

From: [REDACTED]
To: [Privacy Regulations](#)
Subject: Comment on proposed CCPA regulation revisions
Date: Friday, December 11, 2020 12:55:18 PM

§999.306(b)(3): I applaud the proposed revisions to (b)(3). This is a significant, useful clarification and is substantially less unreasonably onerous than the originally proposed language. **A welcome improvement.**

§999.306(f): This new insertion, by contrast, is about as clear as mud, and is ill-conceived.

First, the proposed button adds nothing in terms of clarity about opt-out rights. The graphic looks like a stylized gelatin capsule covered with cryptic markings. **The average consumer is unlikely to grasp the intended significance of the graphic**, or to recognize that the button has anything to do with privacy or opting-out of the sale of their personal information.

For consumers who use screen readers or other assistive technologies, the proposed button will be either invisible or confusing. If the graphic has an ALT tag, which WWCAG 2.0 calls for all but purely decorative images to have for accessibility purposes, the likely contents of that ALT tag would either duplicate the “Do Not Sell My Personal Information” text, which is annoying for assistive technology users, or say something different than the text (e.g., “Opt-Out”), which may be confusing and would muddle the intended clarity of the phrase “Do Not Sell My Personal Information.”

In sum, this graphic is ugly and unhelpful; I don’t believe that the button is in any way clearer than the phrase “Do Not Sell My Personal Information” that is already separately required; and for vision-impaired users, it may actually be LESS clear.

Second, **the wording of this provision makes it unclear if use of the proposed button is intended to be mandatory:** (f)(1) suggests that it is optional (“may be used in addition to posting”), while (f)(2) implies that it MUST be used in addition to and as part of any Do Not Sell My Personal Information link (“Where a business ... shall be added”). I am genuinely uncertain which interpretation your office intends, which is a bad choice for a regulation intended to “promote consumer awareness.”

I would strongly oppose any move to make this ugly, ill-conceived button graphic mandatory as part of the already-required Do Not Sell My Personal Information (DNSMPI) link. In addition to the points noted above, use of the graphic may be impractical or infeasible in a variety of contexts where the link might reasonably be presented — for example, in a bullet-pointed list in a sidebar menu on a web page, or in the footer of an email message. (Not all email clients support the use of graphics within the body or footer of an email message, so the graphic would simply be stripped out in plain-text messages anyway.) Furthermore, since (f)(1) does make clear that the button must be used in addition to the phrase “Do Not Sell My Personal Information,” adding the button would

exacerbate the problem with fitting the link's required anchor text into space-restricted contexts (such as on the settings menu of mobile app or in the narrow sidebar of a website template intended for mobile users) without making it unreadably small or partly cut off. That would serve no one.

Making such a button mandatory would also present yet another arbitrary technical headache for businesses that have already made a good-faith effort to comply with the regulatory requirements. (Indeed, I would question OAG's good faith in promulgating an additional compliance requirement in a set of regulatory revisions that will be seen only by a limited audience and which has a public comment period of only 18 calendar days.)

If the intent is simply to make this graphic (or some hopefully less ugly and less cryptic variant) optional, or optional and encouraged, the proposed text should make that clearer.

§999.315(h): I was dismayed and disheartened to see that OAG has made no attempt whatever to address the problems I previously broached with regard to this proposed addition.

First, let me reiterate that I appreciate the overall intent of this section to discourage businesses from "burying" their opt-out requirements or obfuscating them with confusing language. I don't have a fundamental problem with that goal.

That said, several of the specific provisions OAG has inserted create a series of confusing, arbitrary, impractical, and ultimately unenforceable requirements, which remain unchanged in the current revision.

First among these is §999.315(h)(1), which seeks to impose a specific arbitrary standard for the acceptable number of steps or clicks to opt-out. **This is frankly nonsensical, particularly in view of the additional requirements created by the proposed §999.306(b)(3).** Consider: a brick-and-mortar business such as a grocery store, which sells personal information gathered from consumers in the store in connection with the use of a store "club card." Opting-in may be as simple as taking the new card from an employee and swiping it at the POS terminal. The process of subsequently opting-out would certainly require more steps than that; at a minimum, the consumer would need to provide their club card number (so that the opt-out request is correctly applied to their account) and then indicate their desire to opt-out by pressing or otherwise indicating the desired option.

Similarly, consider a web-based business that runs online advertising and also collects logged-in visitors' email addresses for a mailing list that is also sold to third parties. The online advertising is configured to respond to Global Privacy Control browser settings, so that visitors who send an opt-out signal are not shown advertising that collects personal information, while logged-in visitors can separately opt-out of the sale of their email addresses. In the first case, the visitor's opt-in or opt-out preference is communicated by the browser signal, which requires no clicks at all, and may not provide the website with enough information to individually identify that visitor. In the second case, the visitor would reasonably need to submit an opt-out request that provides their name and email address so that the business may correctly process the request. Under the proposed 999.315(h)(5), the business would be expected to enable consumers to submit the second type of opt-out request using no more clicks than the first (which in this example would be no clicks at all). **That's obviously**

absurd, and completely impracticable.

Again, I recognize and appreciate the desire to discourage opt-out procedures that require an unreasonable number of steps, but the way this provision is worded and its ludicrous demand for parity in situations that are clearly not directly equivalent suggests that whoever wrote this proposed §999.315(h)(1) has simply not thought through the onerous and confusing expectations it creates. I think you're trying to square the circle here, and I see no way to revise this subparagraph to achieve your desired end without the ridiculous and unreasonable problems the present version creates. **I still believe §999.315(h)(1) should be deleted in its entirety from these proposed revisions.**

The other absurd and arbitrary provision here remains §999.315(h)(5), which seeks to require that a consumer not have to "scroll or search" through a webpage to find opt-out instructions.

As I expressed in my previous public comment, I appreciate that the intent is to discourage "burial" of the opt-out instructions, but the wording you've proposed would have the effect of *prohibiting* ANY scrolling, which again is absurd. How much scrolling may be required to reach specific text on a given webpage is directly dependent on the dimensions of the user's browser window, monitor, or mobile device screen, which is completely outside the control of the website's operators. **Even if a business has a separate Do Not Sell My Personal Information page containing clear, reasonably concise instructions for submitting an opt-out request, reaching those instructions may require some scrolling if the page is accessed on a mobile phone.** To the person who wrote this paragraph, I must ask: How big is YOUR phone's screen? My own mobile device has a screen size of 5 inches, measured diagonally (and my previous phone's screen was smaller still), so many webpages that would require little or no scrolling or searching on my desktop will have me scrolling madly away when accessed from my phone. Even on a desktop, if I reduce the size of my browser window and/or enlarge the text for easier reading, it will significantly increase the amount of scrolling involved in reading a particular page or section of a page, even a short one.

That's beyond the control of the websites I visit, and it doesn't necessarily connote any bad faith on their part as regards these regulations; it is simply a plain reality of the physical dimensions of Internet-capable devices and web browsers. Under this proposed rule, such a website would be in technical violation of these regulations and could be legally penalized for it — madness! Similarly, a business could be penalized for technical errors, such as an anchor link that fails to correctly resolve, which is not at all reasonable.

My objections to §999.315(h)(5) could be mitigated through the addition of qualifiers such as "to an excessive or unreasonable degree" to the proposed text. (What is "unreasonable" or "excessive" is obviously a subjective judgment, but so is most of the proposed §999.315(h).) Failing that, 315(h)(5) should be deleted in its entirety. Once again, I understand what you're trying to achieve here, but the writer(s) of this section have not considered the implications of the often-clumsy wording.

I sincerely hope that this time, OAG will take these concerns into consideration prior to finalizing the proposed revisions.

[REDACTED]

[REDACTED]

[REDACTED]

From: [Maureen Mahoney](#)
To: [Privacy Regulations](#)
Subject: CR Comments on Fourth Set of Modifications to the CCPA Regulations
Date: Wednesday, December 23, 2020 10:07:33 AM
Attachments: [CR Comments on 4th Set of Modifications to the CCPA.pdf](#)

Hello,

Attached, please see Consumer Reports' comments on the Fourth Set of Modifications to the CCPA Regulations. Please let me know if you have any questions.

Best,
Maureen

--

Maureen Mahoney, Ph.D.

Policy Analyst

m [REDACTED]

Pronouns: she/her/hers

[CR.org](https://www.consumerreports.org)



This e-mail message is intended only for the designated recipient(s) named above. The information contained in this e-mail and any attachments may be confidential or legally privileged. If you are not the intended recipient, you may not review, retain, copy, redistribute or use this e-mail or any attachment for any purpose, or disclose all or any part of its contents. If you have received this e-mail in error, please immediately notify the sender by reply e-mail and permanently delete this e-mail and any attachments from your computer system.



December 23, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Re: Fourth Set of Modifications to Regulations Implementing the California Consumer Privacy Act (CCPA)

Dear Ms. Kim,

Consumer Reports¹ appreciates the opportunity to comment on the Fourth Set of Modifications to the CCPA Regulations.² We thank the California Attorney General's office (AG) for proposing new regulations to help to make the CCPA work better for consumers. Though the California Consumer Privacy Act (CCPA) is designed to protect consumer privacy, Consumer Reports has found that some consumers ran into difficulties when attempting to opt out of the sale of their information under the CCPA.³ The new proposed rules will help address some—though not all—of these problems. To better ensure that consumers are able to exercise their privacy rights, we reiterate our comments submitted in response to the Third Set of Modifications (attached),⁴ and additionally, recommend that the AG:

¹ Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

² California Attorney General, California Consumer Privacy Act Regulations, Text of Modified Regulations (Dec. 10, 2020), <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-prop-mods-text-of-regs-4th.pdf>.

³ Maureen Mahoney, *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?*, CONSUMER REPORTS DIGITAL LAB (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf.

⁴ Maureen Mahoney, Consumer Reports Comments on the Third Set of Modifications to Proposed Regulations Implementing the California Consumer Privacy Act (Oct. 28, 2020), <https://advocacy.consumerreports.org/research/cr-comments-on-the-third-set-of-modifications-to-proposed-regulations-implementing-the-ccpa/>.

- Finalize the proposed opt-out button design;
- More clearly require companies that sell personal information to include the opt-out button on their homepages, along with the “Do not Sell My Personal Information” link;
- Clarify that if an authorized agent inadvertently submits a request incorrectly, the company must either accept it or inform the agent how to submit it appropriately; and
- Clarify the definition of sale and tighten the restrictions on service providers, to ensure that consumers can opt out of cross-context targeted advertising.

Consumers’ activity online is constantly tracked, and information about their most personal characteristics sold without their knowledge or consent. At the very least, consumers should be able to effectively opt out of the sale of their personal information to third parties. The following reforms, if adopted, will better ensure that consumers are able to do so.

The AG should finalize the proposed opt-out button design.

Consumer Reports has documented that consumers often find it difficult to locate Do Not Sell links on data brokers’ homepages. In our recent study, *California Consumer Privacy Act: Are Consumers’ Digital Rights Protected?*, over 500 consumers submitted Do Not Sell requests to approximately 200 companies on the California Data Broker Registry. Each company was tested by at least three study participants. We found that for 42.5% of sites tested, at least one of three testers was unable to find a DNS link. All three testers failed to find a “Do Not Sell” link on 12.6% of sites, and in several other cases one or two of three testers were unable to locate a link.

In some cases, the opt-out links simply weren’t there; in others, the links were difficult to find. Follow-up research focused on the sites in which all three testers did not find the link revealed that at least 24 companies on the data broker registry did not have the required DNS link on their homepage. All three testers were unable to find the DNS links for five additional companies, though follow-up research revealed that the companies did have DNS links on their homepages. Still, this also raised concerns, since the CCPA requires companies to post the link in a “clear and conspicuous” manner.⁵ If consumer testers who are actively searching for DNS links have difficulty finding them on the homepage, it’s hard to imagine that the everyday consumer will find them.

Thus, we recommend that the AG finalize the opt-out button design as proposed. We appreciate the work that went into developing the opt-out button, which reflects the design and approach recommended by Professor Lorrie Cranor and her colleagues, based on their research.⁶ The

⁵ Cal. Civ. Code §1798.135(a)(1).

⁶ Lorrie Faith Cranor et al., *Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA* at 32 (Feb. 4, 2020), <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cranor-design-eval-usable-icon.pdf>.

proposed opt-out button should help draw the consumer's eye to the Do Not Sell link.⁷ After the button is adopted and placed on homepages, we urge the AG's office to continue to work with researchers, academics, advocacy organizations, and companies in evaluating the efficacy of the design and update if needed to ensure that it is useful for consumers.

The AG should more clearly require companies that sell personal information to post the opt-out button on their homepages, along with the “Do not Sell My Personal Information” link.

Unless use of the button is required, it is unlikely that enough companies will adopt it. We therefore appreciate that the AG has proposed to require companies that sell personal information to post the opt-out button alongside the “Do Not Sell My Personal Information” link on the homepage.⁸ But while we think it is clear that the proposed language in §999.306(f)(1)-(3) requires companies selling personal information to post the button on their homepages, some observers have a different interpretation, that posting of the button is optional.⁹ An optional interface would counter the direct instructions in the CCPA, for the AG to issue rules “For the development and use of a recognizable and uniform opt-out logo or button *by all* businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.”¹⁰ [emphasis added]

To help eliminate any uncertainty that the opt-out button is required, we propose the following tweak to the proposed language:

f) Opt-Out Button. (1) The following opt-out button ~~may~~ **shall** be used in addition to posting the notice of right to opt-out, ~~but~~ **and** not in lieu of any requirement to post the notice of right to opt-out or a “Do Not Sell My Personal Information” link as required by Civil Code section 1798.135 and these regulations. (2) Where a business posts the “Do Not Sell My Personal Information” link, the opt-out button shall be added to the left of the text as demonstrated below. The opt-out button shall link to the same Internet webpage or online location to which the consumer is directed after clicking on the “Do Not Sell My Personal Information” link. (3) The button shall be approximately the same size as any other buttons used by the business on its webpage.

Without more clearly establishing that use of the opt-out button is required on the homepage, it is likely that companies will disregard it. Standardized notice is important to making CCPA

⁷ Lorrie Faith Cranor et al., *CCPA Opt-Out Icon Testing - Phase 2* at 2, 23 (May 28, 2020), <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/dns-icon-study-report-052822020.pdf>.

⁸ Text of Modified Regulations, *supra* note 2, at §999.306(f)(1)-(3).

⁹ See, eg, @JulesPolonetsky, Twitter (Dec. 10, 2020), <https://twitter.com/JulesPolonetsky/status/1337116699548667907>.

¹⁰ Cal. Civ. Code § 1798.185(a)(4)(C).

disclosures meaningful for consumers. And widespread adoption of the button should better ensure that consumers can more easily opt out of the sale of their personal information.

The AG should clarify that if an authorized agent inadvertently submits a request incorrectly, the company must either accept it or inform the agent how to submit it appropriately.

The CCPA's authorized agent provisions, which allow consumers to designate an authorized agent to submit access, deletion, and opt-out requests on their behalf, are crucial to making the CCPA more workable for consumers.¹¹ Instead of submitting hundreds, if not thousands of requests to different companies in order to exercise their privacy preferences, which could end up taking almost as much time as a full-time job, the consumer can simply delegate authority to a third party. Consumer Reports, seeking to help make it easier for consumers to exercise their CCPA rights, has been conducting a study of the authorized agent provision and has submitted opt-out requests on behalf of about one hundred California consumers.¹² (We expect to publish the results of our findings early next year).

Our research has shown that some companies do not clearly describe in their privacy policies the correct methods to submit authorized agent requests—as is required by the CCPA regulations.¹³ It can be difficult for the authorized agent to know the company's preferred process, creating uncertainty as to whether the requests have been honored.

To help address this problem, the AG should require that when an authorized agent inadvertently submits a request through a method not accepted by the company, that the company shall either accept the request or instruct the authorized agent with the correct method of submission. The AG regulations already require companies to treat consumers' verifiable requests in this manner;¹⁴ these protections should be extended to authorized agents, for all requests.

The AG should clarify the definition of sale and tighten the restrictions on service providers, to ensure that consumers can opt out of cross-context targeted advertising.

Finally, in the course of submitting opt-out requests on behalf of consumers, we learned about more companies that claimed that they did not “sell” information under the CCPA, though they shared it with third parties for cross-context targeted advertising.

¹¹ Cal. Civ. Code § 1798.135(a)(1); § 1798.185(a)(7).

¹² Ginny Fahs, *Putting the CCPA into Practice: Piloting a CR Authorized Agent*, Digital Lab at Consumer Reports (Oct. 19, 2020),

<https://medium.com/cr-digital-lab/putting-the-ccpa-into-practice-piloting-a-cr-authorized-agent-7301a72ca9f8>.

¹³ Cal. Code Regs. tit. 11 § 999.308(c)(5) (2020).

¹⁴ *Id.* at 999.312(e).

We reiterate the request from our previous comments to clarify that these data transfers are covered by the CCPA's definition of sale,¹⁵ and to close up exemptions in the service provider exemption that companies have exploited.¹⁶ The CCPA places next to no restrictions on first-party collection and use of data, but it seeks to give consumers control over third-party use of their personal information without their permission. The newly-passed California Privacy Rights Act (CPRA) removes all doubt that these transfers are covered,¹⁷ but those provisions will not go into effect for another two years.¹⁸ Consumers should not have to wait two more years to be able to adequately protect their privacy. We urge the AG to close the loopholes in the definition of sale and service provider without delay.

Conclusion

Thank you for the opportunity to comment on the Fourth Set of Proposed Modification to the CCPA. Please do not hesitate to reach out if you have any questions.

Respectfully submitted,



Maureen Mahoney
Policy Analyst

Attachment

¹⁵ Consumer Reports Comments on the Third Set of Modification to Proposed Regulations Implementing the California Consumer Privacy Act, *supra* note 4, at 7.

¹⁶ *Id.* at 8-9.

¹⁷ See, California Privacy Rights Act, § 1798.120(a); § 1798.140(e)(6), https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.

¹⁸ *Id.* at § 1798.185(d).



