CCPA Text of Modified Proposed AG Regulations
Discussion Draft: IA Comments

Internet Association ("IA") appreciates the opportunity to review and provide the Attorney General's Office ("AGO") feedback on the Text of Modified Regulations for the California Consumer Privacy Act ("CCPA") Regulations ("Modified 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.

This submission marks the third time IA has weighed in on the rulemaking process for CCPA. As expressed in IA's comments submitted during the initial 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 encouraged by the important clarifications and simplifications reflected in the Modified Regulations. However, many of IA's concerns remain about confusing and unnecessary new obligations for businesses that lack justification in the form of meaningful privacy protections for consumers.

It is critical that the final CCPA regulations create clarity regarding business obligations for compliance to fill the gaps in CCPA text, without requiring significant new actions that go beyond the Legislature's original intent for CCPA. This is particularly important now that CCPA has taken effect and enforcement will begin mere months after final regulations will be published.

---

[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).

Section I. General Comments

IA would like to reiterate some of the high level concerns previously raised in our comments to the initial Proposed Regulations as the changes in the Modified Regulations do not fully address these issues:

1. **The Modified Regulations introduce new requirements after the effective date of CCPA.**

The CCPA's provisions became operative on January 1, 2020 pursuant to Cal. Civil Code Section 1798.198(a). Enforcement actions may be brought beginning on July 1, 2020.[4] The has state that it 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. It seems unlikely that the final regulations will be ready in a time frame that allows adequate time for compliance before the enforcement date of July 1, 2020.

On January 1, 2020, months of planning culminated in the launch of numerous new privacy notices, opt-out links, and mechanisms for accessing, downloading, or deleting data as a result of the CCPA. Implementation of CCPA, however, was uneven and inconsistent as a result of drafting issues when CCPA was passed and the lack of regulations to guide and inform implementation. Now that the implementation of CCPA has been achieved, it is time to focus on making sure it works properly and fine tune implementation. It is not the time for Modified Regulations to introduce new requirements with little warning.

As IA noted in its comments to the Proposed Regulations, 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, many months, if not more than a year, 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

[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.

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 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]

While the Modified Regulations make important improvements to the Proposed Regulations, it is still the case that they create new obligations beyond those contemplated in the text of the CCPA.[9] IA reiterates its comments challenging the legal authority to impose new requirements through the regulations[10] and whether such requirements satisfy the thresholds of California administrative law.

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, [11] 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.

2. **The Modified 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.**

In IA's comments to the Proposed Regulations, numerous examples were given of the ways in which the Proposed Regulations introduce new requirements, beyond the scope of CCPA, for which there is no reasonable necessity, and/or fail to meet other requirements of California's statutes and regulations for administrative procedure.[12] Many of the examples cited in IA's

[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 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 Modified Proposed Regulations.
[10] *See* Section II, *infra*, for arguments that new requirements exceed the AGO's authority.
[11] Cal. Gov. Code § 11349(a).
[12] 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

comments remain in the Modified Proposed Regulations and are noted below in Section II. Specific Provisions, including obligations to accept notice of a consumer request to opt-out of sale via device or browser settings; to monitor not just "designated methods" for consumers to make requests, but all potential methods; to track and report publicly on metrics related to consumer requests; to calculate value of consumer data and disclose that in connection with financial incentives; and more.

IA Recommendation: The AGO should substantially revise the Modified 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 Modified Proposed Regulations,[13] a new ISOR that appropriately considers reasonable alternatives,[14] and a new SRIA based on accurate understandings of the business impact of the regulations where they deviate from the requirements of the CCPA.[15]

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

The Modified 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.

---

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."

[13] 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).

[14] Cal. Gov. Code § 11346.2(b)(4).

[15] 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).

IA Recommendation: The AGO should substantially revise the requirements of the Modified Proposed Regulations to remove unnecessary burdens on business and to ensure that consumers benefit from.

Section II. Specific Provisions of Modified Proposed Regulations

§ 999.301 Definitions

- **(a) "Affirmative Authorization"** requires that consumers undergo a two-step process to indicate and then confirm their request to opt-in to sale. 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 Modified 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 to opt-in to the sale of their personal data. 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.[16] To avoid these results, the Modified 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 the right to opt-in to sale, rather than prescribing a specific two-step process in each regulatory provision addressing methods for opting in to the sale of personal information.

  IA Recommendation: Revise the definition of "affirmative authorization" to read, "means an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information. ~~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~~

[16] *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).

