedly agree that consumers should be given access to helpful resources to assist in understanding privacy policies, practices, choices that may be available, and how to exercise statutorily provided rights over personal information. However, just as explained with regard to the inclusion of procedure explanations in the privacy policy, legal explanations should not be included for many of the same reasons. They are subject to change and, in the case of powers of attorney, may be governed by statute and interpretation by courts. They are also complex, and appropriate translations will take time to be prepared and vetted appropriately. Finally, in some cases, the business is not the entity that is best positioned to educate consumers on how the law applies to their specific circumstances. The risks of attempting to do so are likely to outweigh the benefits.

IA Recommendation: Strike Section 999.308(b)(5) in its entirety.

999.312 Methods for submitting requests to know and delete

- **Section 999.312 needs to be updated to reflect recent changes to the underlying statute.** Specifically, A.B. 1564 made changes to Cal. Civ. Code Section 1798.130(a)(1)(A), which now states that "[a] business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115."

  IA Recommendation: Update Section 999.312 to align with recent amendments by adding a provision that mirrors the language of CCPA Section 1798.130(a)(1)(A).

- **Section 999.312 diverges from CCPA's clear requirements regarding designated methods for submitting consumer requests.** First, the Proposed Regulations appear to potentially require a business to have three methods for requests, *e.g.* subdivision (c)(2) Example 2. CCPA simply requires a business to designate two methods. While the AGO's rulemaking authority allows guidance, consistent with CCPA (including as amended) as to appropriate methods and the designation of additional consumer friendly options, a requirement to designate *more* methods than required by CCPA exceeds the requirements of CCPA. The ISOR fails to justify this deviation from CCPA and the additional burden on business.

The Proposed Regulations deviate from CCPA in a more burdensome and troubling way by disregarding the entire concept of "designated methods" for exercising consumer rights. Subdivision (f) requires that a business respond to all requests, *regardless of how they are submitted*, by either treating the requests as properly submitted or sending specific directions to the consumer to correct any deficiencies or follow the specified process.[64] This entirely new proposal undermines the purposes of designating methods for submitting requests and potentially expands the requirements for how a business responds to consumer requests to an untold number of potential avenues of contact.

If a business must respond to a consumer request submitted through an improper channel that will require a business to ensure that all potential avenues of contacting a business or any of its employees, representatives, contractors, service providers, etc. are monitored, all personnel are trained to recognize and determine the appropriate course of action, and are able to ensure that such response happens quickly enough to meet with 10 day deadline for confirmation of a consumer request. The language of subdivision (f) contains no limitation on the potential avenues for contact, stating "[i]f a consumer submits a request in a manner that is not one of the designated methods of submission," the business must respond. While this opens a whole range of potential options for directly contacting the business — such as letters directed to the CEO or General Counsel; emails to random employees in roles unrelated to privacy compliance or user requests; calls to hotlines maintained for conducting employment verification, press inquiries, law enforcement emergencies, or investor relations; requests directed to agents for service of process; walk-in requests to business offices — it also raises the prospect of potentially more indirect submissions of consumer requests, including direct contact to individual employees of a business via social media or email, requests directed to outside vendors such as law firms, or even publicly posting a request directed to a business via an "at mention" on social media. Monitoring this array of channels would be incredibly burdensome for business and would be prone to systematic failures. A request directed to a single employee could sit for months without reply if the employee is on parental leave or has left the company. By contrast, a designated method for submitting a request will have a plan in place to ensure it is appropriately staffed regardless of comings and goings of individual employees. In today's online industry, communication via "snail mail" is virtually obsolete. Because most correspondence are hard copies of documents already available electronically, marketing materials from vendors, or otherwise non-urgent materials, not all hard copy mail will be reviewed with the regularity required to respond within the Proposed Regulations required deadline.

[64] *See also*, ISOR, p. 16.

When this potentially endless array of channels of communication are combined with the training mandate in the Proposed Regulations, the burden becomes even more untenable. The training for personnel who are tasked with responding to consumer requests under CCPA is a reasonable requirement directly provided for in CCPA. However, if every employee of a business is converted into someone who requires training because a consumer request could be directed to them, and they must be able to recognize the nature of the request, know where to direct it or how to respond, and the appropriate timeframe for such response, it potentially amounts to every employee having to be trained on CCPA regardless of the nature of their job role or the likelihood that they will encounter a notice in the scope of their employment.

The AGO has not met its obligations to explain why this necessary, why it is consistent with CCPA's clear language regarding "designated methods," how it furthers the purposes of the CCPA in a material way, whether the burden associated has been considered and is reasonable, or even whether there are any reasonable alternatives to achieve the goal of making sure that a business does not refuse consumer requests because they are deficient based on a technicality. If this is in fact the true purpose of this Section, subdivision (f) is broader than necessary to the extent it imposes requirements on how businesses respond to requests submitted outside of designated methods.

As noted in IA's first comment to this Section referencing the need to align the Proposed Regulations to A.B. 1654, there is clear legislative intent to allow a single online submission mechanism for online companies. It would be inappropriate for this Section to deviate from the clear language of the CCPA, as amended in 2019.

IA Recommendation: Revise Section 999. 312 by striking subdivision (f) in its entirety.

999.313 Requests to know and delete

- **Subdivision (a) of this Section creates new obligations and burdens on business by requiring that a business respond to a consumer request to confirm receipt and provide information on how business will respond**. While in the context of electronically submitted consumer requests, an auto-response can potentially satisfy this new requirement that is dependent on the consumer request being submitted via the "designated method" which the business has configured to send the appropriate auto-response. This is another reason why Section 999.312(f) should be struck, as is discussed above. If this requirement remains in the final regulations, businesses will face significant risks of violating the law because of a failure to provide an auto-response on channels that are not intended for processing consumer requests. Alternatively, a business would be forced to address this risk by sending a response to all inquiries of any kind a response that complies with subdivision (a). This could be very confusing to business partners, customers, job candidates, press, and other

entities that may communicate with a business about issues completely unrelated to CCPA. For channels of communication that are not electronic, the 10 day response time may also be challenging.