October 28, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Re: Third Set of Modifications to Proposed Regulations Implementing the California Consumer Privacy Act (CCPA)

Dear Ms. Kim,

Consumer Reports¹ appreciates the opportunity to submit comments in response to the Notice of the Third Set of Modifications to Proposed Regulations Implementing the California Consumer Privacy Act.² We welcome these proposed changes, especially those prohibiting the use of dark patterns—methods that substantially interfere with consumers’ efforts to opt out of the sale of their information.³ Consumer Reports has recently documented that some consumers are finding it very difficult to opt out of the sale of their information.⁴ In our recent study, over 500 consumers submitted opt-out requests to companies listed on the California data broker registry. Many of them encountered challenges: opt-out links too often were missing from the home page or difficult to find; opt-out processes were unnecessarily complicated, and companies asked consumers to submit sensitive information to verify their identities. In response, consumers sent over 5,000 messages to the AG, urging him to step up enforcement efforts and close up

¹ Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers’ interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

² California Attorney General, California Consumer Privacy Act Regulations, Text of Modified Regulations (Oct. 12, 2020), <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-third-set-mod-101220.pdf>.

³ *Id.* at §999.315(h)(1)-(5).

⁴ Maureen Mahoney, *California Consumer Privacy Act: Are Consumers’ Rights Protected?*, CONSUMER REPORTS (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf.

loopholes in the CCPA that companies have exploited. The guidance on opt outs, including the prohibition on dark patterns, in this latest proposal will go a long way to addressing these problems. But more work is needed to ensure that consumers can properly exercise their privacy rights. We recommend that the AG:

- Finalize the proposed guidance on opt outs, including the prohibition on dark patterns;
- Finalize a design for the opt-out button;
- Require companies to confirm that they have honored opt-out requests;
- Finalize the authorized agent provisions as proposed;
- Close up loopholes in the definition of sale and tighten protections with respect to service providers, to ensure that consumers can opt out of behavioral advertising;
- Clarify that financial incentives in markets that lack competition is an unfair and usurious practice; and
- Establish a non-exclusive list of browser privacy signals that shall be honored as a universal opt out of sale.

Below, we explain these points in more detail.

The AG should finalize the proposed guidance on opt outs, including the prohibition on dark patterns.

We appreciate that the AG has proposed to “require minimal steps to allow the consumer to opt-out” and to prohibit dark patterns, in other words, “a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer’s choice to opt-out.”⁵ These regulations are essential given the difficulties that consumers have experienced in attempting to stop the sale of their information.

Subverting consumer intent online has become a real problem, and it’s important to address. In response to Europe’s recent GDPR privacy law, many websites forced users through confusing consent dialogs to ostensibly obtain consent to share and collect data for any number of undisclosed purposes.⁶ And researchers increasingly have been paying attention to manipulative dark patterns as well. A 2019 Princeton University study of 11,000 shopping sites found more than 1,800 examples of dark patterns, many of which clearly crossed the line into illegal deception.⁷

⁵ § 999.315(h).

⁶ *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy*, NORWEGIAN CONSUMER COUNCIL (Jun. 27, 2018), <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>.

⁷ Mathur, Arunesh and Acar, Gunes and Friedman, Michael and Lucherini, Elena and Mayer, Jonathan and Chetty, Marshini and Narayanan, Arvind, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, Proc. ACM Hum.-Comput. Interact. (2019), <https://webtransparency.cs.princeton.edu/dark-patterns/>.

Use of these dark patterns is already illegal under Unfair and Deceptive Acts and Practices (UDAP) law, but that hasn't been adequate to protect consumers from these deceptive interfaces. For example, the Federal Trade Commission (FTC) sued Age of Learning, an online education service for children, for its deceptive interface that led consumers to believe they were signing up for one year of service, when in fact, by default, they were charged each year.⁸ Attorney General Karl Racine of the District of Columbia recently filed suit against Instacart for using a deceptive interface that made a service fee look like a tip.⁹ Last year, the FTC alleged that Match.com tricked consumers into subscribing by sending them misleading advertisements that claimed that someone wanted to date them—even though many of those communications were from fake profiles.¹⁰ Similarly, in late 2016, the FTC took action against Ashley Madison for using fake profiles to trick consumers into upgrading their membership.¹¹ The FTC took action against Facebook in 2011 for forcing consumers to use a deceptive interface to get them to provide so-called “consent” to share more data.¹² Despite these enforcement actions, the use of dark patterns remains all too common. Given how widespread these interfaces are, it's important to explicitly clarify that they are illegal in the CCPA context.

The proposed rules appropriately rein in the number of allowable steps to opt out.

We appreciate that the proposed rules limit the number of allowable steps in the opt-out process.¹³ As we noted in our recent study, some “Do Not Sell” processes involved multiple, complicated steps to opt out, including downloading third-party software, raising serious questions about the workability of the CCPA for consumers. For example, the data broker Outbrain doesn't have a “Do Not Sell My Personal Information” link on its homepage. The

⁸ Fed. Trade Comm'n v. Age of Learning, Inc., Complaint for Permanent Injunction and Other Equitable Relief, Case No. 2:20-cv-7996. U.S. District Court Central District of California at 4-6 (Sept. 1, 2020), <https://www.ftc.gov/system/files/documents/cases/1723086abcmousecomplaint.pdf>. According to the FTC, this is a UDAP violation. See ¶ 57.

⁹ District of Columbia v. Mapbear, Inc. d/b/a Instacart, Complaint for Violations of the Consumer Protection Procedures Act and Sales Tax Law, Superior Court of the District of Columbia at ¶ 2 (Aug. 2020), <https://oag.dc.gov/sites/default/files/2020-08/Instacart-Complaint.pdf>. The AG alleged that “Instacart’s misrepresentations and omissions regarding its service fee constitute deceptive and unfair trade practices that violated D.C. Code § 28-3904.” See ¶ 86.

¹⁰ Fed. Trade Comm'n v. Match Group, Inc., Complaint for Permanent Injunction, Civil Penalties, and Other Relief, Case No. 3:19-cv-02281, U.S. District Court, Northern District of Texas, Dallas Division at 2 (Sept. 25, 2019), https://www.ftc.gov/system/files/documents/cases/match_-_complaint.pdf. According to the FTC, this is a Section 5 violation. See p. 20-21.

¹¹ Fed. Trade Comm'n v. Ruby Corp. et al, Complaint for Permanent Injunction and Other Equitable Relief, Case 1:16-cv-02438, United States Circuit Court for the District of Columbia at 6 (Dec. 14, 2016), (<https://www.ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf>). According to the FTC, this is a Section 5 violation. See p. 13-14.

¹² Fed. Trade Comm'n, In the Matter of Facebook Inc. at 5-6 (2011) <https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf>. According to the FTC, this is a Section 5 violation. See p. 19.

¹³ § 999.315(h)(1).

consumer can click on the “Privacy Policy” link at the bottom of the page, which sends the consumer through at least six different steps in order to opt out of the sale of their information on that device. (The consumer can cut out several steps by clicking on “Interest-Based Ads” on the homepage.) If a consumer would like to opt out on their phone, they would have to go through another process. And if the consumer clears their cookies, they would need to opt out again. As one consumer told us, “It was not simple and required reading the ‘fine print.’” The proposed rules should help address this problem.

The proposed rules correctly prohibit companies from asking for unnecessary information to opt out.

We also appreciate the guidance that opt-out processes “shall not require the consumer to provide personal information that is not necessary to implement the request.”¹⁴ In our study, participants reported that they gave up the opt-out request 7% of the time. The overwhelming reason for a consumer to refrain from part of a DNS request process, or give up all together, was not feeling comfortable providing information requested. Out of the 68 reports that the tester chose not to provide information they were asked for as part of the process, 59 said it was because they were not comfortable doing so. For example, nearly all consumers declined to provide a photo in order to process their opt-out requests. Out of 7 instances in which consumers reported that they were asked to provide a photo selfie, in 6 the consumer declined.

Consumers told us that they were just as averse to providing government IDs. One tester of Searchbug reported: “I hated having to send an image of my Driver License. I thoroughly regret having done so. It feels like an invasion of privacy to have to do that, just so I can take steps to PROTECT my privacy. Feels wrong and dirty.” Even consumers that ended up providing the drivers’ license ended up confused by the company’s follow-up response. One tester of Hexasoft Development Sdn. Bhd. responded: “After sending them a copy of my California driver license to satisfy their residency verification, I got an email back which simply stated that ‘[w]e will update the ranges in the future release.’ I have no idea what that means.” Out of 17 reports of being asked for an image of a government ID, in 10 the consumer chose not to. Out of 40 reports of being asked to provide a government ID number, in 13 the consumer refrained from providing it.

This information is clearly not necessary, as most data brokers simply requested name, address, and email. Unnecessary collection of sensitive data has significantly interfered with consumers’ ability to exercise their rights under the CCPA, and we appreciate that the proposed rules explicitly prohibit this.

¹⁴ § 999.315(h)(4).

The draft rules correctly stop businesses for making consumers search through a privacy policy to opt out.

We are also pleased that the draft rules preclude businesses from requiring consumers to dig through privacy policies to opt out.¹⁵ In our study, in some cases, consumers proactively reported finding language surrounding the DNS request link and process excessively verbose and hard to understand. For example, one tester reported of the data broker US Data Corporation, “There is a long, legalistic and technical explanation of how and why tracking occurs, not for the faint of heart.” Another said of Oracle America, “The directions for opting out were in the middle of a wordy document written in small, tight font.” Another found the legal language used by Adrea Rubin Marketing intimidating: “they seemed to want to make the process longer and unnecessarily legalese-y, even a bit scary--under threat of perjury.”

Another data broker, ACBJ, placed a “Your California Privacy Rights” link at the bottom of their homepage (rather than a “Do Not Sell My Personal Information” link), which led to their privacy and cookie policy.¹⁶ Once on the policy page, the consumer is forced to search in their browser for the phrase “Do Not Sell My Personal Information” or scroll and scan ten sections of the privacy policy to find the paragraph with a “Do Not Sell My Personal Information” link, or follow two additional links to navigate from the privacy policy table of contents to the “Do Not Sell My Personal Information” link. Upon clicking the “Do Not Sell My Personal Information” link, the consumer is shown a pop-up with a page of additional legal information, and then has to scroll down to a toggle that finally allows them to request their data not be sold. In light of these reports from consumers, we urge the AG to finalize the prohibition on these practices.

The AG should finalize a design for the opt-out button.

Given that many consumers found it difficult to find the Do Not Sell link—it was often labeled with something different, and often buried at the bottom of the page with other links—a standardized graphic button would likely have value in ensuring that consumers would take advantage of that privacy protection. The CCPA directs the AG to design an opt-out button: “a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt out of the sale of personal information.”¹⁷ While the original design came under a fair amount of criticism, a uniform button will likely help consumers seeking to opt out, and the AG should promulgate one as soon as possible.

¹⁵ § 999.315(h)(5).

¹⁶ ACBJ (last visited Oct. 28, 2020), <https://acbj.com/privacy#X>.

¹⁷ Cal. Civ. Code § 1798.185(a)(4)(C).

The AG should require companies to confirm that they have honored opt-out signals.

In our study, many consumers had no idea whether or not their opt-out request had been honored. The uncertainty often left consumers dissatisfied with the opt out. Some companies did notify consumers that their requests had been honored, and this information was characteristic of simple, quick, and effective opt-out processes.

Only in 18% of requests did participants report a clear confirmation from the broker that their data was or would soon not be sold. In 46% of tests, participants were left waiting or unsure about the status of their DNS request. In the 131 cases where the consumer was still waiting after one week, 82% were dissatisfied with the process (60% reported being very dissatisfied, and 22% reported being somewhat dissatisfied). The lack of clarity and closure was reflected in consumer comments such as “left me with no understanding of whether or not anything is going to happen” and “While it was an easy process—I will read their privacy policy to see if there is more [I] have to do to verify they are complying with my request. They left me unsure of the next step.”

The AG should approve the proposed adjustment to the authorized agent provisions.

The authorized agent provisions are an essential part of the CCPA, and Consumer Reports has recently launched a pilot program to perform opt-out requests on consumers’ behalf.¹⁸ The CCPA puts far too much burden on individuals to safeguard their privacy; being able to designate an authorized agent to act on consumers’ behalf can help reduce that burden. The draft regulations support the work of authorized agents submitting access, deletion, and opt-out requests on consumers’ behalf, while ensuring that consumers’ privacy and security is protected.

While the CCPA pointedly does not require identity verification for opt-out requests, access and deletion requests have strong identity verification requirements. The regulations make it appropriately clear that a business may require additional identity verification, but not if the authorized agent can present proof that it holds a power of attorney from the consumer.¹⁹ If multiple companies required a consumer to submit additional identity verification, the authorized agent provision would no longer be practical for consumers. Obtaining a single power of attorney is easier and more efficient than going through many identity verification steps. Industry standards and standard form powers of attorney will make access and deletion pragmatic for the consumer, like the authorized agent opt-out process is currently.

¹⁸ Ginny Fahs, *Putting the CCPA Into Practice: Piloting a CR Authorized Agent*, DIGITAL LAB AT CONSUMER REPORTS (Oct. 19, 2020), <https://medium.com/cr-digital-lab/putting-the-ccpa-into-practice-piloting-a-cr-authorized-agent-7301a72ca9f8>.

¹⁹ § 999.326(b)

The regulations also require companies to honor valid opt-out requests from an authorized agent unless they have a “good-faith, reasonable, and documented belief that a request to opt-out is fraudulent.”²⁰ With these guidelines, an authorized agent that uses industry-standard verification of a consumer’s email address or telephone number will be able to complete an opt out without requiring consumers to provide hundreds, if not thousands, of verifications. This language allows companies to reject fraudulent opt outs without putting additional verification burdens on a consumer using a legitimate authorized agent.

The AG should clarify the definition of sale and tighten protections with respect to service providers, to ensure that consumers can opt out of behavioral advertising.

Many tech companies have exploited ambiguities in the definition of sale and the rules surrounding service providers to ignore consumers’ requests to opt out of behavioral advertising.²¹ Companies such as Spotify and Amazon claim that they are not “selling” data and that consumers can’t opt out of these data transfers—even though they share it with their advertising partners.²² Some companies claim that because data is not necessarily transferred for money, it does not constitute a sale.²³ But addressing targeted advertising is one of the main goals of the CCPA, which has an inclusive definition of personal information and a broad definition of sale to cover transfers of data for these purposes.²⁴

Given the extent of the non-compliance, the AG should exercise its broad authority to issue rules to further the privacy intent of the Act,²⁵ and clarify that the transfer of data between unrelated companies for any commercial purpose falls under the definition of sale. This will help ensure that consumers can opt out of cross-context targeted advertising. We suggest adding a new definition to § 999.301:

“Sale” means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s

²⁰ § 999.315(g)

²¹ Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously—The Attorney General Needs to Act*, DIGITAL LAB AT CONSUMER REPORTS (Jan. 9, 2020), <https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb>.

²² Spotify, “Additional California Privacy Disclosures,” (July 1, 2020), <https://www.spotify.com/us/legal/california-privacy-disclosure/?language=en&country=us>; Amazon.com Privacy Notice,” (January 1, 2020), https://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496&ref_=footer_privacy#GUID-8966E75F-9B92-4A2B-BFD5-967D57513A40__SECTION_FE2374D302994717AB1A8CE585E7E8BE.

²³ Tim Peterson, *‘We’re Not Going to Play Around’: Ad Industry Grapples with California’s Ambiguous Privacy Law*, DIGIDAY (Dec. 9, 2019), <https://digiday.com/marketing/not-going-play-around-ad-industry-grapples-californias-ambiguous-privacy-law/>.

²⁴ Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley—And Won*, N.Y. TIMES (Aug. 14, 2018), <https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html>; Cal. Civ. Code § 1798.140(o); Cal. Civ. Code § 1798.140(t).

²⁵ Cal. Civ. Code § 1798.185(a).

personal information by the business to another business or a third party for monetary or other valuable consideration, or otherwise for a commercial purpose.

Another common way for companies to avoid honoring consumers' right to opt out of behavioral advertising is by claiming a service provider exemption. For example, the Interactive Advertising Bureau (IAB), a trade group that represents the ad tech industry, developed a framework for companies to evade the opt out by abusing a provision in the CCPA meant to permit a company to perform certain limited services on its behalf.²⁶

To address this problem, the AG should clarify that companies cannot transfer data to service providers for behavioral advertising if the consumer has opted out of sale. We reiterate our calls for a new .314(d):

If a consumer has opted out of the sale of their data, a company shall not share personal data with a service provider for the purpose of delivering cross-context behavioral advertising. "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal Information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

Additionally, the AG should take action to stop companies from combining data across clients. Service providers should be working on behalf of one company at a time. Allowing companies to claim that they're just service providers for everyone swallows the rules and lets third parties amass huge, cross-site data sets. The AG has appropriately removed language in an earlier draft, which held that service providers can merge data across clients. But in the absence of a specific prohibition, given its disregard for the FTC consent order, Facebook (and other companies) will likely continue to engage in this behavior. The AG needs to make clear that this is not acceptable. We suggest the following language:

A service provider may not combine the personal information which the service provider receives from or on behalf of the business with personal information which the service provider receives from or on behalf of another person or persons, or collects from its own interaction with consumers.

²⁶ *IAB CCPA Compliance Framework for Publishers & Technology Companies*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2019), https://www.iab.com/wp-content/uploads/2019/12/IAB_CCPA-Compliance-Framework-for-Publishers-Technology-Companies.pdf.

Google and Facebook provide app developers privileged, valuable information—your data—in return for services that help increase engagement with their platforms.²⁷ The AG should refine the regulations in order to give consumers more control over their data with respect to these practices.

The AG should clarify that financial incentives in markets that lack competition is an unfair and usurious practice.