~~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.~~"

- **(h) "Household"** as defined in the Modified Proposed Regulations, in combination with Section 999.318, is improved but still 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.

- **(l) "Price or service difference"** please see discussion of this definition and IA's recommendation for Section 999.337.

999.305 Notice at collection

- **The Modified Proposed Regulations expand the purpose of the Notice of Collection and require that it be linked to on any webpage where personal information is collected, thus requiring multiple privacy notices to be linked to from a single page.** *See* 999.305(a)(3)(a). It is unclear how having a "Notice at Collection" link and a "Privacy Policy" link on each page where personal information is collected benefits consumers, since the information in the Notice at Collection is included within the privacy policy.
- **The Modified Proposed Regulations create a just-in-time disclosure requirement that does not match the concern raised.** Modified Proposed Regulation Section 999.305(a)(4) would require a business that is collecting one piece of personal information that the consumer does not reasonably expect to provide a disclosure providing a summary of every category that is collected. This notice would not be parallel with the unexpected collection and would undermine the Modified Regulations directive for businesses to take reasonable steps to provide meaningful notice to consumers.
- **The Modified Proposed Regulations contradict and enlarge CCPA provisions regarding new purposes for processing personal information.** Modified Proposed Regulation Section 999.305(a)(5) maintains the new requirement introduced via the Proposed Regulations 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 provision has been updated to modify new purposes with the term "materially," this language still 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 or a minor under 16 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 stated,

> *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 reasonably relied on the information provided in the notice at collection when interacting with the business.*[17]

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.[18] 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: IA recommends that subdivision 999.205(a)(4) be revised to require businesses to take steps to provide a meaningful understanding of the processing activity that triggered the requirement to provide just-in-time notice.

Further, IA recommends that the second sentence of 999.305(a)(5) be revised to, "If the business seeks to use a consumer's previously collected personal information for a purpose materially different than what was 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~~."

999.306 Notice of Right to Opt-Out

- **Subdivision (f) introduces the new "Opt-out Button" which has the potential to cause consumer confusion.** The button looks like a toggle that consumers are likely familiar with using to set their preferences in online services or mobile applications. However, the button's only functionality is as a link to a page where the consumer may learn how to exercise their right to opt-out. Consumers familiar with this symbol could be confused into thinking that clicking on the button (which looks like a toggle but which is not a toggle) has some effect. In addition, due to the size requirements for the button and the requirement to have the button accompanied by text, the use of image is likely to take up considerable space on a webpage or mobile screen. Thus, it is unlikely that use of the button will become widespread in electronic applications.

[17] ISOR, p. 8.
[18] *Id.*

Outside of the context of online or app-based services, the toggle button icon makes even less sense as a means to quickly communicate to consumers that they have the ability to opt-out.

IA Recommendation: Continue work to refine the "button" or "logo" to ensure that consumers are able to recognize the purpose of that it symbolizes, are not confused as to its function, and will be able to understand its meaning in all contexts in which it may appear.

999.307 Notice of Financial Incentive

- **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(c)(1)(C) Privacy Policy

- **Subdivision (c)(1)(C))(5) Privacy Policy Disclosures.** The Modified Proposed Regulations would require a business to describe the process it will use to verify the consumer request in its privacy policy disclosure. The processes and information required to verify a consumer's request may need to be changed or upgraded quickly to address emerging security concerns but privacy policies cannot be changed or upgraded as fast.

  IA Recommendation: Allow businesses to disclose a link to the company's current process for verifying requests in its privacy policy instead of describing the entire process.

999.312 Methods for submitting requests to know and delete

- **Section 999.312 diverges from CCPA's clear requirements regarding designated methods for submitting consumer requests.** The Modified Proposed Regulations deviate from CCPA by disregarding the entire concept of "designated methods" for exercising consumer rights. Subdivision (e) 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.[19] This requirement 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. For exclusively online businesses, it is also unclear how

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

this provision interacts with subdivision (a) which states that such a business, if it has a direct relationship with the consumer, "shall only be required to provide an email address for submitting requests to know." Given that subdivision (a) was added to implement A.B. 1564, 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.

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 (e) 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.

When this potentially endless array of channels of communication are combined with the training mandate in the Modified 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 (e) is broader than necessary to the extent it imposes requirements on how businesses respond to requests submitted outside of designated methods.

IA Recommendation: Revise Section 999. 312 by striking subdivision (e) 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(e) 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. In 2019, 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.[20] 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.