CCPA provides 45 days for a business to respond to consumer requests in Section 1798.130. This year, the California Legislature passed A.B. 1355 which amended this provision of the CCPA. While other changes were made to multiple provisions which include the 45 day initial response period language, the Legislature left the response deadline unchanged. In the absence of a statutory requirement for the 10 day deadline, the regulations should only add a new requirement if it is "necessary to further the purposes" of the CCPA.[65] At this point, it is unclear what benefit this requirement offers since the confirmation will only provide consumers with information that is not specific to their situation and is available in the notices and privacy policy (or as IA recommends, other privacy-related help content) mandated by the CCPA.

IA Recommendation: IA reiterates its recommendation that subdivision (f) of Section 999.312 be struck in its entirety for the additional reasons discussed in reference to Section 999.313. In addition, IA recommends that subdivision (a) of Section 999.313 be struck in its entirety.

- **Subdivision (c) is unnecessarily burdensome and duplicative, without adding additional value and transparency for consumers.** As discussed previously, the Proposed Regulations' attempt to rearrange the CCPA's disclosures results in redundant notices, cumbersome privacy policies, and responses to consumer requests that are likely to overwhelm consumers with information that is readily available via privacy policies and notices, potentially obscuring the personal information that is of most value in response to an access request. This subdivision requires businesses to respond to a consumer access request not only with specific pieces of personal information but also with a second set of responses—namely, customized metadata regarding the information collected for each customer, categorized in a complicated manner outlined by the statute. There are numerous reasonable alternatives to this requirement which could lower the burden of this provision: 1) a revision to Section 999.313(c) that would clarify that a company need not additionally fulfill a request to provide categories of information collected if it is also providing specific pieces of information; 2) a revision to Section 999.313(c)(10) that would not require the additional pieces of information listed there (categories of sources, business purpose, categories of parties to whom disclosed/sold and why) to be broken out for each category of information collected; 3) a revision to Section 999.313(c)(11) clarifying that use of the language specifically enumerated in either CCPA or the regulation "provides consumers a meaningful understanding of the categories listed;" 4) a revision to

[65] Cal. Civ. Code § 1798.185(b)(2)(as amended by A.B. 1355).

Section 999.313(c)(9) expanding the circumstances in which a company could rely on a generic articulation of categories in the Privacy Notice, as opposed to a customer-specific feed. For example, the regulation could be broadened to clarify that a business may refer to its privacy policy when its response would be the same for "substantially all" or "most" consumers.

IA Recommendations: Revise subdivision (c) as follows:

- (c)(2) "For requests that seek the disclosure of categories of personal 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 may deny the request to disclose the categories and other information requested and shall inform the requestor that it cannot verify their identity. If the consumer also requested specific pieces of information and the business is discloses specific pieces of information, the business is not required to respond to the request for categories of personal information. If the request is denied in whole or in part, the business shall provide or direct the consumer to its general business practices regarding the collection, maintenance, and sale of personal information set forth in its privacy policy.
- (c)(9) "In responding to a consumer's verified request to know categories of personal information, categories of sources, and/or categories of third parties, a business shall provide an individualized response to the consumer ~~as required by the CCPA. It shall not refer the consumer to the businesses' general practices outlined in its privacy policy~~ unless its response would be the same for ~~all~~ most consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories."

- **Subdivision (c)(1) creates risks of inappropriate disclosure of information about a consumer in response to an unverified consumer request.** The Proposed Regulations treat verification of a consumer request as though it is appropriate to view identity verification across a spectrum of likelihood that the person making the request is the consumer, rather than as being a minimum requirement that must be satisfied. In doing so, the AGO appears to be more concerned about the potential harm to consumers that would result from not being able to access personal information, delete information, or opt-out or in than the harm that may result from bad actors inappropriately exercising a consumer right specifically to engage in illegal or malicious action. IA member companies believe that the concern should focus more clearly on the risks from bad actors. If a business is not responding appropriately to consumer requests, the CCPA provides a remedy in the form of Attorney General enforcement. But for a consumer whose personal information is inappropriately obtained, account contents deleted, or accumulated benefits of a financial incentive program stolen, there is unlikely to be an adequate remedy.

The AGO and the California Legislature know all too well how determined criminals will target consumers and their personal information. California was a leader in passing the first data breach notification requirement in the U.S. to specifically address the harms to consumers from their personal information ending up in the wrong hands. For this reason, IA believes that the Proposed Regulations should not require that a consumer request that is rejected for failing verification be converted into a request to exercise a different CCPA consumer right.

This analysis of subdivision (c)(1) is further complicated by the way the CCPA and the regulations approach categories of personal information. General disclosures of categories of personal information, such as those mandated in notices of collection or a privacy policy, pose no specific challenges since the disclosures are not consumer specific and apply broadly. However, subdivision (c)(1) contemplates disclosure of categories of personal information specific to a particular consumer in cases where there is not appropriate verification to disclose "specific pieces" of personal information. It is unclear what types of information would go beyond generally applicable disclosures of categories of personal information without themselves raising the same issues as personal information. For example, if a request was made for personal information from a company that offers security devices and security monitoring services and the request was rejected for failure to meet the verification requirements, it would not be appropriate for the business to disclose any information, even "categories," to the individual who was unable to verify their identity. Even categories could reveal information that should remain private. For example, the business could disclose that personal information was collected for categories related to security devices, but not categories related to the monitoring service revealing that the account holder does not subscribe to this service. This information could result in a consumer being placed at risk of being targeted for a break-in.

In addition, if the business determines that categories of personal information are the same as those generally available in its privacy policy, the business is not required to send a detailed response to the consumer.