Californians have a right to privacy under the California Constitution, and consumers shouldn't be charged for exercising those rights. Unfortunately, there is contradictory language in the CCPA that could give companies the ability to charge consumers more for opting out of the sale of their data or otherwise exercising their privacy rights.²⁸

To prevent some of the worst abuses associated with financial incentives, discriminatory treatment should be presumed where markets are consolidated and consumers lack choices. The CCPA prohibits financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.²⁹ And, the AG currently has the authority under the CCPA to issue rules with respect to financial incentives.³⁰ Thus, we urge the AG to exercise its authority to prohibit the use of financial incentives in market sectors that lack competition. ISPs, for example, should not be allowed to charge consumers for exercising their privacy rights, because customers lack the meaningful opportunity to find more affordable options elsewhere. For example, for years, AT&T charged usurious rates—about \$30 per month—for not leveraging U-Verse data for ad targeting.³¹ Where consumers have few choices, market forces don't impose sufficient constraints on companies from penalizing exercising privacy rights. And, there is rising concentration across many industries in the United States,³² further highlighted by the creation of a Federal Trade Commission task force to monitor these trends.³³ The AG should exercise its authority to put reasonable limits on these programs in consolidated markets.

²⁷ Chris Hoofnagle, *Facebook and Google Are the New Data Brokers* (Dec. 2018), https://hoofnagle.berkeley.edu/wp-content/uploads/2018/12/hoofnagle_facebook_google_data_brokers.pdf.

²⁸ Cal. Civ. Code §§ 1798.125(a)(2) and .125(b).

²⁹ *Id.* at § 1798.125(b)(4).

³⁰ *Id.* at § 1798.185(a)(6).

³¹ Jon Brodtkin, *AT&T To End Targeted Ads Program, Give All Users Lowest Available Price*, ARS TECHNICA (Sept. 30, 2016), <https://arstechnica.com/information-technology/2016/09/att-to-end-targeted-ads-program-give-all-users-lowest-available-price/>.

³² *Too Much of a Good Thing*, THE ECONOMIST (March 26, 2016), <https://www.economist.com/briefing/2016/03/26/too-much-of-a-good-thing>.

³³ *FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets*, Fed. Trade Comm'n (Feb. 26, 2019), <https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology>.

The AG should clarify a non-exclusive list of browser privacy signals that shall be honored as a universal opt out of sale.

We appreciate that the AG has maintained the requirement that companies must honor browser privacy signals as an opt out of sale.³⁴ Forcing consumers to opt out of every company, one by one is simply not workable. However, the current rules should be adjusted to ensure that it is consumer-friendly. The AG should state that platform-level controls to limit data sharing should be interpreted as CCPA opt outs, including Do Not Track and Limit Ad Tracking. Or at the very least, the AG should clarify how platforms can certify that new or existing privacy settings should be construed as CCPA opt outs.

To encourage the development and awareness of, and compliance with, privacy settings for other platforms, we reiterate our request that the AG to issue rules governing: 1) how the developer of a platform may designate a particular privacy control to be deemed a valid request; 2) how the attorney general shall maintain and publish a comprehensive list of privacy controls to be deemed valid requests; and 3) the conditions under which business may request an exception to sell data notwithstanding a consumer's valid request.

Millions of consumers have signed up for Do Not Track, but there are other settings that are far less well-known, in part because they're not associated with online use. For example, Apple, in 2013 introduced a mandatory "Limit Ad Tracking" setting for iPhone applications, and recently improved that tool to further limit the information advertisers can receive when the setting is activated.³⁵ Consumers also need global opt outs from sale when using their smart televisions and voice assistants. In order to better raise awareness of the different options on the market, to encourage the development of new tools, and to address the lack of clarity around which browser settings must be honored as opt outs, the AG should set up a system in order to make this clear for consumers and businesses.

Additionally, it would be helpful to provide guidance outside of the rule that signals such as the Global Privacy Control—a new, CR-supported effort to create a "Do Not Sell" browser signal³⁶—are likely to be considered binding in the future.

Conclusion

The proposed rules, particularly the guidance on opt-out requests, will help rein in some of the worst abuses of the opt-out process. But more needs to be done in order to ensure that the CCPA

³⁴ § 999.315(c).

³⁵ Lara O'Reilly, *Apple's Latest iPhone Software Update Will Make It A Lot Harder for Advertisers to Track You*, BUS. INSIDER (Sept. 10, 2016), <http://www.businessinsider.com/apple-ios10-limit-ad-tracking-setting-2016-9>.

³⁶ Press release, *Announcing Global Privacy Control: Making it Easy for Consumers to Exercise Their Privacy Rights*, Global Privacy Control (Oct. 7, 2020), <https://globalprivacycontrol.org/press-release/20201007.html>.


is working as intended. We look forward to working with you to ensure that consumers have the tools they need to effectively control their privacy.

Respectfully submitted,

Maureen Mahoney
Policy Analyst
Consumer Reports

From: [Steven K. Hazen](#)
To: [Privacy Regulations](#)
Subject: OAL File No. 2019-1001-05 (comment on Fourth Set of Proposed Modifications to Text of CCPA Regulations)
Date: Wednesday, December 23, 2020 8:30:14 PM
Attachments: [SKHazen Comment on 4th Proposed Regs CCPA \(Dec 23 2020\).pdf](#)

Attached: comment letter by Steven Kelsey Hazen addressing the above referenced announcement and rule making by the Department of Justice.

Steven Kelsey Hazen, Esq.
149 South Barrington Avenue, #245
Los Angeles, CA 90049-3310


December 23, 2020

VIA EMAIL: *PRIVACYREGULATIONS@DOJ.CA.GOV*

Lisa B. Kim, Esq.
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

re Fourth Set of Proposed Modifications to Text of CCPA Regulations
OAL File No. 2019-1001-05

Dear Ms. Kim:

This letter is provided in response to the announcement dated December 10, 2020 of the above-referenced proposed modifications to Regulations promulgated by the Department of Justice pursuant to the California Consumer Privacy Act (the “CCPA”). In that context, I draw your attention to the text of proposed new section (f) of § 999.306 (“Notice of Right to Opt-Out of Sale of Personal Information”). Specifically, there appears to be some confusion as between part (1) and parts (2) and (3), or even contradiction of the former by the latter.

The proposed text of part (1) makes it clear that use of the identified “button” is voluntary: it “may be used in addition to posting the notice of right to opt-out, but not in lieu of ...” complying with requirements of Civil Code section 1798.135 and the regulation implemented under the CCPA. By contrast, the proposed text of parts (2) and (3) might be understood as making use of such button mandatory: “the button shall be added ...” [part (2)]; “button shall be approximately the same size ...” [part (3)]. In each case, the underlining in the quoted text is added for purposes of highlighting the comparison.

In order to be consistent with the provisions of part (1), I suggest that part (2) be modified so that reference in the first sentence of it to “the opt-out button” instead read as follows: “the opt-out button (if used)”. Similarly, I suggest that the first four words of part (3) currently reading “The button shall be” instead read as follows: “The button (if used) shall be”. Making these changes will avoid potential confusion by parties subject to the provisions of the CCPA and the Regulations adopted under them.

Respectfully submitted,

/s/

Steven Kelsey Hazen

From: [Dylan Hoffman](#)
To: [Privacy Regulations](#)
Subject: Internet Association Comments on Fourth Modified CCPA Regulations
Date: Thursday, December 24, 2020 7:47:02 AM
Attachments: [IA Comments on 4th Modified CCPA Regs 12.24.20.pdf](#)

Hi,

Please find attached comments from Internet Association on the Third Modified CCPA Regulations. If you have any questions please let me know.

Best,

--



Dylan Hoffman

Director of California Government Affairs

INTERNET ASSOCIATION

1303 J Street, Suite 400, Sacramento, CA 95814



December 24, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
Email: PrivacyRegulations@doj.ca.gov

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.

IA hopes to continue working with the AGO’s office to clarify these regulations. We are encouraged by some of the recent proposals in the latest Modified Regulations, but have some constructive feedback around certain provisions within the proposed language.

IA COMMENTS

General

As we noted in our comments to the Third Set of Proposed Modifications to CCPA Regulations, IA member companies are concerned about the continuous nature of the CCPA regulations process. We appreciate the AGO doing its part to protect consumers and clarify or provide guidance for some of the confusing language within the CCPA. However, adding new requirements—as these modifications do—makes compliance more difficult for businesses and negatively impacts consumers’ abilities to exercise their rights under the law. While we are supportive of the AGO’s goal to provide greater clarity, closing the door on the rulemaking process for a period of time will allow businesses to implement the current regulations and regulators to identify the true challenges within the new rules.

999.306 (f)

There are several issues with the proposed modifications for an opt-out button and IA respectfully requests that subsection (f) be removed from the proposed modified regulations for the following reasons.

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_fulldoc / (last accessed November 25, 2019).



- **Section 999.306 (f) (1-2)**

- **The interplay between proposed (f)(1) and (f)(2) language is difficult to interpret for both businesses and will ultimately negatively impact consumers.** First, (f)(1) states that the opt-out button may be used in **addition** to posting the notice of right to opt-out, but not “in lieu of” the requirements to post the notice of right to opt-out or the “Do Not Sell My Personal Information” link. Alternatively, subsection (f)(2) seems to require the opt-out button to be added to the left of the “Do Not Sell My Personal Information” link where a business posts it, thus implying that the button is not in fact an optional addition, but instead a requirement.

These conflicting subsections create confusion for both consumers and businesses alike. Businesses looking to comply with the CCPA will suffer from not having a clear standard for implementing their tools to allow consumers to opt out. Consumers will also not be able to identify if they have truly opted out of their personal information being sold with so many different options and links between a “Do Not Sell My Personal Information” button, an opt out toggle, and the language contained in the privacy policy. IA supports the AGO’s goals to have clear and easy to use functions when it comes to consumers actively controlling their personal data, but these provisions do not allow for a consistent and workable standard. Therefore, IA recommends either (1) providing further explanation and clarity to these subsections or (2) removing these proposed modifications to the CCPA.

- **Subsection (f)(2)’s location requirement for the opt out button does not take into account the various mediums of the internet ecosystem.** The provision requires the button next to the “Do Not Sell My Personal Information” link and that it must link to the same notice of right to opt out page as the “Do Not Sell My Personal Information” link. The potential value this button may provide is outweighed by the fact that websites often have limited space, which is especially true for mobile-optimized sites and within mobile apps. In certain circumstances it may be impossible to add this image next to the “Do Not Sell My Personal Information” link in the app’s Settings page, or on the app’s download page of the app store.
- **The proposed opt-out button design is impractical for businesses and consumers.** The proposed button image with a check mark and an “X” mark next to each other is confusing for consumers. It is not easy to identify which mark indicates a consumer has opted out of the sale of their personal data or whether the consumer has taken any action based on the toggle design. Further, the toggle design is not a choice for opting in or opting out for the consumer, but instead a repetitive link for the same place as the “Do Not Sell My Personal Information” button. IA believes this button should be modified in some way from its current design due to (1) the unclear intent of the design and (2) the redundancy of the button, which could cause confusion for consumers wishing to opt out of the sale of their information.

- **Section 999.306 (f)(3)**

- Finally, the requirement in (f)(3) that the opt-out button be “the same size as any other buttons” is similarly confusing. Button sizes are often inconsistent across different pages and between websites, mobile-optimized pages, and mobile apps. It’s unclear whether the button should be the same size as other buttons on that particular page or across multiple pages of a website. This requirement is difficult for businesses to interpret and is likely to result in



inconsistent compliance at best and an impossible standard at worst.

999.315 (h)

- **Section 999.315 (h)(1-5)**

- These sections are intended to provide illustrative examples of how businesses should make requests to opt-out easy for consumers to execute. While the examples are intended to provide clarity, they are framed in a statutory “shall not” form, implying that businesses must comply with their prescriptions.
- IA would recommend the following suggestions below that are inspired by the six verification considerations set forth in section 999.323 (b)(3). Under the aforementioned section, the regulations present the format of a consideration and how a business should apply that consideration. Using this format provides businesses with greater clarity and guidance about how to design and process consumer requests to opt-out.

- **(h)(3)**

- IA member companies are concerned about the current language of (h)(3) limiting businesses’ ability to provide more transparency to consumers. As currently drafted, this subsection could potentially inhibit companies from providing additional context and information to consumers about how they protect and use consumer data. We would recommend that the AGO review this language and IA’s recommendations below to provide consumers with the ability to fully understand the implications of choosing to opt-out prior to making their decision.
- Furthermore, IA is concerned that (h)(3) may raise compelled speech issues, as it would prohibit companies from providing consumers with additional information about the implications of their opt-out.
- IA member companies would encourage the AGO to consider adopting a reasonableness standard, as noted below, for what information companies can provide to consumers during the opt-out decision process. Our companies would like to supply pertinent and reasonable information to consumers to help them make informed decisions about the use of their personal information.

- **IA Suggested Text Alterations:**

- (h) A business’s methods for submitting requests to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out. A business shall not use a method that is designed with the purpose ~~or has the substantial effect~~ of subverting or impairing a consumer’s choice to opt-out. A business shall consider the following factors when creating processes for requests to opt-out: ~~Illustrative examples follow:~~
 - (1) The number of steps included in t~~he~~ business’s process for submitting a request to opt-out as compared to the number of steps included in the~~shall not require more steps than that~~ business’s process for a consumer to opt-in to the sale of personal information after having previously opted out. The number of steps for submitting a



request to opt-out ~~should be~~ measured from when the consumer clicks on the “Do Not Sell My Personal Information” link to completion of the request. The number of steps for submitting a request to opt-in to the sale of personal information ~~should be~~ measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request. The number of steps included in the business’s process for submitting a request to opt-out should not unreasonably exceed the number of steps included in the business’s process for a consumer to opt-in to the sale of personal information after having previously opted out.

- (2) ~~Whether the business uses~~ ~~A business shall not use~~ confusing language, such as double-negatives (e.g., “Don’t Not Sell My Personal Information”), when providing consumers the choice to opt-out. The business should avoid using confusing language such as double-negatives.
- (3) ~~Whether a business unreasonably requires~~ ~~Except as permitted by these regulations, a business shall not require~~ consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request. The business should avoid unreasonably requiring consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request, except as permitted by these regulations.
- (4) ~~Whether t~~he business’s process for submitting a request to opt-out ~~shall not~~ requires the consumer to provide personal information that is not necessary to implement the request. The business should avoid requiring consumers to provide personal information that is not necessary to implement the request to opt-out.
- (5) ~~Whether, u~~pon clicking the “Do Not Sell My Personal Information” link, the business ~~shall not~~ requires the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out. The business should avoid requiring consumers to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out.

Respectfully,

A handwritten signature in black ink, appearing to read "Dylan Hoffman".

Dylan Hoffman
Director of California Government Affairs
Internet Association

From: [Monticollo, Allaire](#)
To: [Privacy Regulations](#)
Cc: [Signorelli, Michael A.](#)
Subject: Joint Ad Trade Comments on Fourth Set of Proposed Modifications to Text of CCPA Regulations
Date: Sunday, December 27, 2020 11:05:12 AM
Attachments: [FINAL Joint Ad Trade Comments on Fourth Set of Modifications to CCPA Regulations.pdf](#)

Dear Privacy Regulations Coordinator:

Please find attached joint comments from the following advertising trade associations on the content of the fourth set of proposed modifications to the text of the California Consumer Privacy Act regulations: the Association of National Advertisers, the American Association of Advertising Agencies, the Interactive Advertising Bureau, the American Advertising Federation, the Digital Advertising Alliance, and the Network Advertising Initiative.

If you have any questions about these comments, please feel free to reach out to Mike Signorelli at

Best Regards,
Allie Monticollo

[Allaire Monticollo, Esq. | Venable LLP](#)
t [REDACTED] | f 202.344.8300
600 Massachusetts Avenue, NW, Washington, DC 20001
[REDACTED] | www.Venable.com

This electronic mail transmission may contain confidential or privileged information. If you believe you have received this message in error, please notify the sender by reply transmission and delete the message without copying or disclosing it.



December 27, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

RE: Fourth Set of Proposed Modifications to Text of California Consumer Privacy Act Regulations

Dear Privacy Regulations Coordinator:

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies, from small businesses to household brands, across every segment of the advertising industry. We provide the following comments to the California Office of the Attorney General ("OAG") on the fourth set of proposed modifications to the text of the California Consumer Privacy Act ("CCPA") regulations.¹

The undersigned organizations' combined membership includes more than 2,500 companies, is responsible for more than 85 percent of U.S. advertising spend, and drives more than 80 percent of our nation's digital advertising expenditures. Locally, our members are estimated to help generate some \$767.7 billion dollars for the California economy and support more than 2 million jobs in the state.²

For more than a year, our members have been communicating with consumers about their CCPA rights and how to effectuate them. As a result, our members have experience in operating under the CCPA and interacting with consumers. We have learned valuable insights about how to support consumer privacy rights under this new legal regime, including that operational flexibility is vital.

Not all interactions with consumers are the same nor are all business operations. There is no "one-size fits all" approach to the CCPA. We and our members strongly support the underlying goals of the CCPA, and we believe consumer privacy deserves meaningful protections in the marketplace. However, as discussed in our previous comment submissions and in this letter, the draft regulations implementing the CCPA should be updated to provide greater clarity, better enable consumers to exercise informed choices, and help businesses in their efforts to continue to provide value to Californians and support the state's economy.³

¹ See California Department of Justice, *Notice of Fourth Set of Proposed Modifications to Text of Regulations and Addition of Documents and Information to Rulemaking File* (Dec. 10, 2020), located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-4th-set-mods.pdf>.

² IHS Economics and Country Risk, *Economic Impact of Advertising in the United States* (Mar. 2015), located at <http://www.ana.net/getfile/23045>.