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

IA Recommendation: IA reiterates its recommendation that subdivision (e) 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 Modified 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. These hyper detailed, specific disclosures duplicate information available via a request to know for specific pieces of information and more general information available in the privacy policy. For example, detailing for each category of personal information each business purpose for which that category of information was disclosed or each category of third party to whom it was sold, but on a customized basis for that specific consumer does not add any information which is not otherwise available via specific pieces of data or from the general information in the privacy policy. This subdivision has no equivalent in any privacy regime, is hugely burdensome, has no corresponding consumer benefit, and is completely unnecessary when a consumer is accessing the actual information.

  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. <u>If the consumer also requested specific pieces of information and the business discloses specific pieces of information, the business is not required to respond to the request for categories of personal information.</u> 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."

- (c)(10) Strike the subdivision as it requires disclosures of categories, including categories of sources, categories of parties to whom the business has disclosed information to by broken out by category of information collected when the consumer is receiving the actual information.
- (c)(11) Clarify that a business has "provide[d] consumers a meaningful understanding of the categories listed" if it has used the language specifically enumerated in the CCPA or the regulations.

- **Subdivision (c)(1) creates risks of inappropriate disclosure of information about a consumer in response to an unverified consumer request.** The Modified 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 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 regulations 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 Modified 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.

Importantly, creating obligations in response to *unverified* requests is contrary to, and inconsistent with, the statute. The CCPA contemplates that unverified requests should be *discarded* precisely because they are unverified: "A business is not obligated to provide information to the consumer pursuant to Sections … 1798.105 … if the business cannot verify … that the consumer making the request is the consumer about whom the business has collected information …" Practically, the very reason a business should discard an unverified request is to protect the consumer—the business is unable to verify the individual's identity and therefore should not act on requests related to that consumer's personal information. And the statute creates a specific mechanism for opting-out of the sale of information. Collapsing verification and opt-out procedures is contrary to the statute and creates vectors for abuse.

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).~~

The deletion of the language of the Proposed Regulations related to security in Subdivision (c)(3) causes concerns about requests to know that adversely impact the rights of other consumers and the security of businesses. Subdivision (c)(3) stated, "[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." This language served as an important protection for businesses that have legitimate concerns that responding to a request to know from a consumer, for example a consumer that defrauded other consumers, could create security risks for other users, individuals, or the business. This provision was clearly in line with CCPA's directive that access requests shall not "adversely affect the rights and freedoms of other consumers."[21] This limitation on the obligations under the CCPA should be reflected in this subdivision of the Modified Proposed Regulations and the original language of the Proposed Regulations retained.

Subdivision (c)(3) creates privacy and security concerns, is overly restrictive, and creates undue burdens for business. The right to know requires a business to disclose to the consumer personal information the business has "collected about that consumer." The statute requires the AGO to promulgate regulations for access requests that "tak[e] into account," inter alia, "security concerns, and the burden on the business." § 1798.185(a)(7). Subdivision (c)(3) properly recognizes that not all personal information a business has about a consumer need be made available. We agree with AGO that access cannot be absolute, for example, it should not apply when a business does not maintain the personal information in a searchable or reasonably accessible format, or when the business maintains the personal information solely for legal or compliance purposes. We appreciate and agree with the recognition that an absolute access requirement is not desirable or consistent with privacy best practices. The proposed provision, however, is too restrictive, does not recognize other important limitations to access, does not sufficiently limit the scope of the right to know to information the business has "collected," and does not recognize security concerns or undue burdens. As currently drafted, subdivision (c)(3) contemplates a four-part test for which, in practice, no information will meet all four prongs—particularly given the requirement that the information be maintained "solely for legal or compliance purposes." For example, information could be held by a business purely for legal compliance purposes, such as pursuant to a preservation request from law enforcement in anticipation of obtaining a court order, but if it is maintained in a "reasonably accessible format" in order to be disclosed to law enforcement once served with an order, this information would be subject to the access request even if it is only stored in a manner accessible to personnel who review and respond to law

[21] Cal. Civ. Code § 1798.145(j).

enforcement requests. Functionally, the four part test is too rigid to limit the scope of access requests.

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

A regulation drawing clearer lines regarding the scope of the right to know will have pro-privacy and pro-security ramifications and will save businesses from having to face significant burdens and legal uncertainty. IA's following recommendation draws a clearer line while properly taking into account the statutory limitation that the business must have "collected" the personal information, and the statutory requirements the regulations consider burden and security.

IA Recommendation: IA recommends retaining and 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, or consumers."