IA Recommendation: Strike language in subdivision (c)(1) mandating that a request that fails verification be considered for disclosure of categories of personal information, as follows, "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).~~

- **Subdivision (c)(3) does not fully safeguard against risks to other consumers' accounts.** Subdivision (c)(3) states, "[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. However, CCPA is clear that access requests shall not "adversely affect the rights and freedoms of other consumers."[66] This limitation on the obligations under the CCPA should be reflected in this subdivision of the Proposed Regulations.

  IA Recommendation: IA recommends amending this to reference security risks to personal information of other consumers as well, by revising the subdivision to read, "substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's or another consumer's account with the business, or the security of the business's systems or networks."

- **Subdivisions (c)(5) & (d)(6)(a) have potential security implications and should be clarified to reduce such risks and to ensure its requirements do not encourage activity that would itself violate state or federal law.** The subdivisions require that if an access or deletion request is denied because of federal or state law, the consumer be notified of the reason why. This has potential implications for responses to from consumer seeking access to information related to law enforcement requests. If a business is prevented by law from disclosing the request, it will also be prevented by law from disclosing that a non-disclosure provision associated with a law enforcement request is the reason why the request was denied. Other reasons for denying requests could result in greater risk of fraud or security threats. In general, this subdivision should make clear that if the basis for denying a consumer request is an exception to CCPA, the business should not have to disclose the reason.

  IA Recommendations:
  - Revise subdivision (c)(5) as follows, "If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor ~~and explain the basis for the denial~~. If the request is denied only in part, the business shall disclose the other information sought by the consumer."
  - Revise subdivision (d)(6)(a) as follows, "Inform the consumer that it will not comply with the consumer's request ~~and describe the basis for the denial, including any statutory and regulatory exception therefor~~;"

[66] Cal. Civ. Code § 1798.145(j).

- **Subdivision (c)(7) should be clarified to specify that a business may use a password protected account to respond to consumer requests submitted via an authorized agent.** This is necessary to ensure that online accounts, particularly those for whom verified personal information such as name, address, phone numbers, and other identifying information are not needed can be used to ensure that the party who will obtain the information has been properly authenticated using the account security controls that govern the log-in process for the password protected account.

  IA Recommendation: Revise subdivision (c)(7) as follows: If a business maintains a password-protected account with the consumer, it may comply with a request to know, submitted by a consumer or an authorized agent, by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 4.

- **Subdivision (d)(1) requires that deletion requests that cannot be verified be treated as requests to opt-out, creating risks that consumers will lose potential benefits and potentially disrupt services, without ever indicating that it is their preference.** CCPA does not specify that a consumer request to opt-out of sale requires verification, however where an individual has made an attempt to verify account ownership and failed, there may be sufficient indicia that it is not the account holder. The AGO does not weigh any benefits that the consumer may associate with allowing the business to engage in the "sale" of personal information and which may form the basis of an affirmative choice not to opt-out. However, the CCPA clearly adopted an opt-out regime that is designed to put that choice in consumer hands. If the Legislature thought that the activity captured in the "opt-out of sale" provision inherently lacked any value to consumers, it could have designed CCPA differently to reflect that choice. It chose not to and the AGO should not attempt to rewrite CCPA by creating avenues where by a consumer may passively become opted-out (and unable to be invited to opt back in for a year) as though there is no value.

999.314 Service Providers

- **Subdivision (c) imposes unjustified limitations on service providers' permissible uses of data.** These limitations contradict and go beyond the statutory definitions of "business purpose" and "service provider" in a few key ways. The CCPA explicitly exempts from "sale" disclosures to "service providers" for a broad list of enumerated "business purposes" defined under the statute, subject to certain contractual limitations.[67] Importantly, the statute defines "business purpose" to include both a business's or a service provider's operational purposes or other notified purposes.[68]

[67] Cal. Civ. Code § 1798.140(t).
[68] Cal. Civ. Code § 1798.140(d).

The statutory text also permits a service provider to use the personal information it receives from one business for such business purposes of both that business and the service provider where the use is authorized as part of the contracted-for "services" provided to the business and is otherwise consistent with the CCPA.[69]

Because business purposes may include using personal information received from one business in a way that might also provide some benefit to other businesses, the CCPA is best interpreted to permit the service provider to use the personal information that it receives in a way that might provide some benefit to itself or to its business partners, as long as such use is consistent with the business purposes identified in the written agreement between the business and the service provider and otherwise permitted by the CCPA.[70]

Subdivision (c) states:

> *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. 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.*

The plain text of the subdivision appears to prohibit service providers from using the personal information they receive from one entity to provide services to another person or entity, unless such services are necessary for detecting security incidents or preventing fraud or other illegal activity.

The Proposed Regulations improperly focus solely on the business purpose of the business, and ignore the fact that the statutory definition of "business purpose" also includes the use of personal information for the "service provider's operational purposes or other notified purposes."

Second, the activities included in the list of business purposes (such as "performing services on behalf of the business or service provider, including providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider") may require the combination and use of personal information received from and for the benefit of multiple businesses in order to provide such services to the business that provided the data. As such, focusing solely on the business purposes of the business, as the Proposed Regulations do, would both render the language surplusage, contrary to well-established canons of statutory

[69] Cal. Civ. Code § 1798.140(v) & § 1798.140(t)(2).
[70] Cal. Civ. Code § 1798.140(v).

interpretation, as well as potentially render impermissible a number of the activities explicitly included on the list of permissible business purposes.

IA Recommendation: Revise subdivision to read, "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. 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, engage in solely internal uses, or another business purpose that is consistent with the terms of the agreement with the businesses.

- **Subdivision (d) imposes new obligations on service providers to respond to consumer requests.** It requires that a service provider that receives but "does not comply" with a consumer's request to know or delete must inform the consumer of the reason for the denial, explain that the consumer should submit the request directly to the business, and when feasible, provide the contact information for the business. This requirement creates new obligations for service providers not present in CCPA. In addition, it seems to recognize that in most instances the business, and not the service provider, is the correct entity to respond to a consumer request by directing a service provider to explain to the consumer that the request should be directed to the business and provide the contact information if possible. And yet, it also confusingly suggests that independent of redirecting the consumer, a denial of a consumer request must be given an explanation of why (which seems to imply that this a reason other than that the request should be directed to the business).