³ Our organizations have submitted joint comments throughout the regulatory process on the content of the OAG's proposed rules implementing the CCPA. See *Joint Advertising Trade Association Comments on California Consumer Privacy Act Regulation*, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-45day-comments.pdf> at CCPA 00000431 - 00000442; *Revised Proposed Regulations Implementing the California Consumer Privacy Act*, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-15day-comments-set1.pdf> at CCPA_15DAY_000554 - 000559; *Second Set of Proposed Regulations Implementing the California Consumer Privacy Act*, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-45day-comments.pdf> at CCPA_2ND15DAY_00309 - 00313; *Third Set of Proposed Regulations Implementing the California Consumer*

Companies and consumers have been adapting to the “Do Not Sell My Personal Information” tagline for more than a year. This effort has included refashioning digital properties, as well as instituting backend processes to meet the compliance requirements of the CCPA even as a new ballot initiative, the California Privacy Rights Act (or “Proposition 24”), was moving forward. These most recent proposed modifications by the OAG to the CCPA regulations set forth ambiguous terms surrounding a proposed online button almost a full year after the law went into effect. Among other things, this round of modifications fails to clarify whether the button is optional or mandatory. The proposed changes also do not leave room for the deployment of alternative icons, such as the CCPA Privacy Rights Icon in market provided by the Digital Advertising Alliance (“DAA”),⁴ or other methods, such as a text only link in applicable scenarios, to facilitate consumers’ right to opt out of personal information sales. The OAG should reconsider these provisions, or at the very least clarify them so businesses can take steps to comply with the new terms as soon as possible.

Additionally, changes the OAG made during the third set of proposed modifications to the CCPA regulations set forth a prescriptive interpretation of the law that could limit businesses’ ability to support employment in California and the state’s economy during these unprecedented times. We reassert the issues we previously raised with those provisions in this submission. As explained in more detail in the sections that follow below, the OAG’s potential changes to Section 999.315 would inhibit consumers from receiving transparent information and impinge on businesses’ right to free speech. In addition, the proposed modifications to Section 999.326 would not provide any protections for consumers related to their communications with authorized agents, as such agents are not presently held to similar consumer notice rules as businesses. Finally, the OAG’s proposed edits to Section 999.306 regarding offline notice of the right to opt out could stymie the flexibility businesses need to provide effective offline notices to consumers. We consequently ask the OAG to strike or modify these changes per the below comments.

Our members are committed to offering consumers robust privacy protections while simultaneously providing them with access to ad-funded news, apps, and a host of additional online services. These are offerings we have all become much more dependent on in recent months with the widespread proliferation of the COVID-19 pandemic. Ad-supported online content and services have been available to consumers and will continue to be available to consumers so long as laws allow for innovation and flexibility without unnecessarily tilting the playing field away from the ad-subsidized model. We believe a regulatory scheme that offers strong individual privacy protections and enables continued economic advancement will best serve Californians. The suggested updates we offer in this letter would improve the CCPA regulations for Californians as well as protect the economy.

I. The Regulations Should Clarify That the Proposed New Button is Discretionary and Not Preclude Use of Other Icons Presented in Conjunction with the Text Link

In the fourth set of proposed modifications to the CCPA regulations, the OAG reinserted terms setting forth a specific graphic for a button enabling consumers to opt out of personal information sales. The proposed modifications state that the proposed button “*may* be used” in addition to posting a notice of the right to opt-out online, but not in lieu of such notice or the “Do Not Sell My Personal Information” link.⁵ In the very next subsection, the proposed rules state that when a business provides a “Do Not Sell My Personal Information” link, the proposed button “*shall* be added to the left” of the link.⁶ The language describing the proposed button is thus unclear, as it does not adequately explain whether providing the

Privacy Act, located at <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-written-comm-3rd-15-day-period.pdf> at CCPA_3RD15DAY_00111 - 00118.

⁴ DAA, *Opt Out Tools*, located at <https://www.privacyrights.info/>.

⁵ Cal. Code Regs. tit. 11, § 999.306(f)(1) (proposed Dec. 10, 2020) (emphasis added).

⁶ *Id.* at § 999.306(f)(2) (emphasis added).

button is discretionary or mandatory for businesses that sell personal information. We ask the OAG to confirm that the proposed button is discretionary as well as to provide flexibility for businesses to use alternative, industry-developed icons that signal the right to opt out of personal information sales to California consumers.

As the founding members of the DAA YourAdChoices program and corresponding icon,⁷ we understand the benefits a widely recognizable icon can bring to provide transparency and choices to consumers. In fact, in November 2019, the DAA announced its creation of a tool and corresponding Privacy Rights Icon to provide consumers with a clear and recognizable mechanism to opt out of personal information sales under the CCPA.⁸ Icons and corresponding privacy programs created by the DAA have a history of success. The YourAdChoices icon has been served globally at a rate of more than one trillion times per month, and its recognition continues to grow. In a 2016 survey, more than three in five respondents (61 percent) recognized the YourAdChoices icon at least a little, and half (50 percent) said they recognized it a lot or somewhat. For the CCPA, there is a need for flexibility in how this novel law is implemented in the market. The OAG should allow the marketplace to determine the best opt-out button approach, including allowing the option for use of an icon promulgated in relation to industry-driven opt-out mechanisms, rather than creating uncertainty by mandating a new graphic that businesses must use.

Moreover, adding the button as a requirement now, nearly a year after the CCPA became effective and more than five months after the OAG began enforcing the law, would create unnecessary new compliance costs for businesses to reconfigure websites and consumer-facing properties after they have already taken significant steps to update their practices per the CCPA's requirements. We therefore ask the OAG to clarify that the new opt-out button is discretionary rather than mandatory, and businesses that provide a "Do Not Sell My Personal Information" link are not required to also provide the proposed button. We also ask the OAG to provide flexibility for businesses to utilize other icons to signal a consumer's right to opt out of personal information sales, such as the DAA's CCPA Privacy Rights Icon. The OAG should reconsider the need to create new iconography and should instead partner with industry on the already existing DAA Privacy Rights Icon to help lead consumers to choices about how their personal information is used and shared.

II. The Regulations Should Support Consumers' Awareness of the Implications of Their Privacy Decisions, Not Hinder It in Violation of the First Amendment

The proposed online and offline modifications unreasonably limit consumers' ability to access accurate and informative disclosures about business practices as they engage in the opt out process. Ultimately, this restriction on speech would not benefit consumers or advance a substantial interest. The proposed rules state: "Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request."⁹ This language unduly limits consumers from receiving important information as they submit opt out requests. It is also overly limiting in the way that businesses may communicate with consumers. As highlighted above, data-driven advertising provides consumers with immensely valuable digital content for free or low-cost, as well as critical revenue for publishers, by increasing the value of ads served to consumers. As the research cited above also confirms, consumers have continually expressed their preference for ad-supported digital content and services, rather than having to pay significant fees for a wide range of apps, websites, and internet services they use. However, as a result of the proposed modifications, consumers' receipt of factual, critical information about the nature of the ad-supported

⁷ Digital Advertising Alliance, *YourAdChoices*, located at <https://youradchoices.com/>.

⁸ DAA, *Digital Advertising Alliance Announces CCPA Tools for Ad Industry* (Nov. 25, 2019), located at <https://digitaladvertisingalliance.org/press-release/digital-advertising-alliance-announces-ccpa-tools-ad-industry>.

⁹ Cal. Code Regs. tit 11, § 999.315(h)(3) (proposed Oct. 12, 2020).

Internet would be unduly hindered, thereby undermining a consumer’s ability to make an informed decision. A business should be able to effectively communicate with consumers to inform them about how and why their data is used, and the benefit that data-driven advertising provides as a critical source of revenue.

It is no secret that consumers greatly value the information they can freely access online from digital publishers. However, local news publishers, for instance, continue to struggle to get readers to pay subscription fees for their content, even though this content is highly valuable to consumers and society. Thus, most news publishers have become increasingly reliant on tailored advertising, because it provides greater revenue than traditional advertising.¹⁰ However, the proposed modifications, as drafted, could obstruct consumers from receiving truthful, important information by hindering a business’ provision of a reasonable notice to consumers about the funding challenges opt outs pose to their business model.

The CCPA regulations should not prevent consumers from receiving and businesses from providing full, fair, and accurate information during the opt out process. The proposed modification would impede consumers from receiving important information about their privacy choices, such as information about the vital nature of the ad-supported Internet, and, as explained in Section III, they may be contemporaneously receiving partial or misleading negative information about their opt out rights.

To ensure a fully informed privacy choice, consumers must have every ability to access information about business practices and the benefits of the digital advertising ecosystem. Providing ample and timely opportunities for consumers to gain knowledge about their choice to opt out is of paramount importance to avoid confusion and ignorance; this allows a consumer to be fully informed about the actual implications of their decision. By prohibiting a business from requiring a consumer “to click through or listen to reasons why they should not submit a request to opt-out *before* confirming their request” the regulations do not safeguard against this concern. As presently written, the proposed modification appears to limit businesses’ ability to provide such vital information as a consumer is opting out, even if such information is presented in a seamless way. It is unclear what amount of information, or what method in which such information is presented, could constitute a violation of the rules. Instead of setting forth prohibitive rules that could reduce the amount of information and transparency available to consumers online, the OAG should prioritize facilitating accurate and educational exchanges of information from businesses to consumers. As a result, we ask the OAG to revise the text of the proposed modification in Section 999.315(h)(3) so that businesses are permitted to describe the impacts of an opt-out choice while facilitating the consumer’s request to opt out.

Additionally, the restrictions created by this proposed modification infringe on businesses’ First and Fourteenth Amendment right to commercial speech. As written, Section 999.315(h)(3) restricts the information consumers can receive from businesses as they submit opt out requests by limiting the provision of accurate and truthful information to consumers. The Supreme Court has explained that “people will perceive their own best interest if only they are well enough informed, and . . . the best means to that end is to open the channels of communication, rather than to close them. . . .”¹¹ Because this proposed regulation prescriptively regulates channels of communication, it violates the First and Fourteenth Amendments.

The state may not suppress speech that is “neither misleading nor related to unlawful activity” unless it has a substantial interest in restricting this speech, the regulation directly advances that interest,

¹⁰ DAA, *Study: Online Ad Value Spikes When Data Is Used to Boost Relevance* (Feb. 10, 2014), located at <https://digitaladvertisingalliance.org/press-release/study-online-ad-value-spikes-when-data-used-boost-relevance>.

¹¹ *Virginia Pharmacy Board v. Virginia Citizens Consumer Council*, 425 U. S. 748, 770 (1976).

and the regulation is narrowly tailored to serve that interest.¹² The proposed regulation fails each part of the test:

- **No substantial interest:** Although there is no stated justification in the proposal, the most likely interest would be to streamline opt out requests by making it easier and faster to submit opt-outs. The OAG presumably wants nothing to impede consumers from opting out, but it is unclear because the OAG has not affirmatively stated its purpose for the proposed modification. Consumers should be made aware of the ramifications of their opt out decisions as they are opting out – not after confirming a request – so they do not make opt out choices to their detriment because they do not know the effect of such choices. For this reason, they should be able to receive information from businesses about the consequences of their opt out choices as they are submitting opt out requests. Providing information concerning the impact of an opt out is not an impediment to the process, but rather improves it.
- **No advancement of the interest:** If streamlining opt out requests to remove perceived impediments is the justification for the proposed rule, then the proposal does not advance that interest. The proposed regulation already includes many other specific requirements that facilitate speed and ease of opt-outs, including a requirement to use the minimal number of steps for opt-outs (and no more than the number of steps needed to opt in), prohibiting confusing wording, restricting the information collected, and prohibiting hiding the opt-out in a longer policy, all of which directly advance this interest without suppressing speech. The proposed rule limiting businesses from clicking through or listening to reasons would not make the opt out process easier for consumers, because it could result in consumers making uninformed choices if they are not notified of the consequences of their decision to opt out as they are making it. A “regulation may not be sustained if it provides only ineffective or remote support for the government’s purpose.”¹³ This proposed regulation is both ineffective and provides no support for the government’s purpose.
- **Not narrowly tailored:** The proposed regulation is an overly broad and prescriptive restriction on speech that hinders accurate and educational communications to consumers about the consequences of a decision to opt-out. The regulations already include various other provisions that work to streamline the opt out process. “[I]f the governmental interest could be served as well by a more limited restriction on commercial speech, the excessive restrictions cannot survive.”¹⁴ As noted above, there are many ways to craft regulations to require simple and fast opt-out mechanisms that do not suppress lawful and truthful speech.

In sum, the regulation violates each and every prong of the framework for evaluating commercial speech. “As in other contexts, these standards ensure not only that the state’s interests are proportional to the resulting burdens placed on speech but also that the law does not seek to suppress a disfavored message.”¹⁵ The proposed regulation would do exactly that. Thus, it is a content-based restriction on speech, subject to heightened scrutiny. The U.S. Supreme Court has made clear that the burden is on the government to justify content-based restrictions on lawful speech, and the failure to even state a basis for this restriction fails to meet this requirement.¹⁶ The OAG should revise the text of the proposed

¹² *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980); *see also Individual Reference Services Group, Inc. v. F.T.C.*, 145 F. Supp. 2d 6, 41 (D.D.C. 2001).

¹³ *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980).

¹⁴ *Id.*

¹⁵ *Sorrell v. IMS Health Inc.*, 564 U.S. 572, 565 (2011).

¹⁶ *E.g., Reed v. Town of Gilbert*, 576 U.S. 155, 171 (2015) (citing *Arizona Free Enter. Club’s Freedom Club PAC v. Bennett*, 564 U.S. 721 (2011)).

modification in Section 999.315(h)(3) to avoid running afoul of the First and Fourteenth Amendments and to ensure consumers may receive information about the impacts of an opt out request as they engage in the opt out process with a business.

III. The Proposed Modifications Should Impose the Same Notice Requirements on Authorized Agents as They Impose on Businesses

The proposed modifications to the CCPA regulations would require a business to ask an authorized agent for proof that a consumer gave the agent signed permission to submit a rights request.¹⁷ Although this provision helps ensure businesses can take steps to verify that authorized agents are acting on the true expressed wishes of consumers, the proposed modifications do not offer consumers sufficient protections from potential deception by authorized agents. For example, while the proposed modifications would impose additional notice obligations on businesses,¹⁸ those requirements do not extend to authorized agents. Authorized agents consequently have little to no guidelines or rules they must follow with respect to their communications with consumers, while businesses are subject to onerous, highly restrictive requirements regarding the mode and content of the information they may provide to Californians. The asymmetry between the substantial disclosure obligations for businesses and the lack thereof for authorized agents could enable some agents to give consumers misleading or incomplete information. We encourage the OAG to take steps to modify the proposed modifications to the CCPA regulations in order to equalize the notice requirements placed on businesses and agents, thus ensuring consumers can act on an informed basis under CCPA. In Section II of this submission, we discuss related First Amendment and communications fairness issues implicit in a balanced consumer privacy notice regime.

IV. Proposed Modifications to the CCPA Regulations Should Enable Flexibility in Methods of Providing Offline Notice

The proposed modifications to the CCPA regulations related to offline notices present a number of problems for consumers and businesses. As written, the CCPA implementing regulations already provide sufficient guidance to businesses regarding the provision of offline notice at the point of personal information collection in brick-and-mortar stores.¹⁹ The proposed modifications are more restrictive and prescriptive than the current plain text of the CCPA regulations, would restrict businesses' speech, would remove the flexibility businesses need to effectively communicate information to their customers, and would unnecessarily impede business-consumer interactions. We therefore ask the OAG to update the proposed modifications to: (1) remove the proposed illustrative example associated with brick-and-mortar stores, and (2) explicitly enable businesses communicating with Californians by phone to direct them to an online notice where CCPA-required disclosures are made to satisfy their offline notice obligation, a medium which is more familiar to consumers for these sorts of disclosures along with having the added benefit of being able to present additional choices to the consumer. This sort of operational flexibility is necessary for businesses to convey important notices in context.

The proposed modifications would require businesses that sell personal information to "inform consumers by an offline method of their right to opt-out and provide instructions on how to submit a request" when interacting with consumers offline.²⁰ The proposed modifications proceed to offer the following "illustrative examples" of ways businesses may provide such notice: through signage in an area where the personal information is collected or on the paper forms that collect personal information in a

¹⁷ Cal. Code Regs. tit. 11, § 999.326(a) (proposed Oct. 12, 2020).

¹⁸ *Id.* at § 999.315(h)(3).

¹⁹ Cal. Code Regs. tit. 11, § 999.305(a)(3)(c) (finalized Aug. 14, 2020).

²⁰ Cal. Code Regs. tit. 11, § 999.306(b)(3) (proposed Dec. 10, 2020).

brick-and-mortar store, and by reading the notice orally when personal information is collected over the phone.²¹ While the illustrative examples set forth limited ways businesses can give notice in compliance with the CCPA, they are more restrictive than existing provisions of the CCPA regulations and detract from the flexibility businesses need to provide required notices that do not burden consumers or cause unreasonable friction or frustration during the consumer's interaction with the business.

The illustrative example related to brick-and-mortar store notification sets forth redundant methods by which businesses may provide notices in offline contexts. The CCPA regulations already address such methods of providing offline notice at the point of personal information collection by stating, “[w]hen a business collects... personal information offline, it may include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online.”²² The proposed modifications regarding notice of the right to opt out in offline contexts are therefore unnecessary, as the regulations already address the very same methods of providing offline notice and offer sufficient clarity and flexibility to businesses in providing such notice.

In addition, the proposed modifications related to brick-and-mortar store notification are overly prescriptive. They include specific requirements about the *proximity* of the offline notice to the area where personal information is collected in a store. The specificity of these illustrative examples could result in over-notification throughout a store as well as significant costs. For example, the proposed modification could be interpreted to require signage at each cash register in a grocery store, as well as signage at the customer service desk, in the bakery area of the store where consumers can submit requests for cake deliveries, and in any other location where personal information may be collected. They also do not account for different contexts of business interactions with consumers. A business operating a food truck, for instance, would have different offline notice capabilities than an apparel store. A single displayed sign in a brick-and-mortar store, or providing a paper version of notice, would in most instances provide sufficient notice to consumers of their right to opt out under the CCPA. Bombarding consumers with physical signs at every potential point of personal information collection could be overwhelming and would ultimately not provide consumers with more awareness of their privacy rights. In fact, this strategy is more likely to create privacy notice fatigue than any meaningful increase in privacy control, thus undercutting the very goals of the CCPA.