Specifically, IA recommends that subdivision (c)(3) be amended to the following:

> A business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems, networks, or consumers. In responding to a request to know, a business is not required to provide personal information that meets any of the following conditions, provided the business describes to the consumer the categories of records that may contain personal information that it did not provide it because it meets one of the conditions stated below:

a. The business does not maintain the personal information in a searchable or reasonably accessible format;
b. The business maintains the personal information solely for legal or compliance purposes;
c. The business does not sell the personal information and does not use it for any commercial purpose.
d. The business does not associate the personal information with a consumer in the ordinary course of business; or
e. The personal information was not collected from the consumer or a third party, but was instead derived internally by the business

- **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) adds new requirement that should be removed.** This subdivision would require that for any consumer making a deletion request, if a business cannot verify the consumer's identity, the business must "ask the consumer if they would like to opt-out of the sale of their personal information and shall include either the contents of, or al link to, the notice of right opt-opt out in accordance with section 999.206." This conflates the consumer expectations between opt-out requests and requests to delete. Further, it would have businesses combine two different request flows.

  IA Recommendation: Remove the requirement of an opt-opt prompt for consumers who cannot be verified during a deletion request. Alternatively, allow businesses to link to the privacy policy disclosure so consumer's who cannot be identified in a deletion request can find information on how to exercise all of their privacy rights.

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).[22] 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~~, 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. 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 (d) 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) in conflict and inconsistent with the statute, 2) not necessary; 3) beyond the authority of the AGO's rulemaking mandate; 4) it has not been adequately justified in the ISOR; 5) the financial impact was not adequately considered in the SRIA; and 6) 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 Modified Proposed Regulations require "an interactive webform accessible via a clear and

[22] 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.

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 Modified 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.
- The Modified Regulations continue to conflate the CCPA's "Do Not Sell" requirements with tangentially related Do Not Track settings. 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."[23] This makes it harder, not easier, for consumers.

- The proposed regulation is therefore contrary to and inconsistent with the statutory text and purpose, and creates significant uncertainty and vagueness for both consumers and businesses regarding the opt-out right. They also exceed the delegation of authority to the AGO, as the statute instructs the AGO to :facilitate" opt-out requests and to promote "the development and use of a recognizable and uniform opt-out logo" -not to create *new ways* in which to characterize a consumer's behavior as an opt-out request.

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 global privacy controls, such as a browser plugin or privacy setting, device 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 (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. Businesses must provide notice to consumers 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 essentially providing criminals with blueprints as to how to get around their fraud detection systems and protocols.

[23] 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 Modified 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.

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.[24] 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).

- **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.**

[24] *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 provisions of subdivision (g) are vague. First, the definition of "commercial purposes" in the CCPA is extremely broad.[25] This term is seldom used in the CCPA or in the Modified 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 Modified Proposed Regulations' approach to "designated methods" for submitting requests and the inclusion of browser signals and other automated controls as "requests" to opt-out.
- Alternatives to the recordkeeping and publication requirements in the Modified 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 require businesses to maintain internal documentation of compliance with CCPA's requirements that would be available for review as a part of an enforcement investigation.
- 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 Modified 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 Modified 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 final CCPA

[25] Cal. Civ. Code § 1798.140(f).

regulations 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 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 or clarify what rights a consumer may have regarding personal information collected while they were a member of household once they leave the household.
  - This section of the Modified Proposed Regulations should be revised to tie "household" to a shared account, such as an account that specifically allows sub-accounts for spouses or children and for which all parties to the account will have notice of the potential that other household members participating in the account may be able to access information related to the use of the account.
  - 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 Modified 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 Modified 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.[26] 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 Modified 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 Modified 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.[27] Under COPPA and the COPPA Rule, new approved methods for parental consent may become available in the future and

[26] Cal. Civ. Code § 1798.135(c).
[27] *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.")

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."[28] 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 Modified 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.[29]

  IA Recommendation: Revise subdivision (a)(1) to read, "A business that has actual knowledge that it sells 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 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 Modified 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

[28] ISOR, p. 34.
[29] 15 U.S.C. § 6502(d).

"created by this title."[30] Where the California Legislature wanted to incorporate future provisions created by AGO rulemaking in CCPA, it did so with specific language.[31] 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 Modified 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.

  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

[30] *See* Cal. Civ. Code § 1798.125(a)(1).
[31] *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").

value of data to a business is variable, particularly as the amount of data grows.[32] 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.

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