  IA Recommendation: Subdivision (d) should be struck in its entirety.

- **The Proposed Regulations should clarify that businesses do not have to use specific contractual language as long as the language conveys the requirements of the CCPA.** This section should clarify that no specific contractual language is necessary to comply with the requirements of the CCPA regarding business arrangements between businesses and service providers. Instead language that conveys the restrictions and obligations required by CCPA suffices to not only meet statutory obligations, but also to establish the appropriate roles and responsibilities of the entities participating in the business arrangement. Due to the potential proliferation of state privacy laws, existing sector-specific federal privacy laws, and global privacy frameworks and country-specific laws, businesses should not be required to use any CCPA-specific language in contracts and business agreements to determine the nature of the business relationship and to ensure that necessary privacy and security protections apply to consumer personal information.

- **The Proposed Regulations' clarification of who is a service provider conflicts with the CCPA and stands to subject entities outside California to CCPA without an appropriate nexus.** Subdivision (a) says that persons or entities that: (1) provide services to a person or organization that is not a "business;" and (2) that would otherwise be considered a "service provider" shall be deemed a service provider for purposes of the regulations and CCPA. The ISOR suggests that a service provider acting on behalf of an entity that is not a "business" will be subject to the "less stringent requirements" of a "service provider."[71] It specifically mentions service providers for nonprofits and government. But this change would also apply to other entities that do not qualify as a "business," for example, because they do not "do business in California."

  The ISOR explains that this is necessary because the definition of "Service Provider" doesn't adequately account for service providers who collect information on behalf of a business, rather than receiving information directly from the business. This appears to be a narrow problem which could be resolved with a narrow fix without expanding the requirements of the CCPA unnecessarily. By eliminating "business" from the definition of "service provider," the AGO removes a primary nexus in CCPA to California and has a potentially sweeping impact on out-of-state commerce that is outside its regulatory purview.

999.315 Requests to opt-out

- **Subdivision (a) requires that a business provide two or more designated methods for a consumer to opt-out from sale, one of which must be an interactive webform, adding an additional requirement to the CCPA.** CCPA Sections 1798.120, 1798.130, and 1798.135 only contemplate one method for opt-out from sale which is specified in Section 1798.135(a)(1).[72] While allowing more flexibility to businesses to adopt additional methods to offer to consumers to exercise their rights may be appropriate in terms of furthering the purposes of the title, a mandate to adopt multiple methods or to use any specific method other than the statutorily-mandated link exceeds the AGO's rulemaking authority.

  IA Recommendation: The Proposed Regulation should be revised to make the designation of any additional methods, beyond the link required in Section 1798.135(a)(1), discretionary, as follows: "A business shall provide ~~two or more designated methods for submitting requests to opt-out,including~~, at a minimum, an

[71] ISOR, p. 21.
[72] IA notes that the proposed ballot initiative by Alastair Mactaggart, as submitted to the AGO by letter dated October 9, 2019, (as amended November 13, 2019) would add language to CCPA 2018 to incorporate the concept of "opt-out preference signals" as an alternative mechanism to the single method of a "clear and conspicuous link" required by the CCPA as currently enacted. *See* Section 13, amending Cal. Civ. Code § 1798.135, of the text of the ballot initiative attached to the November letter (version three). Presumably, this indicates that Mr. Mactaggart agrees that CCPA 2018 does not include this option.

interactive webform accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information," or "Do Not Sell My Info," on the business's website or mobile application. A business may, at its discretion, designate additional methods by which it will accept consumer requests to opt-out of sale of personal information."

- **There are technical and legal issues with the requirement in subdivision (c) that businesses that collect personal information from consumers online must treat consumer-enabled privacy controls as a valid request to opt-out under 1798.120.**
    - This method was not contemplated in the CCPA, as is discussed above in regard to subdivision (a). This requirement does not comply with the CA APA and regulations as it is: 1) not necessary; 2) beyond the authority of the AGO's rulemaking mandate; 3) it has not been adequately justified in the ISOR; 4) the financial impact was not adequately considered in the SRIA; and 5) reasonable alternatives were not adequately considered.
    - The language regarding the opt-out logo or button indicates an intent for that option to be used "by all businesses to promote consumer awareness of the opportunity to opt-out…" 1798.185(a)(4)(C). The Proposed Regulations require "at a minimum, an interactive webform accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information," or "Do Not Sell My Info," on the business's website or mobile application."
    - If the business must provide two or more designated methods and one must be the webform/button/link, the business should be able to choose the other option to designate. As is discussed in IA's comments on Section 999.312 of the Proposed Regulations regarding designated methods to submit access and deletion requests, this provision essentially eliminates any business choice and control over how to take-in consumer requests and to ensure adequate resources, technology, and training for handling consumer requests via the designated channels. Given the serious nature of the legal obligations which are triggered by a consumer request to opt-out, businesses need to have clarity around the potential avenues by which such requests will be submitted so that they may ensure the appropriate measures are in place for compliance. Creating uncertainty about which channels could be used for making such requests sets businesses up for failure.
    - While some businesses already offer account controls which may allow opt-out from sale to occur in a manner that is secure and will allow the consumer and the business to have a shared understanding of the nature and scope of the consumer's choice, there are significant issues of how a browser-plug in or another type of browser signal should be applied (for devices, browsers, consumers), how such a signal would interact with other rules (e.g., CCPA's waiting period to request opt-in), and would impact other users of shared devices or shared "unique identifiers" such as IP addresses. A consumer may

think that use of a browser-based signal has an impact beyond what is technologically feasible, since it will be specific to that browser on that specific device and cannot be applied across all of the consumer's browsers and devices without specific action from the consumer. If a consumer wants to accomplish an "account-wide" opt-out, it will need to do so through direct communication with an online business in a manner that is specifically connected to the consumer's account. In addition, some browser or device based controls may deprive consumers of notice regarding the potential ramifications of their choice to opt-out, the availability of a financial incentive, or an alternative option that would allow the consumer a more nuanced choice than "all or nothing."[73]

IA Recommendation: This requirement should be made discretionary for online businesses that can implement it in a manner with adequate controls to determine the intent of the consumer to opt-out from sale and the scope of how such opt-out should be applied. This may be accomplished by revising subdivision (c) as follows, "If a business collects personal information from consumers online, the business **may** ~~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 submitted pursuant to Civil Code Section 1798.120 **if the controls allow the consumer to clearly indicate an intent to opt-out of sale, in whole or in part, for an online account maintained with the business** ~~for that browser or device, or, if known, for the consumer~~."