Additionally, the proposed modifications' illustrative example of providing notice orally to consumers on the phone appears to suggest that reading the full notice aloud is the only way businesses can provide CCPA-compliant notices via telephone conversations. Reading such notice aloud to consumers would unreasonably burden the consumer's ability to interact efficiently with a business customer service representative and would likely result in consumer annoyance and frustration. Requiring businesses to keep consumers on the phone for longer than needed to address the purpose for which the consumer contacted the business would introduce unneeded friction into business-consumer relations. Instead, businesses should be permitted to direct a consumer to an online link where information about the right to opt out is posted rather than provide an oral catalog of information associated with particular individual rights under the CCPA.

The proposed modifications' addition of illustrative examples regarding methods of offline notice is unnecessary, redundant, inflexible, and likely highly costly for many businesses. These modifications would result in consumer confusion, leave businesses wondering if they may take other approaches to offline notices, and if so, how they may provide such notice within the strictures of the CCPA. We therefore ask the OAG to remove the proposed illustrative example associated with brick-and mortar stores

²¹ *Id.*

²² Cal. Code Regs. tit. 11, § 999.305(a)(3)(c) (finalized Aug. 14, 2020).

as well as clarify that businesses communicating with consumers via telephone may direct them to an online website containing the required opt out notice as an acceptable way of communicating the right to opt out.

* * *

Thank you for the opportunity to submit input on the content of the proposed modifications to the CCPA regulations. Please contact Mike Signorelli of Venable LLP at [REDACTED] with any questions you may have regarding these comments.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's

Christopher Oswald
SVP, Government Relations
Association of National Advertisers

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau

David LeDuc
Vice President, Public Policy
Network Advertising Initiative

Clark Rector
Executive VP-Government Affairs
American Advertising Federation

Lou Mastria
Executive Director
Digital Advertising Alliance

From: [Cameron Demetre](#)
To: [Privacy Regulations](#)
Subject: TechNet 4th round of comments for CCPA Regulations
Date: Sunday, December 27, 2020 11:49:27 AM
Attachments: [TechNet CCPA Regulation Letter 12.27.20.pdf](#)

Hello Lisa,

Please see TechNet's letter regarding the fourth round of CCPA regulation comments.

Kind regards,

Cameron Demetre
Executive Director | California & the Southwest
[TechNet](#) / The Voice of the Innovation Economy
(c) [REDACTED] | [REDACTED]
Twitter: @TechNetSouthwest





TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet California and the Southwest | Telephone 916.600.3551
915 L Street, Suite 1270, Sacramento, CA 95814
www.technet.org | @TechNetUpdate

December 27, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Department of Justice
300 Spring Street, 1st Floor
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

Dear Attorney General Becerra,

TechNet appreciates the opportunity to submit written comments regarding the fourth set of proposed modifications to the California Consumer Privacy Act ("CCPA") regulations.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic startups and the most iconic companies on the planet and represents three million employees and countless customers in the fields of information technology, e-commerce, the sharing and gig economies, advanced energy, cybersecurity, venture capital, and finance.

TechNet member companies place a high priority on consumer privacy. We appreciate the aim of the CCPA to meaningfully enhance data privacy and some of the latest modifications in response to the previous iteration of comments specifically as it relates to § 999.306, which will provide more clarity for consumers to help avoid confusion in offline settings and more acutely syncing with CCPA statute. However, we continue to be concerned that CCPA regulations are not finalized and it is not clear when these new draft regulations would be final and implemented. This raises significant compliance problems for a law that took effect January 1, 2020 and for which enforcement began July 1, 2020. We believe these modifications should include language making the changes effective six months to one year from publication of final regulations. This will give businesses the opportunity to properly implement complex regulations for a complex law. This implementation time is especially important during the ongoing COVID-19 crisis where personnel are working remotely and businesses are continuing to recover from services being shut down.

TechNet's comments are concentrated on two components of the regulations:

1. § 999.326 Verification Requests of Authorized Agents

TechNet remains concerned as it relates to the role businesses should have in requiring identify verification for authorized agents — two forms of identify verification are necessary in helping to mitigate fraudulent activity. We believe a

business should be allowed, both, to verify a consumer's identify and to also confirm that the consumer they provided the authorized agent permission to submit the request is valid in order to avoid identify theft.

2. § 999.306 Proposed Opt-Out Icon

The recent passage of Proposition 24- the California Privacy Rights Act (CPRA) requires a rulemaking which will establish a process to select an effective icon. This requisite renders a robust stakeholder process to identify the merits of any particular icon and the efficacy by which it will develop a concise, usable instrument. Identifying an icon now would circumvent the process just after one was approved by the voters. The icon development process should go through the CPRA route in the soon-to-be established California Privacy Protection Agency.

Additionally, there remains a lack of clarity as to the discretion of utilizing the opt-out button identified in § 999.306. § 999.306 (f)(1) suggests companies have a choice with respect to whether they want to present the button, however, Section (f)(2) strongly suggests that the button is required for anyone putting up a Do Not Sell My Personal Information link. As a result, these provisions appear to conflict as to the requirement to include an Opt-Out icon. Withal, the requirement of the specific icon delineated in the regulations looks like a button adjacent to the link, which will only be confusing to consumers as it could be mistaken for a button to effectuate the opt-out, leading them to overlook the link itself. For these reasons, we believe the CPRA process will help to address some of these concerns.

TechNet thanks you for taking the time to consider our comments on the proposed modifications to the CCPA regulations. We again urge that any new proposed modifications give businesses proper time to come into compliance with the regulations. Our goal for all CCPA regulations is that they should help facilitate compliance on the part of California businesses, while ensuring that consumers have the information necessary for them to make informed decisions regarding their rights under the CCPA.

If you have any questions regarding this comment letter, please contact Cameron Demetre, Executive Director, at [REDACTED] or [REDACTED].

Thank you,



Cameron Demetre
Executive Director, California and the Southwest
TechNet

Privacy Regulations

From: Stephanie Lucas [REDACTED]
Sent: Sunday, December 27, 2020 3:07 PM
To: Privacy Regulations
Subject: Comment on 4th Set of Proposed Modifications: CCPA
Categories: Written Comment

My name is Stephanie Lucas, and I'm a web design professional (and a proud native Californian).

This is the first time I've used the public comment option on any legislation. First, I want to express that I understand how much work and effort your office has put into this process, and I appreciate the opportunity to comment.

I would like to respectfully voice specific technical considerations from the standpoint of web and app design. I have worked in the design field for over 25 years, and specifically in web and app design for about 15 years. Upon reviewing the guidance for the "button" as well as the research study that led to this design, I have significant concerns about this guidance, which I'll explain as concisely as I can.

First, here is the visual graphical element I'm referring to (for the remainder of this email I'm going to call it a "visual graphic element" because the taxonomy that's being used ("button"/"icon") is itself one of my principal concerns.



Next, to quote the *"NOTICE OF FOURTH SET OF PROPOSED MODIFICATIONS TO TEXT OF REGULATIONS AND ADDITION OF DOCUMENTS AND INFORMATION TO RULEMAKING FILE"*:

"The notice of right to opt-out shall be designed and presented in a way that is easy to read and understandable to consumers."

My assertion is that this visual graphic element conflicts with this requirement in at least two ways, listed below.

Concern 1: Button, toggle, or Icon?

I'll have to beg your patience with this, but it's a legitimate issue. In the [study that informed this guidance](#), the visual graphic element is referred to throughout not as a "button" but as an "icon." This may seem like a silly distinction, but it isn't: **To be honest, this is actually a huge issue that questions the validity of applying this study to the Attorney General's guidance at all.**

A **button** is the name of a design element that has a specific function *and specific rules and best practices*. A button needs to - on its own - *clearly represent what action it represents*. This is a very

foundational web design principle. Most buttons have text that states the action. This visual element has two abstract symbols that don't mean anything without context.

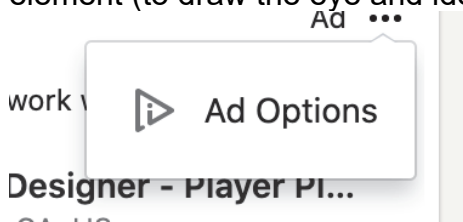
Buttons also have their own rules when it comes to programming for accessibility.

Further, it's evident that this new visual graphic element is an **iteration of the "red toggle"** from the initial guidance. I maintain it still will be mistaken for a toggle, or that at minimum there will be confusion caused by the visual similarity. A quick visual scan reveals 2 very toggle-type characteristics/cues: *1. It's basically the same shape as a toggle* *2. It's half/half blue and white, like a toggle*. Those characteristics should be reconsidered.

By comparison, an **icon** is a visual symbol for *wayfinding and identifying*. Speaking from years of experience in this field: It's critically important to not conflate these two terms. Based on the purpose expressed in both the Attorney General's guidance and the study I linked, the element is meant to *draw the eye and make sense to the user to help them understand they have a choice*. That has the characteristics of an icon, not a button.

I'm not splitting hairs here: designers (the people who will have the job of implementation) will have a difficult time if there's ambiguity over whether this is a button or icon.

For example, the "Ad Options" visual element (the triangle) is an icon, not a button. I believe this icon is for the same purpose that the Attorney General's office has in mind for the CCPA visual graphic element (to draw the eye and identify).



Since the guidances have begun rolling out, I'm seeing both the term "button" and "icon" being used interchangeably in discussions - if you look ahead to the actual implementation phase of this, it's critical for product teams to understand whether it's an icon or a button. I believe the AG's office is going to create more confusion than solve it if this current guidance is delivered.

Concern 2: Accessibility

Again quoting *"NOTICE OF FOURTH SET OF PROPOSED MODIFICATIONS TO TEXT OF REGULATIONS AND ADDITION OF DOCUMENTS AND INFORMATION TO RULEMAKING FILE"* the user experience should be:

"reasonably accessible to consumers with disabilities"

I am troubled to see that [the study that informed this decision the study that informed this decision](#) doesn't seem to have sought out any participants with disabilities (if it did, that doesn't seem to be communicated in the summary report).

It's important to understand that accessibility is ***not just making sure that elements work with screen reader technology***. Disability also extends to a spectrum of cognitive limitations as well as other considerations.

The CDC currently reports that over 25% of the population of California is contending with some type of disability.

If disabled individuals were not included in the study that examined comprehension and clarity around this visual graphic element, that means that *an enormous amount of consumers WON'T be served* by this requirement.

Since this new guidance was introduced in October, even so-called “abled” people - people with law degrees - have expressed confusion over what this visual graphic element means. What chance do consumers on the disability spectrum have?

Because the guidance appears to mandate the use of this visual graphic element, I think it's extremely important to get it right.

To summarize, in my opinion if this element is meant to draw the eye, it should:

- Be presented for user testing to study participants with a spectrum of disabilities
- Be re-evaluated to make it look less like a toggle
- Be consistently referred to as an *icon* and not a button, with guidance that it can *only be used if it's associated with text for context*
- Be optional

Thank you for your time. I am happy to be contacted for any further conversation on this at:



Stephanie Lucas

From: [Sara DePaul](#)
To: [Privacy Regulations](#)
Cc: [Carl Schonander](#); [Jeff Joseph](#); [Christopher Mohr](#); [Sara Kloeck](#)
Subject: SIIA Comments to Notice of Fourth Set of Proposed Modifications to the CCPA Regulations
Date: Monday, December 28, 2020 9:20:35 AM
Attachments: [SIIA Comments CCPA Regs Fourth Modifications FNL.pdf](#)

On behalf of the Software & Information Industry Association (SIIA), I am attaching our comments to the notice of a fourth set of proposed modifications for filing by the deadline today. Thank you, and happy holidays.

Best,

Sara DePaul

Associate General Counsel & Senior Director, Technology Policy
SIIA - The Software & Information Industry Association
1090 Vermont Ave NW, Sixth Floor, Washington, DC 20005
[REDACTED] Office / [REDACTED] Mobile / @saracdepaul Twitter
[siianet/policy](#)



Accelerating Innovation in
Technology, Data & Media

202.289.7442 1090 Vermont Ave NW Sixth Floor
www.siiia.net Washington DC 20005-4905

Software & Information Industry Association Comments Regarding the Notice of Fourth Set of Proposed Modifications to CCPA Regulation

The Software & Information Industry Association (SIIA) welcomes the opportunity to provide written comments regarding the Notice of Fourth Set of Proposed Modifications to the regulations regarding the California Consumer Privacy Act (CCPA). SIIA is the leading organization representing financial information, education technology, specialized content, information and publishing, and health technology companies. Our diverse membership of more than 700 companies and associations help learners of all ages prepare to succeed in their future, manage the global financial markets, develop software that solves today's challenges, provide critical information that helps inform global businesses large and small, and innovate for better health care and personal wellness outcomes.

SIIA's members are dedicated to data privacy, as a matter of regulatory obligation, responsible stewardship of data, and good customer care and service. On behalf of our members, we advocate for a national data privacy standard that robustly protects consumers while allowing innovation and competition. As you know, achieving these aims is complex and requires both thoughtful analysis of the impact of data provision regulatory provisions and identifying opportunities for interoperability with other data privacy frameworks when possible.

In general, we are neutral on the proposed modifications to the regulation. For the most part, the proposed modifications succeed in their goal to clarify existing regulatory provisions. We are concerned, however, by the proposed change to re-introduce an opt-button, albeit as a button that businesses that can optionally include next to their Do Not Sell link. While this is superficially consumer friendly, it is likely to lead to consumer confusion due to the lack of uniformity of use. Earlier provisions that would have mandated an opt-out button were removed for good reasons which likely will inhibit its adoption by businesses. We request that the Attorney General delete this proposed addition to Section 999.306, particularly at this late stage.

Additionally, we are concerned with significant divergences between the CCPA, its implementing regulations, and the recently passed California Consumer Privacy Rights Act. We encourage the Attorney General to either use the CCPA rulemaking authority to close these gaps or to exercise his prosecutorial discretion to put industry on notice that they are not liable for business practices that will be lawful when the CPRA implements in 2023. We note two glaring gaps that require such action by the Attorney General.

First, we remain concerned with the CCPA's broad First Amendment defects, including with respect to its regulation of publicly available information. We have explained the substantive reasons for the CCPA's First Amendment problems,¹ and will not repeat them here

¹ See SIIA's March 27, 2020 Comments, available at: <https://www.siiia.net/Portals/0/pdf/Policy/Privacy%20and%20Data%20Security/SIIA%20Comments%20on%20CCPA%20Regs%2027%20MAR.pdf?ver=2020-03-30-092111-393>; February 25, 2020 Comments; available at: <https://www.siiia.net/Portals/0/pdf/Policy/SIIA%20Comments%20re%20CCPA%20Regs%20Feb%202020%20FNL%20FLD.pdf?ver=2020-03-27-131710-980>; December 6, 2019 Comments, available at:

in any depth, except to say that our prior filings have discussed the CCPA's unconstitutional regulation of public domain information that is widely available in private hands. And as we have brought to your attention in those same comments, your office is empowered by the CCPA to fix the statute's constitutional flaws through the rulemaking process. See *also* CCPA 1798.185(a)(3). Exercise of that power is imperative, not only with respect to insulating the CCPA from a fatal First Amendment attack but also to harmonize with the California Privacy Rights Act, which is constitutionally sound with respect to publicly available information.

The failure of the Attorney General's office to address this will create a significant practical problem. The CPRA will cure the CCPA's constitutionally invalid regulation of the public domain when it takes effect on January 1, 2023. Maintaining the CCPA's unconstitutional regulation in the intervening period, therefore, is neither beneficial to consumers nor businesses. For consumers, maintaining this unconstitutional reach extends "data rights" they are not entitled to as a matter of constitutional law and that will sunset by 2023. Business are presented with a Hobson's choice: they must either risk an enforcement action between now and the statute of limitations for the expiration of CCPA claims **or** bear the expensive burden of being whipsawed by a statutory obligation that will cease to exist in two years. Maintaining the CCPA's treatment of publicly available information will have consequences that are unfair, untenable, and unconstitutional.

We therefore respectfully urge the Attorney General to use his authority under Section 1798.185(a)(3) to standardize the treatment of publicly available information by either modifying the regulations to exclude the entire public domain as required by the First Amendment or to set forth an enforcement moratorium with respect to publicly available information that will be subject to the CPRA exclusions on January 1, 2023.

Second, the CCPA and CPRA's differences with respect to requests to opt-out and user-enabled global privacy controls create unfair and unnecessary compliance tensions. The implementing regulation for the CCPA, for instance, requires a business that collects personal information online to treat user-enabled global privacy controls as a signal of a consumer's choice to opt-out of the sale of their information. See Section 999.315(d). The CPRA, in contrast, does not require businesses to treat user-enabled global privacy controls as an opt-out. Instead, businesses can meet obligations relating to requests to opt-out either through the primary opt-out mechanism in Section 1798.135(a) *or* through an opt-out preference signal as set forth in Section 1798.135(b)(1). See *also* Section 1798.145(b)(3) ("A business that complies with subdivision (a) of this Section is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b).").

Barring action by the Attorney General to correct this discrepancy, businesses will be required either to risk enforcement action or comply with the CCPA by enabling both the Do Not

<https://www.siiia.net/Portals/0/pdf/Policy/SIIA%20Comments%20re%20CCPA%20regs%206%20DEC%20FNL%20%20FILED.pdf?ver=2020-01-17-135803-493>.

Sell Link **and** user-enabled privacy controls as requests to opt-out until January 1, 2023 when the CPRA implements and gives them a different choice. Leaving this conflicting obligation in place is unfair and against the wishes of the Californian electorate. As with the CCPA's unconstitutional regulation of the public domain, we urge the Attorney General to fix this tension either through the rulemaking process or through an enforcement policy statement that sets forth an intention not to bring enforcement actions for alleged CCPA violations that would not violate the CPRA.