- **Subdivision (f) purports to make a consumer's opt-out of sale retroactive, by requiring that a business notify each third party who purchased consumer's personal information in the 90 days prior to the opt-out.** This is inconsistent with the CCPA and imposes a significant technical challenge and burden, neither of which are adequately considered in the ISOR or in the SRIA. Section 1798.120(d) states that, "a business that has received direction from a consumer not to sell the consumer's personal information, ...shall be prohibited...from selling the consumer's personal information *after* its receipt of the consumer's direction." (*emphasis added*) Section 1798.135(a)(4) states, "[f]or consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business." Nothing in CCPA's rulemaking provisions related to opt-out of sale empower the AGO to disregard the clear language of the statute and convert a forward-looking obligation into a retroactive mandate. The rulemaking provision of CCPA tasks the AG

[73] Version 3 of the 2020 ballot initiative to amend CCPA 2018 also acknowledges the need for rules regarding uses of opt-out signals in Section 13, by proposing an amendment to Cal. Civ. Code § 1798.135 to add as new (b)(1) a provision that allows use of opt-out preference signals that comply with technical specifications set forth in regulations to be promulgated under the statute. If the final regulations for CCPA 2018 will include a requirement to recognize an "opt-out preference signal" as currently contemplated in the Proposed Regulations, then such a rulemaking in line with the proposed rulemaking mandate in Version 3 of the 2020 ballot initiative, described with specificity in the proposed new Cal. Civ. Code § 1798.185(20), should be added.

with, "establishing rules and procedures for...business compliance with a consumer's opt-out request."[74]

The ISOR seeks to justify the introduction of this new obligation by noting a perceived gap in the CCPA, that because the CCPA does not require businesses to disclose the specific names of third parties to whom personal information has been sold, a consumer who wants to control the sale of their information will not know all entities who have it. The ISOR states,

> *Because the CCPA only requires businesses to disclose the categories of third parties with whom it sold the consumer's information, and not their specific identities, this subdivision places the onus on the business to forward the consumer's request to those businesses that it sold their information within the 90 days prior to receiving the consumer's request.*[75]

However, the ISOR fails to recognize the role of consumer choice in exercising the opt-out. During the 90 days prior to the consumer submitting the request to opt-out from sale, the consumer will have been on notice of the right to opt-out because they will have been provided a notice of that right through the Notice at the time of Collection,[76] the Privacy Policy,[77] and the Notice of the Right to Opt-Out of Sale (a persistent notice via a prominent link or logo).[78] The transfers that occur in those 90 days occur following notice, but before the consumer indicates a choice to opt-out to the business. The business should be able to act in reliance on the choices that consumers make to exercise their rights under CCPA. The ISOR fails to establish that consumers generally have an expectation and a desire, once they have decided to opt-out, to make that decision retroactively and that opting a consumer out of the sale of personal information on a going forward basis fails to effectuate the intent of the consumer or the intent of the California Legislature when it designed this provision.

In introducing this new requirement in the Proposed Regulations, the AGO also imposes a significant new burden on businesses. Retroactive application is not required by the rulemaking mandate in Section 1798.185(a)(4)(B), thus IA presumes the AGO relies on the more general rulemaking authority of Section 1798.185(b)(2) which allows rulemaking "as necessary to further the purposes of this title." However, it is worth noting that the underlying premise of this change to CCPA does not merely fill in a gap in detail; it second guesses determinations of the Legislature. First, the Legislature determined that providing consumers with categories of third parties in disclosures was an appropriate balance of the burden on business and the value of transparency and consumer control over their personal information. As the ISOR makes clear, the AGO

[74] Cal. Civ. Code § 1798.185(a)(4)(B).
[75] ISOR, p. 25.
[76] Proposed regulation § 999.305(b)(3).
[77] Proposed regulation § 999.308(b)(1)(e).
[78] Proposed regulation § 999.306.

has done its own weighing of this balance and rejected it. This is beyond the AGO's authority. Second, the Legislature determined that a forwarding-looking only opt-out was the appropriate balance of these same equities. Again, the AGO has inappropriately substituted its judgment for that of the Legislature.

It is also not clear whether the AGO considered the burden on business of imposing this retroactive requirement. Other than the glancing statement that the 90 day time period is an appropriate limit to manage the burden,[79] there is no discussion of the burden, nor any consideration of reasonable alternatives in the ISOR. The SRIA does delve any deeper into the nature of this burden. Given the breadth of the definition of "sale," this burden should not be underestimated in terms of the number and complexity of different types of transactions to which it may apply. Creating an entirely new requirement to track sales and to be able to connect a specific consumer's data to specific transactions going back 90 days is a significant new burden. Developing mechanisms, whether automated or manual, to contact each party to transactions involving a specific consumer and providing them the necessary information to even identify the consumer is a daunting task as well, particularly when remaining mindful of the extraordinarily broad definition of the personal information in CCPA. For example, because of the inclusion of "unique identifiers" as personal information, if a consumer, Jane Doe, opts out from sale of personal information a business must identify all personal information associated with Jane Doe, all transactions involving sale in the past 90 days for any piece of Jane Doe's personal information including an IP address or device ID, and notify all parties to such transactions by providing sufficiently clear direction that the third party recipients can identify the information in their systems and take action to prevent further sale. Before the AGO imposes this burden, it merits consideration of less burdensome alternatives, including shorter time frames and not creating the new requirement at all.[80]

IA Recommendation: Strike subdivision (f) in its entirety.

- **Subdivision (h) creates security risks for consumers and businesses by requiring a business to disclose in response to a suspected fraudulent consumer request the reason why it is believed to be fraudulent.** Subdivision (h) provides that a request to opt-out does not need to be verifiable, but a business can decline to comply if they have a "good faith, reasonable, and documented belief" that the request is fraudulent. Business must provide notice to consumer and explain why the business believes it is fraudulent. Such disclosures may harm business efforts to protect against fraud and undermine consumer protections for security and privacy. By explaining to a potential bad actor why the business has determined they are a bad actor, the business is

[79] ISOR, p. 25.
[80] By suggesting that less burdensome alternatives be considered, IA does not intend to imply, contrary to the paragraphs above, that IA believes that such alternatives are within the AGO's rulemaking authority.

essentially providing criminals with blueprints as to how to get around their fraud detection systems and protocols. Please see also IA comments, *supra*, regarding Section 999.313.

999.316 Requests to opt-in to sale after opting-out

- Please see IA comments, *supra*, regarding Section 999.301(a), the definition of "affirmative authorization" regarding the risks for requiring consumers to go through a two-step process. For the reasons explained with regard to the definition of affirmative authorization, subdivision (a) of this Section should be revised to eliminate mention of the two-step process and should be substituted with the term "affirmative authorization."

  IA Recommendation: Revise subdivision (a) to read, "Requests to opt-in to the sale of personal information shall require affirmative authorization ~~use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in~~."

999.317 Training and record-keeping

- **The training requirement in subdivision (a) is vague and overly burdensome and offers no additional protections for consumers.** The CCPA already includes reasonable training requirements for staff dedicated to handling consumer requests under the statute.[81] Subdivision (a) expands this requirement to a mandate that individuals responsible for handling consumer inquiries "shall be informed of all the requirements in the CCPA and these regulations" rather than only the relevant Sections of CCPA. CCPA is a complex and difficult to understand statute that encompasses not only consumer rights but also enforcement, rulemaking authority, and security breach remedies. To require staff dedicated to handling consumer requests to be trained on *all* of CCPA, rather than the provisions which relate to consumer requests and consumer rights expands the CCPA's training mandate in a way that is unhelpful and may lead to more confusion and less effective training. The ISOR suggests that the training mandate was expanded because of gaps in CCPA's text. If there are specifically relevant Sections of CCPA to which the training requirement should apply because they are related to the exercise of consumer rights, then it would have been preferable for the AGO to expand the requirement to those Sections rather than the entirety of the statute and the regulations.

  IA Recommendation: Strike the entirety of subdivision (a).

[81] *See, e.g.*, Cal. Civ. Code § 1798.135(a)(3) which provides, "Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Section 1798.120 and this Section and how to direct consumer to exercise their rights under those Sections."

- **The recordkeeping requirement in subdivision (g) is vague, imposes an unjustified burden on business without promoting transparency to consumers or accountability, and exceeds the AGO's rulemaking authority.**
    - The provisions are vague. First, the definition of "commercial purposes" in the CCPA is extremely broad.[82] This term is seldom used in the CCPA or in the Proposed Regulations and it is unclear as to whether or not "business purposes" are encompassed or excluded from the scope. In addition, it is not clear what types of activities constitute "receipt" for commercial purposes. This is particularly troubling given the Proposed Regulations' approach to "designated methods" for submitting requests and the inclusion of browser signals and other automated controls as "requests" to opt-out.
    - The ISOR does not support the necessity of the new tracking and reporting obligation. It simply states, "This subdivision is necessary to inform the Attorney General, policymakers, academics, and members of the public about businesses' compliance with the CCPA."[83] It further states that it considers the burden by limiting application to businesses that handle a large amount of California consumer data (10 percent of state population or more). The SRIA, however, states that "there is no detailed data on how many California consumers all companies in the state have."[84] It "speculates" that "all firms with more than 500 employees" will be subject to the subdivision, which it states includes 9,858 businesses.
    - The SRIA "assumes," without any cited basis, that the businesses subject to the subdivision's recordkeeping requirements are "likely to have mature systems for identifying, processing, and analyzing personal information from their data mapping and consumer response systems, ...that there is no incremental cost of actually collecting this information."[85] There is no reasonable basis for the SRIA to "assume" that nearly 10,000 California businesses have in place systems to determine, for example, the date of receipt of a request to opt-out of sale and the date on which the business has fully complied with the requirements of the Proposed Regulations to notify all third parties who have received the data in the 90 days prior to the consumer's opt-out. Since businesses had no notice of the retroactive application of CCPA's opt-out provision prior to publication of the Proposed Regulations, it would have been impossible for businesses to know of this requirement and to have already built systems capable of complying with new recordkeeping obligations in connection with it. Thus, the SRIA estimate of $984/year per business for satisfying this obligation seems fatally flawed and inaccurate.[86]

[82] Cal. Civ. Code § 1798.140(f).
[83] ISOR, p. 28.
[84] SRIA, p. 26.
[85] *Id.*, p. 27.
[86] *Id.*