Dated: December 28, 2020

Respectfully submitted,



Christopher A. Mohr, VP for Intellectual Property and General Counsel

Sara C. DePaul

Associate General Counsel & Senior Director for Technology Policy

Software & Information Industry Association

www.siiia.net

From: [Melanie Tiano](#)
To: [Privacy Regulations](#)
Subject: CTIA Comments Fourth Set of Modified Regulations
Date: Monday, December 28, 2020 12:31:13 PM
Attachments: [image002.png](#)
[CTIA - Comment on CCPA Fourth Set of Modified Regulations 12.28.20.pdf](#)

Good afternoon.

Attached are CTIA's comments in response to the Fourth Set of Modified Regulations.

Please let me know if you have any questions.

Thank you,

Melanie Tiano



Melanie K. Tiano
Director, Cybersecurity and Privacy
1400 16th Street, NW
Washington, DC 20036
[REDACTED] (office)
[REDACTED] (mobile)

Before the
STATE OF CALIFORNIA DEPARTMENT OF JUSTICE
ATTORNEY GENERAL'S OFFICE
Los Angeles, CA 90013

In the Matter of)	
)	
California Consumer Privacy Act)	Public Forums on the California
Rulemaking Process)	Consumer Privacy Act
)	
)	

COMMENTS OF CTIA

Gerard Keegan
Vice President, State Legislative Affairs

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th St. NW, Suite 600 Washington,
DC 20036
(202) 736-3200
www.ctia.org

December 28, 2020

TABLE OF CONTENTS

INTRODUCTION	3
I. § 999.306 Notice of the Right to Opt-Out of the Sale of Personal Information	3
a. The Department should clarify that use of an opt-out button is voluntary.	3
b. The proposed button is potentially confusing to consumers.....	4
II. § 999.326. Authorized Agent.....	5
a. CTIA requests that the Department maintain the current version of § 999.326 (a) but clarify that businesses may require authorized agents to verify their own identities. ...	5
CONCLUSION.....	7

Before the
STATE OF CALIFORNIA DEPARTMENT OF JUSTICE
ATTORNEY GENERAL'S OFFICE
Los Angeles, CA 90013

In the Matter of)	
)	
California Consumer Privacy Act Rulemaking)	Public Forums on the California
Process)	Consumer Privacy Act
)	

INTRODUCTION

CTIA appreciates the opportunity to provide these comments on the California Department of Justice's ("Department's") Fourth Set of Modified Proposed Regulations ("modified regulations") to implement the California Consumer Protection Act of 2018 ("CCPA" or "Act"). CTIA appreciates the Department's continued efforts to revise and clarify the final regulations. However, CTIA is concerned that regulations as the modifications propose may cause confusion, will not serve to further the purposes of the Act, and could allow for fraudulent requests for consumers' personal information. CTIA's concerns pertain to the following sections of the modified regulations:

- § 999.306. Notice of the Right to Opt-Out of the Sale of Personal Information; and
- § 999.326. Authorized Agent.

Where appropriate, CTIA provides alternative regulatory language to address the issues identified herein.

I. § 999.306 Notice of the Right to Opt-Out of the Sale of Personal Information

a. The Department should clarify that use of an opt-out button is voluntary.

CTIA appreciates the Department's efforts to develop a framework for use of an opt-out button that is both consumer-friendly and practical. However, while it appears the intent of the

Attorney General was to create a standardized, voluntary opt-out button,¹ the modified regulations create confusion due to inconsistencies between § 999.306(f)(1) and § 999.306(f)(2). In particular, subsection (1) states that the opt-out button “*may* be used in addition to posting the notice of the right to opt-out”, while subsection (2) states that the button “*shall* be added to the left of the [Do Not Sell My Personal Information Link].”

To avoid confusion and more clearly reflect the intent of the Attorney General, CTIA recommends that the Department revise § 306(f) as follows:

§ 999.306(f) . . . (1) *The following opt-out button may be used in addition to ~~posting the notice of right to opt-out~~, but not in lieu of any requirement to post the notice of right to opt-out or a “Do Not Sell My Personal Information” link as required by Civil Code section 1798.135 and these regulations.*

(2) *Where a business posts the “Do Not Sell My Personal Information” link, the opt-out button, ~~should the business choose to use it~~, shall be added to the left of the text as demonstrated below. The opt-out button, ~~if used~~, shall link to the same Internet webpage or online location to which the consumer is directed after clicking on the “Do Not Sell My Personal Information” link.*

(3) *The button, ~~if used~~, shall be approximately the same size as any other buttons used by the business on its webpage.*

b. The proposed button is potentially confusing to consumers.

The design of the proposed opt-out button is potentially confusing and suffers from many of the same issues as the opt-out button proposed by the Department in its first set of modifications, dated February 10, 2020. CTIA has many of the same concerns with this button as it had with the initial opt-out button.²

¹ See Initial Statement of Reasons, Proposed Adoption of California Consumer Privacy Act Regulations, State of California Department of Justice, Office of the Attorney General (Oct. 11 2019) <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf>, § 306 (e) (noting the process for development of a button that *may be used in addition to* but not in place of the posting of a notice of the right to opt out of the sale of personal information) (emphasis added).

² See Comments of CTIA, *In the Matter of California Consumer Privacy Act Regulations*, California Office of the Attorney General, Request for Comments, February 25, 2020 (noting that the proposed opt-out button was needlessly misleading because it gave the appearance of an immediate interactive opt-out control rather than a link to a page with more information).

In particular, the presence of both a checkmark and an “x” may mislead consumers, who might reasonably believe that by: (1) clicking different sides of the button, consumers could indicate their distinct data selling preferences; (2) clicking the button, consumers could immediately operationalize their data selling preferences (as opposed to being directed to the same website as clicking on the adjacent “Do not sell my personal information” link); and/or (3) clicking the button, consumers could only indicate their consent to the sale of their personal information, which would otherwise be restricted. In addition, several participants in a study that originally tested the proposed opt-out button reported that they viewed the button as an opt-*in* mechanism.³

Accordingly, CTIA recommends that the Department reconsider the proposed design of the current proposed opt-out button, due to the risk it poses of confusing consumers.

II. § 999.326. Authorized Agent.

a. CTIA requests that the Department maintain the current version of § 999.326(a) but clarify that businesses may require authorized agents to verify their own identities.

CTIA reiterates the concerns expressed in its October 28, 2020 comment regarding the security risks associated with consumer information requests submitted through authorized agents.⁴ In particular, the revisions proposed to § 999.326(a) in the Third Set of Modified Proposed Regulations that remain in the current proposal would unnecessarily limit businesses’ ability to implement necessary antifraud measures related to verifying requests submitted by purported authorized agents. CTIA believes that the current version of § 999.326(a)⁵ provides a preferable framework for businesses to address such risks as compared to the revisions that

³ Cranor et al., *Design and Evaluation of a Usable Icon and Tagline to Signal an Opt-Out of the Sale of Personal Information as Required by CCPA* 31 (2020), <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cranor-design-eval-usable-icon.pdf>.

⁴ See Comments of CTIA, *In the Matter of California Consumer Privacy Act Regulations*, California Office of the Attorney General, Request for Comments, October 28, 2020.

⁵ Cal Code Regs tit. 11, § 999.326(a) (2020).

remain in the current proposal. As noted in the Department’s Final Statement of Reasons, the current version of § 999.326(a) allows businesses the “discretion to determine, based on the [regulations’ general rules regarding identity verification],”⁶ which requirements set forth in § 999.326(a) are appropriate for a given request. In addition, the regulations’ general rules regarding identity verification contain guiding principles that require businesses to establish a “reasonable method” for verification, as well as “reasonable security measures to detect fraudulent identity-verification activity.”⁷

These guiding principles make clear that businesses’ identity verification processes, including for authorized agents, must be reasonable in light of the particular circumstances at issue. The limitations proposed in the modified regulations, on the other hand, would prohibit businesses from requiring all of the forms of verification outlined in § 999.326(a) *even if requiring all of those measures would be reasonable* in light of the security risks facing that particular business and its consumers.

In addition, and in accordance with these principles, CTIA recommends that businesses be expressly permitted to require authorized agents to verify their own identity. This additional verification measure may be necessary to avoid situations whereby fraudsters pose as authorized agents to gain access to consumers’ personal information, and businesses should have the flexibility to employ such a measure where appropriate.

CTIA therefore requests that the Department maintain the current version of § 999.326, and clarify that businesses may require authorized agents to verify their own identities, and proposes the following language be inserted into the current version of § 999.326(a):

⁶ Final Statement of Reasons, Proposed Adoption of California Consumer Privacy Act Regulations, State of California Department of Justice, Office of the Attorney General 48 (June 1, 2020) <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor.pdf>.

⁷ Cal Code Regs tit. 11, § 999.323 (2020).

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require that the authorized agent verify their own identity and/or that the consumer do the following:

CONCLUSION

CTIA appreciates the Department's consideration of these comments and stands ready to provide any additional information that would be helpful.

Respectfully submitted,

/s/ Gerard Keegan

Gerard Keegan
Vice President, State Legislative Affairs

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA

1400 16th St. NW, Suite 600
Washington, DC 20036
(202) 736-3200

December 28, 2020

From: [Emery, Emily](#)
To: [Privacy Regulations](#)
Subject: MPA Comments on Fourth Set of Proposed Modifications to Text of CCPA Regulations
Date: Monday, December 28, 2020 1:09:57 PM
Attachments: [MPA Comments on Fourth Set of Proposed CCPA Modifications.pdf](#)

Attached, please find comments on the fourth set of proposed modifications to the text of regulations implementing CCPA submitted on behalf of MPA - The Association of Magazine Media.

We appreciate the opportunity to provide the attached comments for your consideration.

Wishing you a happy new year,
Emily Emery

Emily Emery
Director of Digital Policy
MPA - The Association of Magazine Media

Cell: [REDACTED]

Office: [REDACTED]
[REDACTED]

December 28, 2020

The Honorable Xavier Becerra
California Department of Justice
ATTN: Lisa B. Kim, Privacy Regulations Coordinator
300 South Spring Street, First Floor, Los Angeles, CA 90013

Submitted via email to PrivacyRegulations@doj.ca.gov

RE: Comments from MPA – the Association of Magazine Media on the Fourth Set of Proposed Modifications to Text of Regulations to Rulemaking [OAL File No. 2019-1001-05]

Dear Attorney General Becerra:

MPA – the Association of Magazine Media represents over 500 magazine media brands that deliver compelling and engaging content across online, mobile, video, and print media. Having testified on behalf of our members and provided previous rounds of comments on modified language proposed by the Office of the Attorney General (“OAG”), we appreciate the opportunity to offer additional comments on the fourth set of proposed modifications to the regulations implementing the California Consumer Privacy Act (“CCPA”).

On the date of these comments, the rulemaking provisions of the California Privacy Rights Act (“CPRA”) are already in effect. Further, the CCPA implementation process is now in its second year. Our members have devoted significant resources to make good-faith efforts to comply with existing CCPA requirements and will continue to invest in preparing for CPRA compliance. We ask that the OAG keep these efforts in mind when considering any additional proposed changes as businesses seek to simultaneously implement both the impending CPRA privacy framework and modifications to the current framework.

In response to the latest proposed modifications in the sections below, MPA offers the following recommendations concerning requirements for offline notice of right to opt-out, the proposed number of allowable steps for opt-out, and requests made through authorized agents. MPA’s suggested additions are indicated in ***bold italicized underline***.

I. The OAG should clarify in its modifications to Section 999.306(b)(3) that in instances where personal information is collected through a printed form that is to be mailed back to the company, that the offline notice may include a web address that the customer can access to opt-out of the sale of their personal information.

MPA appreciates the clarifying language proposed by the OAG on Section 999.306(b)(3) that makes the notification process for the right to opt-out more evident for businesses seeking to

implement the requirement. In addition to collecting personal information online and at brick-and-mortar locations, the magazine media industry, as with other industries, may collect personal information that consumers complete through a printed form and then submit by mail, such as an order card inserted in a print issue of a magazine.

Magazine readers support and understand that publishers may use the information collected to offer other titles of interest, product recommendations, or in the furtherance of other positive consumer experiences. Publishers support making it easy for a consumer to understand how to opt-out of these offerings, including when a consumer submits information through a printed form that the consumer mails back to the business.

Where businesses like magazine publishers execute the common, expected, and CCPA-compliant practice of leveraging consumer data collected through offline means, the OAG should confirm that to provide notice at the point of collection of personal information, it is sufficient for a business to direct a customer to a web address where the consumer may choose to instruct the business that sells personal information to stop selling their personal information.

MPA made the following recommendation in [comments](#) regarding the third round of proposed modifications and raises it again here: MPA recommends that the OAG modify Section 999.306(b)(3) to include an additional illustrative example:

(c) A business that sells personal information from consumers that it collects through printed forms by mail may provide notice by including on the paper forms that collect the personal information a web address directing consumers to where the consumer may choose to opt-out of the sale of their personal information.

This addition – clarifying that providing a web address on printed material is an offline notice – would aid in compliance for offline printed notices. This illustrative example for printed materials sent through the mail is consistent with Section 999.305(b)(3) in which offline notices may direct consumers to where the “Do Not Sell My Personal Information” webpage can be found online. It is also analogous to the proposed illustrative example in Section 999.306(b)(3)(a) for brick-and-mortar stores (which may post signage).

This method of notice also enhances data privacy and security by minimizing the amount of data a business must collect in printed form to validate and execute a consumer’s request, allowing businesses to standardize operations, including the ability to have a single, centralized location where opt-out information is maintained.

II. The OAG should clarify in Section 999.315 that offers to customers are allowed if the display of such offers adds no additional steps to the opt-out process.

MPA agrees that the steps for submitting a request to opt-out should be minimal and should not subvert consumer intent. Magazine media consumers often benefit from renewal offers that reduce the price of a subscription. Posting notice of an offer of a discounted subscription without

creating an additional required step or friction for the consumer provides value to the consumer without impairing a consumer's ability to execute their request to opt-out. The CCPA regulations should explicitly permit businesses to present a notice of benefits for the consumer should they elect to remain opted-in.

Consumers may also benefit from electing to opt-out of certain services or offerings while not opting-out entirely. Businesses should be permitted to enhance the consumer experience and better serve consumer intent by providing an easy opt-out process that allows the consumer to indicate his or her desired preferences. Businesses should be allowed to display an interface that enables the consumer to effectuate a full or partial opt-out or select/de-select from a listing where multiple offerings exist as long as one of the de-selection options is inclusive of all of the business' use of consumer data.

MPA made the following recommendation in [comments](#) regarding the third round of proposed modifications, and again in these comments: MPA urges the OAG to add the following clarification to Section 999.315(h)(3):

(3) Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request. *A business may display information that provides context to enable a consumer to reconsider their interest in opt-out or to elect a partial opt-out provided that display does not require additional steps or subvert or impair a consumer's choice to opt-out. A display that provides an offer of additional goods or services shall not count in the number of steps to opt-out if the consumer is not required to take an additional step if they do not wish to take advantage of the offer.*

III. In Section 999.326(a) on authorized agents, the OAG should restore businesses' ability to make good-faith efforts to engage with the consumer to both directly verify their identity and confirm with the consumer that they have authorized an agent's request.

MPA welcomes the additional clarifying text from the OAG that businesses may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request.

MPA urges the OAG to make an additional modification to the proposed text that would further improve businesses' ability to make good-faith efforts to protect consumers' data privacy and security.

The statutory CCPA text allows businesses to authenticate "right to know" and data deletion requests filed by consumers directly or through authorized agents and to do so by presenting the same interface online for either method. For example, businesses currently commonly utilize a consumer's email address to map to an account and process a request.

Since the effective date of the CCPA, many businesses have identified troubling practices by authorized agents that undermine consumers' data privacy and security, and these unauthorized

requests continue to escalate. Therefore, MPA is concerned that in precluding businesses' ability to seek both verification and confirmation of authorization, the proposed language in Section 999.326(a) will impede necessary steps that businesses would take to respond to suspected consumer fraud instances perpetrated by entities improperly representing themselves as authorized agents.

Maximizing consumer data protection requires that businesses may both directly verify identity with the person to whom the request is related and confirm that the consumer provided the agent's authorization to submit the request. While MPA appreciates the addition of requiring a consumer to provide signed permission to the authorized agent, the most secure verification method remains in allowing a business to have direct contact with the consumer to both confirm identity and confirm that the consumer granted permission to an authorized agent.

If a business can only verify the consumer's identity, they're not able to alert the customer to a potentially unauthorized request. If a business can only confirm that an individual granted authorization, the unverified respondent of such an authorization request could still be the perpetrator of the unauthorized request. Both of these scenarios imperil consumers' data.

Requiring both steps is necessary for data security best practices, and businesses can execute both steps in a single correspondence to minimize inconvenience for the consumer.

MPA made the following recommendation in [comments](#) regarding the third round of proposed modifications, and again in these comments. MPA urges the OAG to restore the enacted text that allows businesses to exercise both verification methods:

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to ~~do either of the following~~:

(1) Verify their own identity directly with the business.

(2) Directly confirm with the business that they provided the authorized agent permission to submit the request.

MPA again notes the critical role that direct first-party engagement with consumers can have in enhancing data security, protecting privacy, and preventing fraudulent activity.

MPA and our members appreciate the opportunity to provide our views for your consideration.

In adopting the clarifications proposed above, the OAG will enhance the magazine media industry's ability to operationalize consistent privacy-protective practices that enhance reader trust, preserve the viability of media resources that consumers enjoy, and sustain vital journalism on which consumers rely for critical information.

Respectfully submitted,

Brigitte Schmidt Gwyn
President and Chief Executive Officer

Rita Cohen
Senior Vice President, Legislative and Regulatory Policy

Emily Emery
Director, Digital Policy

From: [Dale Smith](#)
To: [Privacy Regulations](#)
Cc: [Dale R. Smith Jr.](#)
Subject: Submission of Comments: NOTICE OF FOURTH SET OF PROPOSED MODIFICATIONS TO TEXT OF REGULATIONS
Date: Monday, December 28, 2020 1:15:23 PM
Attachments: [footerNew2.bmp](#)
[20201228 CCPA Comments \(1\).pdf](#)

Dear Ms. Kim:

Attached please find our .pdf document containing comments relating to the 4th set of proposed CCPA regulation modifications.