- Alternatives to the recordkeeping and publication requirements in the Proposed Regulations were not adequately considered. The ISOR is not clear as to what types of alternatives to detailed metrics on consumer requests were considered to achieve the goals of transparency and accountability. It appears that the only alternatives considered were not having any requirements for reporting metrics or applying the metric reporting to all businesses. While California law does not require the AGO to invent alternatives where none exist, alternatives do exist in leading privacy regimes around the globe including the GDPR. For example, the AGO could have considered an in-take mechanism for consumer complaints regarding responses to consumer requests, periodic audits of businesses, or purely internal documentation of compliance with CCPA's requirements.
- Given the lack of understanding of the nature of the burden on businesses subject to the recordkeeping requirements and the potential that the aims could be achieved through less burdensome alternatives, the subdivision should be struck from the Proposed Regulations.
- While the problems with the mismatch between the burdens of the provision and the benefits form an adequate basis for the subdivision to be deleted from the Proposed Regulations as inconsistent with the APA, it is also worth noting that CCPA does not mandate this record-keeping requirement, nor any regulations in this area. Thus, this subdivision would only be appropriate if it was determined to be "necessary" to further the purposes of CCPA. The AGO has failed to meet this threshold.
- Given that the basis for such a recordkeeping obligation would be the rulemaking authority in Cal. Civ. Code Section 1798.185(b), the AGO is not subject to a requirement to publish the regulations by July 1, 2020 and also has significant discretion to allow a period of time for businesses that would have to comply with this new obligation to build the necessary systems and come into compliance. If the AGO keeps this proposed requirement, it should allow covered businesses one year to come into compliance after the regulation take effect and after a business becomes subject to the requirement.

IA Recommendation: Subdivision (g) be struck in its entirety.

999.318 Access/Deletion for households

- **This section does not adequately address safety concerns raised with the "household" provision as it relates to access/deletion requests for several reasons:**
  - It assumes that a business will know how many individuals are members of a household which is unrealistic and an obstacle that cannot be overcome.
  - It assumes that an abusive member of a household will not coerce other members of the household to provide consent in order for the abuser to maintain control over his/her victims activities.

- It fails to establish any timeframe for the concept of household, so it is not clear whether a friend who stays in a spare room for a month while looking for a new place to live is a member of the household, is a member for just that month, or shall be considered a member of the household forever.
- It also is not clear how it will be established that a shared access point, device, IP, or other identifier is connected with a group of people who form a "household" versus, for example, a hotel business center.
- This section of the Proposed Regulations should be struck unless adequate detail can be added that explains how households should be defined, how members of a household must establish their identity as a member of the household, and how a business can determine for each household that it has received consent from each member.
- This section should also be struck unless a mechanism can be developed to ensure that members of a household cannot be coerced or intimidated into providing consent for an access or deletion request.

IA Recommendation: The AGO should strike this section in its entirety from the Proposed Regulations and further contemplate the guidance in A.B. 1355 to address the safety concerns posed by "households" in the context of access and deletion requests. Such regulations can be issued separately from the regulations required to be issued by July 1, 2020, and processing of requests related to households postponed until such time as these critical issues of physical safety can be addressed.

999.324 Verification for password-protected accounts

- **Subdivision (a) should make clear that a business may require that a consumer request submitted through an authorized agent be authenticated through a password-protected account** as discussed in IA's comments to Section 999.313(c)(7), *supra*. In addition to IA's prior recommendation to revise Section 999.313, IA also recommends that subdivision (a) of Section 999.324 is revised to make this explicit.

  IA Recommendation: Revise subdivision (a) to read, "If a business maintains a password-protected account with the consumer, the business may require the consumer to verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in Section 999.323. A business may require the consumer to verify the consumer's identity and the consumer's permission to act on the request of an authorization agent through the business's existing authentication practices for the account. The business shall also require a consumer to re-authenticate themselves before disclosing or deleting the consumer's data."

999.326 Authorized agent

- **The interaction of the verification and authorized agent provisions do not provide needed clarity regarding proper verification and authentication of agents.** The verification provisions of the Proposed Regulations do not adequately explain the proper interaction of a business' discretion in authentication with the requirement that authorized agents be allowed to make requests on behalf of consumers. In addition, it is not clear how business can be expected to reasonably authenticate agents. Because of these difficulties, as IA proposed in relation to Section 999.313(d)(7) and Section 999.324, businesses should be able to rely on their authority to require consumers to use existing accounts to make requests, to also require agents must make the requests through those same accounts as a way of demonstrating the agent's authority. The verification sections of these regulations should also provide greater specificity as to how authentication of authorized agents should progress including providing more substantial guidance on the minimum evidence required and a safe harbor for businesses.
- **Regulations are not clear regarding the use of an authorized agent to exercise the various consumer rights created by CCPA.** The CCPA only specifically includes the ability to authorize another person to exercise the right to opt-out of sale.[87] As has been previously discussed in the connection with use of an authorized agent, the difficulty of authenticating the agent's identity and authorization from the consumer create significant risks for consumers and will burden businesses who will work diligently to avoid acting on fraudulent requests. Consistent with CCPA, the Proposed Regulations should restrict use of authorized agents to the exercise of the right to opt-out sale.

999.330 Minors under 13 years of age

- **The Proposed Regulations should clarify the knowledge standard.** The standard governing the "knowledge" a business must have to trigger a duty to obtain affirmative authorization for the sale of the personal information of consumers under 13 in order must be consistent with the Children's Online Privacy Protection Act ("COPPA"). Under COPPA, a website operator must obtain parental consent when it has actual knowledge that it is collecting personal information from a user who is a child, not from "children" in general. This is reflected in the COPPA statute, regulations and longstanding FTC commentary.[88] Requiring a standard different from what is required under COPPA would cause confusion and potentially complicate a business's efforts to protect

[87] Cal. Civ. Code § 1798.135(c).
[88] *See, e.g.*, 15 U.S.C. 6502(a)(1) ("It is unlawful for . . . any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b).") (emphasis added); 16 C.F.R. 312.3 ("It shall be unlawful for . . . any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part") (emphasis added); FTC, Complying with COPPA: Frequently Asked Questions A.14 ("COPPA covers operators of general audience websites or online services only where such operators have actual knowledge that a child under age 13 is the person providing personal information.").

minors and their personal information. What is more, it would be impermissible under COPPA's preemption clause.[89]

- **The Proposed Regulations should be clear that a consent methodology that satisfies COPPA necessarily satisfies the "affirmative authorization" requirement of the CCPA.** Under COPPA's preemption standard, it is clear that the Attorney General may not impose additional or otherwise inconsistent consent requirements beyond those imposed by COPPA. Under COPPA and the COPPA Rule, new approved methods for parental consent may become available in the future and such methods should be available to be used by the clear terms of the CCPA regulations.
- **Subdivision (a)(1) requires "affirmative authorization" of the sale of personal information that is in "addition to any verifiable parental consent" required by COPPA creating a duplicative requirement for businesses that are covered by COPPA.** This provision could be drafted more narrowly to fit the need explained in the ISOR. The ISOR explains that "[t]his is necessary because the CCPA's prohibition on the sale of children's personal information covers information regardless of whether collected online, offline, or from a third party."[90] IA has no objection to entities that are not subject to COPPA being required to follow CCPA requirements. However, for a business that is subject to COPPA and has a federally-complaint process to obtain consent from parents or guardians of minors, there is no justification for requiring a completely separate and secondary consent flow. This is particularly true given that the Proposed Regulations accept the adequacy of the existing COPPA parental consent mechanisms, by adopting them for the CCPA parental opt-in to sale. A more narrow provision requiring a COPPA-compliant parental consent process that also addresses opt-in to sale under the CCPA *or* a CCPA-compliant parental opt-in to sale process adequately addresses the critical interest in child safety and privacy, as well as parental interests in being empowered to make safety and privacy decisions on behalf of their young children. IA also believes that the imposition of additional requirements on "operators" regulated by COPPA is inconsistent with the preemption clause in COPPA.[91]

  IA Recommendation: Revise subdivision (a)(1) to read, "A business that has actual knowledge that it collects or maintains the personal information of a child~~ren~~ under the age of 13 shall utilize ~~establish, document, and comply with~~ a reasonable method, in light of available technology, for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. Verifiable parental consent that complies with the Children's Online Privacy Protection Act and regulations thereunder shall satisfy this obligation. ~~This affirmative~~

[89] *See* 15 U.S.C. § 6502(d) ("No State or local government may impose any liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action described in this chapter that is inconsistent with the treatment of those activities or actions under this section.")
[90] ISOR, p. 34.
[91] 15 U.S.C. § 6502(d).

~~authorization is in addition to any verifiable parental consent required under the Children's Online Privacy Protection Act...~~"

999.336 Discriminatory practices

- Please also see IA comments and recommendations related to financial incentives in regards to Proposed Regulations Section 999.307, *supra*.
- **Subdivision (a) ties CCPA's non-discrimination provisions to the exercise of consumer rights created by regulations which exceeds the AGO's rulemaking authority.** The CCPA is clear that non-discrimination obligations only apply to the rights "created by this title."[92] Where the California Legislature wanted to incorporate future provisions created by AGO rulemaking in CCPA, it did so with specific language.[93] Thus, consistent with rules of statutory construction, an intent to include new rights created by regulation cannot be read into Section 1798.125 of CCPA. This also exceeds the rulemaking mandate in Section 1798.185(a)(6) which charges the AGO with "establishing rules and guidelines regarding financial incentive offerings." Thus, this subdivision should be revised to be consistent with CCPA.

  IA Recommendation: Revise subdivision (a) as to read, "[a] financial incentive or a price or service difference is discriminatory, and therefore prohibited by Civil Code Section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA ~~or these regulations~~."

999.337 Calculating value of consumer data

- **There is no basis for a requirement to calculate and disclose the value of consumer data in CCPA.** In fact, the California Legislature had at least one bill introduced in the 2019 which would have amended CCPA to require exactly this. A.B. 950 proposed to require businesses to disclose the monetary value of consumer data, but that bill did not pass. If CCPA included this requirement, such a bill would not have been necessary. In addition, unlike other bills that would have amended CCPA which were considered and ultimately passed in the same legislative session, A.B. 950 was not acted on by legislators. Where the Legislature chooses not to enact a proposal, the AGO should not legislate such proposal through the rulemaking process.
- **This new obligation is not necessary, is burdensome, and is of questionable value.** The SRIA notes a significant lack of agreement on how to value data and on whether it can be done accurately. This lack of agreement is reflected in this Section of the Proposed Regulations in that it allows a number of different methodologies for calculating the value of data. The lack of an agreed method of calculation means that the approaches taken and the resulting values will differ significantly which will limit the utility to consumers.

[92] *See* Cal. Civ. Code § 1798.125(a)(1).
[93] *See, e.g.*, Cal. Civ. Code § 1798.140(i)("and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185").

The perceived value of data is subjective, in flux and depends on context. Because data lacks clear, objective value, academics have come up with wildly different estimates for the value of certain services to people, and experts are likely to come up with differing values for other services as well. More generally, the idea of valuing personal information and it being disclosed in a general fashion will bear no relation to the actual value of the data. The actual value of personal data will be highly variable, based not just on the specific business but also larger market considerations. For example, the value of data to a business is variable, particularly as the amount of data grows.[94] Depending on other variables in a given business arrangement, the value of the personal information could also vary widely.

Concerning free, ads-based services, personalized services, people don't give up or exchange data for their experience; instead the experience is made possible by data. This is an important distinction. Data is what 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 with people's data. It's that they make money by selling ads: 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.

Given the significant questions about how to generate a value for data and well-founded skepticism on whether any disclosed value for data will accurately inform consumers of information related to the transaction they are considering, there is not an adequate benefit to consumers to justify the corresponding burden to business. Needless to say, undertaking an entirely new process to generate a value of data for publication to consumers will require businesses to engage in work that is not required by the CCPA, will require substantial investigation to determine the most workable methodology among those approved in the Proposed Regulation, and new legal risks for potentially publishing a figure that is challenged.

The AGO should strike this provision and allow the plain language of the CCPA to guide business and regulatory enforcement efforts on whether financial incentive programs have an appropriate correlation of value to the consumer and value to the business.

IA Recommendation: Strike Section 999.337 in its entirety.

[94] https://www.nber.org/papers/w24334.pdf