Please contact me if you have any difficulty with their usage.

Thank you, and best wishes for a safe and happy 2021.

Dale Smith, CIPT

DALE R. SMITH, CIPT

Futurist



View my blog at: privacyelephant.com



December 28, 2020

Lisa B. Kim
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Via Email to: PrivacyRegulations@doj.ca.gov

Attn: Honorable Xavier Becerra, Attorney General

Re: Comments on NOTICE OF FOURTH SET OF PROPOSED MODIFICATIONS TO
TEXT OF REGULATIONS, Released December 10, 2020

Dear Mr. Becerra:

The subject of this comment is the newly-added “Opt-Out Button” proposed in §999.306(f) and the overall effect the implementation of notice transparency may have on CCPA/CPRA success in achieving California's goal of protecting consumer’s privacy.

In that connection, we write to make the following observations:

1. As introduced under §999.306 Notice of Right to Opt-Out of Sale of Personal Information, the “Opt-Out Button” as presented in §999.306(f) is linked directly to and solely associated with presenting the “Do Not Sell My Personal Information” right (DNSMPI) and choice to consumers. DNSMPI is its sole function, by definition.

This implementation fulfills the OAG’s pending requirement of 1798.185(a)(4)(C) to provide a uniform opt-out button. As a consequence, however, the “Opt-Out Button” becomes just that ... a button provided for the sole purpose of opting-out. Any use of the OOB for another purpose is confusing and at cross purposes with the regulation.

2. Paragraphs §999.305 Notice at Collection of Personal Information and §999.307 Notice of Financial Incentive are equally foundational elements of CCPA notice transparency. Both are similar in scope and purpose to §999.306. And as a means of just-in-time briefing of consumers on privacy rights, they are equally important as the DNSMPI because:
 - Not every company collects PI from consumers.
 - Not every company that collects PI from consumers sells it.
 - Not every consumer seeking contact/category/purpose/policy information (at collection time) is interested in exercising DNSMPI rights.
 - Companies who do not sell PI (and do not display a DNSMPI) run the risk of being seen as consumer-unfriendly based on logo confusion. (“If I can’t see the DNSMPI, this must be a bad company.”)
3. From a consumer’s point of view, we believe that Notice at Collection and Notice of Financial Incentive are equally important as Notice of Right to Opt-Out in terms of consumer access. Each should be equally available and accessible at points of consumer access and PI ingress.
4. As the CCPA regulations are operationalized, there is a risk that the single-purpose Opt-Out Button as currently specified could be misunderstood and misused by companies and consumers alike to be a “CCPA privacy information button”, to be pressed for any privacy purpose. Allowing this to happen could lead to a chaotic breakdown of essential communication between companies and consumers, which should be avoided at all costs.
5. With California now in the driver’s seat for implementing privacy legislation that could form the model for many North American jurisdictions (including a national US law), we believe that the time is right for practical operational guidance to be put forward. California needs to get this right, or risk losing consumer trust for the privacy community in general.



As one means to fill this transparency “vacuum”, we suggest employing a standardized graphic framework (trigger) image at consumer touchpoints that allows companies of all sizes to guide consumers’ attention to simply organized just-in-time information covering all elements of consumer access, not just DNSMPI.

We suggest the adaptation of the Nutrition Label-style framework for this purpose. The NL paradigm readily accommodates consumers access to information under all three notice types, as well as providing single-click linked access into a company’s mother privacy policy document as a final point of reference.

A testament to the flexibility and acceptance of the NL paradigm can be seen displayed on food items of every size, description, and composition in stores everywhere. Each Nutrition Facts label lists simple facts in order of importance to consumers. A Privacy Facts label builds on that same simplicity, but leverages technology by displaying simple and concise privacy information in real time as directed by the consumer.

Use of the NL paradigm brings a number of non-CCPA benefits:

- It provides an operational means for transitioning away from the misuse of “cookie notices” and “cookie banners” as vessels for dispensing CCPA/CPRA information.
- As a national privacy law is debated in Washington, a well-conceived and implemented CCPA/CPRA notice model will attract the attention of many state jurisdictions, leading to passage of a comprehensive national law rather than a fragmented quilt of state regulations. This would be a testimony to California’s thought leadership and a large benefit to the nation’s consumers in general.
- As the US struggles for privacy adequacy with the EU and other continents, the flexibility and scope of the NL paradigm can work to promote transparency agreement across continents. Nutrition Labels are used and trusted around the world, not just in the USA.



Regarding our specific comment on the 4th set of proposed regulations, we suggest that language be added within the regulations to name the Nutrition Label paradigm as a recognized foundational tool for meeting the notice transparency requirements of CCPA/CPRA.

Additional descriptive information on practical CCPA notice implementation can be found in PrivacyCheq's previous comment submissions to the CCPA Proposed Regulation which closed on [December 6, 2019](#), [February 24, 2020](#), [March 27, 2020](#), and [October 28, 2020](#).

We thank you for these opportunities to comment.

A handwritten signature in black ink, appearing to read "DRA", with a long horizontal stroke extending to the right.

Dale R. Smith, CIPT
Futurist



From: [Mohammed, Shoeb](#)
To: [Privacy Regulations](#)
Cc: [Leder, Leslie](#)
Subject: CalChamber Comments to Fourth Proposed Modifications to CCPA Regulations
Date: Monday, December 28, 2020 2:58:51 PM
Attachments: [image001.png](#)
[CalChamber Comments to Fourth Modified CCPA Regulations.pdf](#)

Dear Lisa Kim,

Attached please find CalChamber's comments to the Fourth Set of Proposed Modifications to Text of CCPA Regulations.

Thank you,

Shoeb Mohammed
Policy Advocate
California Chamber of Commerce



December 28, 2020

SENT VIA EMAIL

Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, 1st Floor
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

Re: Written Comments to Fourth Set of Proposed Modifications to Text of CCPA Regulations
OAL File No. 2019-1001-05

SUMMARY

The California Chamber of Commerce (CalChamber) respectfully submits the following comments to the Attorney General's (AG) Fourth Set of Proposed Modifications to Text of California Consumer Privacy Act (CCPA) Regulations. Recommended changes are formatted as edits to the final form of the fourth set of proposed modifications to the regulations. Recommended changes to the final form of the proposed modifications are displayed with additions in underline and deletions in ~~strikeout~~. Additionally, in Section III, we reiterate our concern that the current rulemaking activities violate the Administrative Procedures Act.

COMMENTS

I. SECTION 999.306 – Notice of Right to Opt-Out of Sale of Personal Information.

A. Issue: It is unclear whether the Opt-Out Button is optional because §999.306(f)(1) conflicts with §999.306(f)(2).

1. Proposed Regulation: §§ 999.306(f)

§999.306(f)(1) states the intention to make the Opt-Out Button optional by use of the term “may.” It reads, in relevant part, that the Opt-Out Button “may be used in addition to” ... “but not in lieu of any requirement to post the notice of right to opt out or a ‘Do Not Sell My Personal Information’ link.” In conflict, §999.306(f)(2) suggests that the Opt-Out Button is mandatory by use of the term “shall.” It states that the button “shall” be added where a business posts the “Do Not Sell My Personal Information” link. Accordingly, (f)(2) is in conflict with (f)(1).

Additionally, §999.306(f)(1) contains a duplicative clause that makes the regulation unclear as drafted. Subsection (1) states: “The following opt-out button may be used in addition to posting *the notice of right to opt out*, but not in lieu of any

requirement to post *the notice of right to opt out...*” (emphasis added). The duplicative use of the clause “the notice of right to opt-out” is unnecessary and confusing. We therefore recommend deletion.

2. Recommended Changes: Revise §§999.306(f) to clarify that the Opt-Out Button is optional, and strike duplicative language for clarity, as follows:

999.306(f) Opt-Out Button

(1) The following opt-out button may be used in addition to ~~posting the notice of right to opt out~~, but not in lieu of any requirement to post the notice of right to opt-out or a “Do Not Sell My Personal Information” link as required by Civil Code section 1798.135 and these regulations.

(2) Where a business posts the “Do Not Sell My Personal Information” link, the opt-out button, should the business choose to use it, shall be added to the left of the text as demonstrated below. The opt-out button, if used, shall link to the same Internet webpage or online location to which the consumer is directed after clicking on the “Do Not Sell My Personal information” link.

(3) The button, if used, shall be approximately the same size as any other button used by the business on its webpage.

II. SECTION 999.326 – Authorized Agent.

- A. Issue: Businesses are prohibited from using multiple forms of identity verification when requests to access consumer data come from authorized agents.

1. Proposed Regulation: §§ 999.326(a)

When a request to access or delete information comes from a party claiming to act on behalf of a consumer, a business must be permitted to use multi-step verification to ensure each request is legitimate and prevent unauthorized access. The language in the current regulations, approved by the Office of Administrative Law and effective on August 14, 2020, permits businesses to use three verification elements outlined in §999.326(a)(1)-(3) of those regulations. The proposed changes by the Attorney General initially proposed in the Third Set of Modifications, which also appear in this Fourth Set, depart from this standard, limiting businesses to only two forms of verification when three would provide additional security for consumer information.

2. Recommended Changes: Revise §§999.326(a) to allow businesses to use all three verification methods as follows:

§999.326 Authorized Agent

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to do both ~~either~~ of the following:

(1) Verify their own identity directly with the business.

(2) Directly confirm with the business that they provided the authorized agent permission to submit the request.

III. The Fourth Proposed Modifications Violate the Administrative Procedures Act

This Fourth Set of Proposed Modifications, made in response to comments to the Third Set of Proposed Modifications, is unlawful because it violates the procedural requirements of Government Code §1130 et seq, the California Administrative Procedures Act (APA).

GC 11346.4(b) provides that a Notice of Proposed Action is valid for one year. This Fourth Set of Modifications was issued in response to comments made to the Third Set of Modifications. The Third Set of Modifications was unlawful because it was published on October 12, 2020, more than one year after the original the Notice of Proposed Action dated October 11, 2019. Because 2020 is a leap year, the proposed third set was published 367 days after the original Notice of Proposed Action. Therefore, the third and fourth sets of proposed modifications are unlawful and invalid.

CalChamber restates our comment in Section I of CalChamber's comments to the third set of proposed modifications, dated October 28, 2020. We respectfully request the Department to withdraw the third and fourth proposed sets of modifications to the text of the California Consumer Privacy Act regulations and restart a new notice period under the APA.

Respectfully,

A handwritten signature in black ink, appearing to read 'Shoeb Mohammed', is written over a horizontal line.

Shoeb Mohammed
California Chamber of Commerce

From: [Jesse Vallejo](#)
To: [Privacy Regulations](#)
Cc: [Kyla Christoffersen Powell](#); [Jaime Huff](#)
Subject: Comments by the Civil Justice Association of California on Fourth Set of Proposed Regulations for the CCPA
Date: Monday, December 28, 2020 3:26:27 PM
Attachments: [image001.png](#)
[CJAC Comments CCPA Revised Regulations 12-28-20.pdf](#)

Hello,

Please find attached the comments by the Civil Justice Association of California on the fourth set of proposed regulations for the California Consumer Privacy Act.

Thank you,

[Jesse Vallejo](#)

Legislative and Communications Coordinator

Mobile [REDACTED] | www.cjac.org



CIVIL JUSTICE
ASSOCIATION OF CALIFORNIA



December 28, 2020

Xavier Becerra, Attorney General
California Department of Justice
1300 I Street, Suite 1740
Sacramento, CA 95814

Lisa B. Kim
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

Re: *Comments by the Civil Justice Association of California on Fourth Set of Proposed Regulations for the California Consumer Privacy Act*

Dear Attorney General Becerra:

The Civil Justice Association of California ("CJAC") appreciates the opportunity to provide comments on this latest version of the proposed regulations implementing CCPA.

CJAC respectfully requests the Office of the Attorney General address the following issues:

1. Clarify that use of the opt-out button is optional since it is duplicative and may be confusing.

The proposed Section 999.306(f) indicates the opt-out button is optional at the outset but then follows with language suggesting it is mandatory. Subsection (f)(1) states the opt-out button "**may** be used in addition to a notice of right to opt-out, but not in lieu of any requirement to post the notice of right to opt-out or a 'Do Not Sell My Personal Information' link" (emphasis supplied). However, subsection (f)(2) states that "Where a business posts the 'Do Not Sell My Personal Information' link, the opt-out button **shall** be added to the left of the text" (emphasis supplied).

We request clarification the button is optional. It appears that (f)(2) is mandating the position of the button only, but the language is unclear. Since the notice of right to opt out or a "Do Not Sell My Personal Information" ("DNS") link is required regardless, the button is duplicative and could also be confusing. Some consumers may believe that merely clicking the toggle-like button effectuates the opt-out, when the button is just another link to the DNS page. In light of this, it is best left to the business to decide whether the button will facilitate the opt-out process on a given web page. We also suggest providing flexibility to businesses with the design and placement of the button, as businesses may find approaches that are simpler and clearer for the consumer.

Accordingly, we recommend revising subsections 999.306(f)(1) and (2) as follows:

(f) Opt-Out Button.

(1) The following opt-out button or one that is similar may be used in addition to posting the notice of right to opt-out, but not in lieu of any requirement to post the notice of right to opt-out or a "Do Not Sell My Personal Information" link as required by Civil Code section 1798.135 and these regulations. **Businesses are not required to use an opt-out button.**

(2) ~~Where~~ **When** a business **chooses to use the opt-out button with** ~~posts~~ the “Do Not Sell My Personal Information” link, the opt-out button shall be added to the ~~left of~~ **next to** the text, **similar to what is as** demonstrated below. The opt-out button shall link to the same Internet webpage or online location to which the consumer is directed after clicking on the “Do Not Sell My Personal Information” link.

(3) The button shall be approximately the same size as any other buttons used by the business on its webpage.

2. Allow businesses to request two forms of identity verification from authorized agents to provide better protection of consumers.

CJAC requests the below language be revised per the below to allow businesses to require two forms of identity verification from authorized agents, which will provide stronger protection of consumers and their information from fraudsters:

§ 999.326 Authorized Agent.

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request **along with two forms of identity verification**. The business may also require the consumer to do either of the following:

- (1) Verify their own identity directly with the business.
- (2) Directly confirm with the business that they provided the authorized agent permission to submit the request.

3. Provide a reasonable implementation period for the latest revisions.

Given the complexity and burden of implementing new regulations, which has been further exacerbated by remote workforces and shutdowns, we ask the Attorney General to specify in the regulations that businesses have at least six to 12 months from final adoption of the regulations to implement them before they are enforced. This will also provide certainty businesses need, especially during these times.

Conclusion

Addressing the forgoing concerns will help reduce unnecessary enforcement and litigation burdens on businesses, the courts, and your Office. We are happy to answer any questions you may have and look forward to the opportunity to work with your Office on improvements to the regulations.

Thank you for your consideration,



Kyla Christoffersen Powell
President and Chief Executive Officer

From: [Lisa LeVasseur](#)
To: [Privacy Regulations](#)
Subject: Comments on Fourth Round of amendments
Date: Monday, December 28, 2020 3:37:10 PM
Attachments: [CCPA Fourth Round Comments.pdf](#)

Dear Ms. Kim,

Please find our written comments on the fourth round of amendments to the CCPA attached.

Warmly,

Lisa LeVasseur

Executive Director, Me2B Alliance

December 28, 2010

Lisa B. Kim
Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
Email: PrivacyRegulations@doj.ca.gov

Re: *OAL File No. 2019-1001-05: NOTICE OF FOURTH SET OF PROPOSED
MODIFICATIONS TO TEXT OF REGULATIONS AND ADDITION OF DOCUMENTS
AND INFORMATION TO RULEMAKING FILE*

Dear Ms. Kim:

Thank you for the opportunity to submit comments in response to the fourth set of proposed modifications made to the regulations regarding the California Consumer Privacy Act (CCPA).

The Me2B Alliance is a non-profit organization founded in 2019 with a mission of performing independent product testing/certification on connected technology—essentially measuring the ethical behavior of technology. Our primary ethos is that *respectful technology* is better for both people (“Me-s”) and businesses (“B-s”). Our ethical foundation for *respectful technology* lies in what we call the Me2B Rules of Engagement, which mirror the attributes of healthy human inter-personal relationships.

Why use the characteristics of healthy human relationships as an ethical north star? Because we *are* in relationships with connected technology: it observes us, talks to us, interacts with us—just like people. When technology treats us with respect, it engenders greater trust in connected products and services, and the companies that provide them.

A crucial principle in the Me2B Rules of Engagement is *Respectful Defaults*:

Respectful Defaults - *In the absence of stated preferences, we default to the most conservative behavior.*

Note this also aligns with the Privacy by Design principle: “Privacy as the default setting.”ⁱ In particular, we strongly suggest that opting-in to information sharing or selling should

be the default standard for Web interactions; it reflects a more respectful default than requiring people to opt-out.

General Problems with Opting-Out

The current opt-out mechanism is problematic on multiple fronts:

1. It only applies to the “sale” of user data and not to sharing of user data, even though portable data can be shared with a service provider, who could sell the data without any notice or consent.
2. It places the burden on the individual to, in essence, opt-in to privacy, which fails to align with the human right of privacy; it also fails the principle of privacy as the default setting in Privacy by Design.
3. It presents significant difficulty in developing a global privacy signal standard, as the European Union in recent decisions has made clear that opt-out is not GDPR compliant.
4. Opting-Out presents a particularly confusing user interface (UI) in communicating a negative/opt-out (see also comments below regarding section 999.315).

In addition to the general comments above, the Alliance would like to submit its views on two discrete but important proposed changes to the draft regulations.

1. 999.306(b)(3): “sells” versus “collects”

Revisions to section 999.306, subd. (b)(3) would “clarify that a business selling personal information collected from consumers in the course of interacting with them offline shall inform consumers of their right to opt-out of the sale of their personal information by an offline method.”

Part of this revision would alter the language in (b)(3) to cover a business that “sells” personal information, rather than “collects” such data from consumer.

This language change is troubling on several fronts. First, it greatly narrows the scope of covered interactions with consumers. Clearly “selling” is a subpart of data “collecting”. Or to be more precise, “selling” is a specific use of data after the act of “collecting.” We believe all people should be notified of information collection whether it’s intended to be “sold” (CCPA definition) or used strictly in the context of the vendor/first party. This is particularly important during the national COVID pandemic, with known mobile data sharing from SDKs installed in apps, which are being shared through service provider loopholes and then sold by subsequent parties in the data supply chains without notice to users.

Second, “selling” is a more ambiguous term than “collecting.” A company theoretically could evade the assumed intent of the provision by adopting a cramped definition of selling data.

Third, allowing data collection, even in the absence of sales, increases security risks for the user. Collection of data entails storing it on third party servers, where it would be subject to outside breaches and other harms.

Finally, while CCPA mostly restricts the “sale” of user data, and the newly-passed CPRA expands to restrict the “sharing” of user data, these two conflicting standards, without any technical consent-sharing mechanisms, present an impossible scenario for end-users or auditors to track the flow of their user data, and ensure that portable data isn’t sold by parties who legally acquired the ‘shared’ user data under CCPA frameworks.

2. 999.315(f): the “opt-out button”

Proposed section 999.315, subd. (f) describes a uniform button (or logo) to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

Usability Issues with Opt-Out

Based on the findings of Cranor et al (listed as a resource in this round of proposed changes) which recommends an interactive simple text statement (“do not sell my data”) without an icon as the most understandable UI per their testing, we are surprised to see the recommendation of an (untested?) generic checkmark icon.

From Cranor et alⁱⁱ:

“None of the tested icons should be used to symbolize Do Not Sell. Instead, the link text should be used on its own or different icons should be developed and tested.... adding any of these icons to the link text introduced misconceptions regarding the opt-out button’s purpose compared to presenting the link text on its own.”

It should be noted that the four icons tested by Cranor et al were all significantly more meaningful than the proposed check-mark button proposed in this revision.

In fact, using a checkmark with a negative statement sets up a particularly challenging UI for people, which is well understood in the art of UI designⁱⁱⁱ.

Additionally, in another listed resource, “An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites”^{iv}:

“In asking for consent, websites should present a clear, affirmative action, and ask visitors for agreement rather than incorporating the consent into default settings, such as pre-checked boxes (Art. 4).”

We contend that mandating opting-out of selling data is tantamount to a default setting allowing the selling of data. Instead, people should be presented with a clear, affirmative [opt-in] action to **allow** the selling of their data.

Location of Opt-Out Signal on Infinite Scroll Pages

Furthermore, the suggested practice under CCPA to place a “Do Not Sell My Information” link in the footer of websites, is not possible for websites with “infinite scrolling” functionality, where new stories or content constantly populates as soon as a user scrolls to the bottom of the page where the footer links exist^v. This concept also doesn’t work on publishers with paywalls – where a user visits a page and is immediately both tracked and identified by javascript pixels on the page, but also unable to click on any elements besides the subscription notices to execute an effort to opt-out of any data sales. GDPR on the other hand, approaches consent from a position where a website can’t use UI/UX tricks, locked-in pop-ups, infinite scrolling and other “scroll & click tricks” to collect consent or make it possible to opt-out. By making this “opt-out” instead of “opt-in,” many users must sometimes navigate purposefully-broken websites that restrict clicks, scrolling, engagements (newspaper paywalls) and prevent users from being able to express their lack of consent for data sales.

Users Are Less Likely to Change Default Settings

Requiring people to opt out of selling their data is essentially a default setting that allows vendors to sell the data of users. Research shows that default settings favor whoever benefits from the default setting.

“The same applies to privacy settings, researchers [have found](#) in [several studies](#).

“Several possible reasons for not changing the default settings exist: cognitive and physical laziness; perceiving default as correct, perceiving endorsement from the provider; using the default as a justification for choice, lacking transparency of implication, or lacking skill,” researchers from the Goethe University Frankfurt and Nelson Mandela Metropolitan University [wrote in 2013](#).^{vi}

“If we assume that marketers, consumers, and policy-makers all share the goal of separating interested from uninterested consumers, our findings suggest some constructive advice regarding the role of defaults. In our research, defaults have a sizable effect, and the best way of controlling these effects may well be to neutralize them as much as possible.”^{vii}

Changing to a Positive Statement

If we were to modify the confusing negative language of the proposed “Do Not Sell” button and instead reword it in a positive manner it would essentially be, “I want data privacy”. This option should be tested and considered.

Opting-In Better Aligns with Judicial Opinions in the EU

Due to the maturity of the GDPR (relative to the CCPA), consent mechanisms have been more deeply scrutinized and tested in the European Union. Consent for data usage must be provided by “clear affirmative action”--i.e. opt-in. Whereas in the CCPA, the individual is defaulted into allowing the sale/sharing of information until they opt-out. The EU and Germany have upheld support for opting-in in the past year, affirming that opt-out is *not* valid consent.

From the Court of Justice of the European Union, October 2019^{viii} [bold text below for emphasis and focus, not from original source]:

*“In today’s judgment, the Court decides that the **consent** which a website user must give to the storage of and access to cookies on his or her equipment **is not validly constituted by way of a prechecked checkbox which that user must deselect to refuse his or her consent.**”*

From the related case, May 28, 2020, the German Federal Court of Justice (*Bundesgerichtshof*, “BGH”) decided on the “Planet49” case regarding cookies^{ix}:

*“The BGH ruled that Section 15 para. 3, sentence 1 TMA must be interpreted in light of and in conformity with Art. 5 para. 3 of the ePrivacy Directive as meaning that the use of cookies for creating user profiles for the purposes of advertising or market research **requires the user’s consent**. Following the decision of the CJEU, the BGH **further ruled that the user’s consent cannot be obtained by way of a pre-ticked checkbox which the user can uncheck.**”*

And from the UK’s ICO (Information Commissioner’s Office), “Consultation: GDPR consent guidance”, March 31, 2017^x:

“Clear affirmative action means someone must take deliberate action to opt in, even if this is not expressed as an opt-in box. For example, other affirmative opt-in methods might include signing a consent statement, oral confirmation, a binary choice presented with equal prominence, or switching technical settings away from the default.

The key point is that all consent must be opt-in consent – there is no such thing as ‘opt-out consent’. Failure to opt out is not consent. You may not rely on silence, inactivity, default settings, pre-ticked boxes or your general terms and conditions, or seek to take advantage of inertia, inattention or default bias in any other way.”

Opting-In Eases Global Privacy Signal Standardization Efforts

Changing from opt-in to privacy to opt-in to selling/sharing data will align this important regulation more closely to the EU approach, which will facilitate the development of a global privacy signal standard. Currently, there is effort in the W3C to develop a global standard for a Global Privacy Control signal that is facing difficulties with reconciling a signal and a default setting that works everywhere.

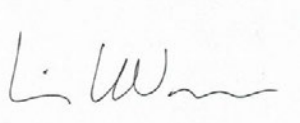
Recommendation

For the reasons stated above we strongly recommend changing the default from an opt-out of selling my data to opt-in to selling my data. Doing so will result in a privacy-respecting and Privacy by Design-compliant default, an easier to understand user-interface, and an easier path to a global privacy signal standard.

In the absence of this, positive language of the control/button (or logo) such as, “I want data privacy” (yes/no) should be evaluated.

On behalf of the Me2B Alliance, thanks again for the opportunity to provide feedback on this important regulation for California, the US and the world.

Sincerely,



Lisa LeVasseur
Executive Director, Me2B Alliance

ⁱ https://en.wikipedia.org/wiki/Privacy_by_design

ⁱⁱ "CCPA Opt-out Testing – Phase Two", Cranor, Habib, et al, May 28, 2020. [CCPA Opt-Out Icon Testing - Phase 2 - DNS \(ca.gov\)](#)

ⁱⁱⁱ [Checkboxes - Checkbox label negating - User Experience Stack Exchange](#)

^{iv} "An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites", Habib, Zou et al, USENIX Symposium on Usable Privacy and Security (SOUPS) 2019. August 11–13, 2019, Santa Clara, CA, USA.

^v <https://oag.ca.gov/data-broker/registration/193828>

^{vi} "Default settings for privacy -- we need to talk" Albert Ng, December 21, 2019, CNET. [Default settings for privacy -- we need to talk - CNET](#)

^{vii} Defaults, Framing and Privacy: Why Opting In-Opting Out¹ (columbia.edu) Defaults, Framing and Privacy: Why Opting In-Opting Out

^{viii} "Storing cookies requires internet users' active consent", Court of Justice of the European Union PRESS RELEASE No 125/19 Luxembourg, 1 October 2019 Judgment in Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände–Verbraucherzentrale Bundesverband eV v Planet49 GmbH.

^{ix} "Germany: The decision of the German Federal Court of Justice on cookie consent – and further implications", *Global Compliance News*, Julia Kaufman, July 19, 2020. [Germany: The decision of the German Federal Court of Justice on cookie consent - and further implications \(globalcompliancenews.com\)](#)

^x "Consultation: GDPR consent guidance", Information Commissioner's Office, March 31, 2017. [draft-gdpr-consent-guidance-for-consultation-201703.pdf \(ico.org.uk\)](#)

From: [Jacob Snow](#)
To: [Privacy Regulations](#)
Subject: Privacy and Consumer Organization Comments on Proposed CCPA Rulemaking
Date: Monday, December 28, 2020 3:53:15 PM
Attachments: [2020.12.28 - Fourth Coalition Comments re OAG Regs.pdf](#)

Attached are comments from a coalition of privacy and consumer protection organizations regarding the Fourth Set of Modifications to Proposed Regulations under the California Consumer Privacy Act.

Best,

Jake Snow
Technology and Civil Liberties Attorney
ACLU of Northern California
he/him/his | [REDACTED] | @snowjake

**Comments to the
California Office of the Attorney General**

**Notice of Fourth Set of Modifications
to Proposed Regulations under
The California Consumer Privacy Act**

Submitted via Email to PrivacyRegulations@doj.ca.gov

December 28, 2020

On Behalf of the Following Organizations:



The “Do Not Sell My Personal Information” Icon Will Help Ensure That Californians Are Made Aware of Their Privacy Rights.

The undersigned organizations sincerely appreciate your ongoing efforts to establish a workable, standardized icon to signal to consumers their right to opt-out of the sale of their personal information under the California Consumer Privacy Act.

The proposed icon is an improvement on the icon recommended in earlier drafts of the regulations, and more clearly conveys the presence of privacy choices. Testing by Professor Lorrie Faith Cranor and the CyLab Security and Privacy Institute at Carnegie Mellon University demonstrated that any icon divorced from an accompanying tagline is likely to be misinterpreted by consumers.¹ This icon and the “Do not sell my personal information” tagline will help ensure that Californians are made aware of their privacy rights.

Condensing the universe of concepts associated with privacy, choice and specifically the sale of personal information to a single, standardized icon is a monumental challenge. In responding to the issues we've raised in previous comments, your Office has demonstrated a commitment to developing workable solutions to the most difficult policy areas of the California Consumer Privacy Act. We remain hopeful that, despite the unavoidable potential for this icon to be misconstrued, these regulations will build broad public awareness and help make the privacy-choices icon iconic.

Signed:

American Civil Liberties Union of California

Common Sense Kids Action

Electronic Frontier Foundation

Privacy Rights Clearinghouse

¹ Cranor, *et al.*, CCPA Opt-Out Icon Testing – Phase 2, p.5 (May 28, 2020).

From: [Halpert, Jim](#)
To: [Privacy Regulations](#)
Cc: [Kingman, Andrew](#)
Subject: State Privacy & Security Coalition -- Comments re AG's Office CCPA 4th Modified CCPA Rules December 28 2020.DOCX
Date: Monday, December 28, 2020 5:07:33 PM
Attachments: [State Coalition -- Comments re AG's Office CCPA 4th Modified CCPA Rules December 2u 2020.DOCX](#)

Dear Ms. Kim,

Attached are the State Privacy & Security Coalition's comments on the latest version of the proposed CCPA rule revisions.

We would very much appreciate your office reviewing the entirety of these comments carefully.

Respectfully submitted – Jim Halpert

Jim Halpert
Partner

T
M

DLA Piper LLP (US)
dlapiper.com
<https://www.dlapiper.com/en/us/people/h/halpert-jim/?tab=credentials>

The information contained in this email may be confidential and/or legally privileged. It has been sent for the sole use of the intended recipient(s). If the reader of this message is not an intended recipient, you are hereby notified that any unauthorized review, use, disclosure, dissemination, distribution, or copying of this communication, or any of its contents, is strictly prohibited. If you have received this communication in error, please reply to the sender and destroy all copies of the message. To contact us directly, send to postmaster@dlapiper.com. Thank you.

STATE PRIVACY & SECURITY COALITION

December 28, 2020

Lisa B. Kim, Privacy Regulations Coordinator
California Department of Justice
300 Spring Street, 1st Floor
Los Angeles, CA 90013
PrivacyRegulations@doj.ca.gov

Re: Comments Regarding Title 11(1)(20): Fourth Set of Proposed Modification of Text of Regulations

I. Introduction

The State Privacy & Security Coalition is a coalition of 29 companies and 7 trade associations across the retail, payments, communications, technology, fraud prevention, tax preparation, automotive and health sectors. We work for laws and regulations at the state level that provide strong protection for consumer privacy and cybersecurity in a consistent, workable manner that reduces consumer confusion and unnecessary compliance burdens and costs.

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

We appreciate the clarifications that the 4th modifications have made to the examples in § 999.306(b) that align them much more closely with the requirements of the statute and avoid significant potential consumer confusion.

On the other hand, we remain very concerned that proposed § 999.326(a) would seriously weaken authentication of authorized agents when they ask to exercise right to know and data deletion rights on behalf of state residents and result in a material increase in California residents' exposure to account takeovers from fraudulent authorized agent requests. We understand that your office is not requesting comments on this issue, but urge you to review our comments below, as they more fully explain the risks to privacy associated with the proposed changes to § 999.326(a).

In addition, the "do not sell" icon that is now proposed in § 999.306(f) is not well-designed "to promote consumer awareness of the opportunity to opt-out of the sale of personal information" and should instead be developed per the procedures set forth in § 1798.185(a)(4)(C) of the CPRA, instead of being thrust into the CCPA regulations at this late juncture. Furthermore, the language in § 999.306(f)(2) is ambiguous and should be clarified, if this provision is incorporated in the next version of final rules.

STATE PRIVACY & SECURITY COALITION

1. The proposed restriction in § 999.326(a) on authenticating third party right to know and data deletion requests should be clarified or stricken in the final rule to reduce risk of pretexting and fraud.¹

Right to know and data deletion requests pose greater data security risk because they allow a fraudulent requester to obtain personal data, or delete or otherwise manipulate account information and potentially hijack the account. The Final Rules impose greater authentication requirements for right to know and data deletion requests because of the heightened security and privacy risks these rights pose if wielded by fraudsters or hackers.

These very same risks counsel strongly against cutting back on businesses' leeway to authenticate right to know and data deletion requests filed by a purported authorized agent.

We are unclear about the rationale for shifting the submission of proof of the signed permission authorizing the agent from the consumer to the authorized agent. While the addition of such an option might be workable, allowing a business to do only one (and not both) of further authentication steps risks increased fraud.

We request the following amendment to § 999.326(a), as follows:

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require that the consumer authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to do ~~either of do~~ the following:

A business should not be barred from both asking the consumer to verify their identity with the business *and* obtaining confirmation that the consumer provided the agent permission to submit the request. Both pieces of information are necessary to confirm that a request is not fraudulent. Otherwise, a fraudster can either: (1) submit a request in the name of an actual consumer who has not authorized the request, or (2) create a fake account in the same name as an actual consumer, thereby making the fake account appear more real, but submit the access or deletion request for the actual consumer's account. For these reasons, both confirmations are *very important* to prevent fraudulent requests for these rights that, as the final regulations acknowledge, pose greater risks to consumers.

2. The Proposed Icon is Premature and Should Be Addressed in the CPRA Rulemaking

The CPRA requires a rulemaking in the next [18 months] that will establish a process to select an effective icon. Selecting an icon without any procedure for doing so is unwise because a consumer testing process is the best way to ensure that the icon is understood and provides a clear, positive user experience. Furthermore, establishing the icon now would either preempt the process approved by the

¹ This section contains a more detailed explanation of risks associated with the proposed revision to this section and we respectfully request that your Office review this section of our comments even though the latest version of the proposed rules does not make a change to the previous proposal.

STATE PRIVACY & SECURITY COALITION

voters, or would result in a second icon being chosen under the CPRA development process, needlessly confusing California consumers.

The proposed rules are actually the *seventh* proposed version of CCPA rules. These repeated changes needlessly complicate CCPA compliance during an economic downturn and in the case of a second icon, would defeat the purpose of branding a symbol of how to exercise the CCPA do not sell right.

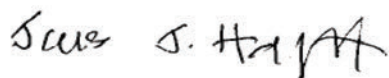
For all these reasons, it is better to wait, remove this provision, and follow the CPRA process in selecting the icon.

However, if the Attorney General's Office decides to add a "do not sell" icon provision, it should clarify the language in proposed § (f)(2), to make clear that the location requirements apply, "If the business posts the icon." This could be accomplished by amending the text as follows:

(2) If a business posts the icon, it shall ~~Where a business posts the "Do Not Sell My Personal Information" link, add the opt-out button shall be added to the left of the location text where a business posts the "Do Not Sell My Personal Information" link,~~ as demonstrated below. The opt-out button shall link to the same Internet webpage or online location to which the consumer is directed after clicking on the "Do Not Sell My Personal Information" link.

This change would avoid potential confusion between the text of paragraph (1), which states that posting the icon is voluntary, and paragraph (2) which prescribes where to post the icon, but could be read as requiring that the icon be posted in all cases. Mandating use of the icon without user testing and the process to be developed under the CPRA would compound the problems posed by hasty implementation of the icon.

Respectfully submitted,



Jim Halpert, Counsel
State Privacy & Security Coalition