

**From:** [REDACTED]  
**To:** [Privacy Regulations](#)  
**Subject:** RE: Comment on proposed regulatory amendments  
**Date:** Tuesday, October 13, 2020 2:43:22 AM

---

[REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED]  
[REDACTED]

---

[REDACTED]

---

**From:** [REDACTED]  
**Sent:** Monday, October 12, 2020 12:58 PM  
**To:** 'PrivacyRegulations@doj.ca.gov' <PrivacyRegulations@doj.ca.gov>  
**Subject:** Comment on proposed regulatory amendments

[REDACTED]  
[REDACTED]  
[REDACTED]

---

The proposed addition to § 999.315 seeks to further complicate the opt-out right regulations, which are already overreaching and invite fraud and abuse, by imposing an additional series of confusing stipulations that would make it significantly harder for online businesses to comply in good faith with the regulations.

First, the stipulation proposed in (h)(1) for counting a number of steps is confusing, nonsensical, and completely arbitrary. **It would significantly penalize, to no good purpose, businesses like mine that use webforms as a means of processing CCPA requests.** By setting an arbitrary standard for number of clicks or number of steps, this stipulation would arbitrarily penalize the use of CAPTCHAs or other means to ensure that the webform is being submitted by a human user rather than bots, who are drawn to webforms like moths to a flame. Since the regulations are written to require that businesses respond promptly to ALL requests, even obviously fraudulent ones, **this expectation would devastate small businesses like mine.** I have only modest online traffic, but if I post a webform without a CAPTCHA or other means of separating human users from bots, I may get HUNDREDS of obviously fraudulent spam submissions a day. As a sole proprietor, I simply do not

have the time to handle that volume of responses.

**Furthermore, this stipulation would effectively require that all means of submitting requests involve the same number of steps, which is obviously and fundamentally ridiculous.** For a consumer who has an established ongoing relationship with a business -- for example, a customer who logs into an account with an online retailer -- the process of submitting an opt-in or opt-out request may be as simple as a single click on their account settings page; in that case, the business already knows who the consumer is and has mechanisms in place for managing their information. For a website visitor who does NOT have an established relationship with the business, they will almost certainly need to indicate to the business who they are (and that they're human) so that the business can respond to and process their request. Once a business has received an opt-out request from a given consumer, processing an opt-in-request from the same individual is an inherently simpler process.

**These procedures clearly, logically, NECESSARILY involve a different number of steps,** so to stipulate that they not only shouldn't but may NOT by law require a different number of steps is absurd. That is not practical, practicable, or enforceable, and represents a further unwarranted overreach by OAG.

I strongly recommend that (h)(1) be struck in its entirety. If OAG attempts to revise the wording of this provision in an effort to clarify this mess, it's likely to compound rather than resolve the issues it presents.

The proposed example in (5)(h) is in some respects even more concerning. I grasp that the intent is to discourage businesses from "burying" opt-out instructions in voluminous text, but stipulating that "the business shall not require to search or scroll through the text of a privacy policy or similar document or webpage" would effectively allow OAG to set arbitrary, undefined expectations for what constitutes excessive "searching or scrolling." Even a fairly straightforward Do Not Sell My Personal Information webpage, containing specific instructions for submitting requests, may require a fair bit of scrolling if a consumer accesses the page from a mobile phone rather than a desktop computer. It also threatens to penalize businesses for minor technical errors, such as an anchor link (that is, a hyperlink pointing to a specific anchor at a specific position on a given webpage) that fails to correctly resolve due to connection issues beyond the business's reasonable control.

I do not object in principle to the proposed text of section (h), but the illustrative examples offer a disturbing indication that OAG's intention is to find ways to arbitrarily penalize businesses for minor procedural issues. Many business are striving in good faith to meet the often confounding expectations established in these regulations, but OAG seems determined to make that as difficult as possible.

My recommendation is to strike (h)(1) and (h)(5) in their entirety.

Regarding the proposed addition to § 999.326, the proposed change is, refreshingly, a straightforward and sensible clarification of the existing text.

---

---

[REDACTED]

**From:** [Adam Schwartz](#)  
**To:** [Privacy Regulations](#)  
**Subject:** EFF comments on proposed Cal DOJ regulations re CCPA (OAL file no. 2019-1001-05)  
**Date:** Tuesday, October 20, 2020 12:46:38 PM  
**Attachments:** [2020-10-20 - EFF comments re Cal DOJ proposed regs re dark patterns.pdf](#)

---

Salutations. EFF submits the attached comments in support of the "dark patterns" regulations proposed by the California DOJ at Section 999,315(h) of the third set of proposed modifications of CCPA regulations, published on October 12. Sincerely, -Adam

--

Adam Schwartz | Senior Staff Attorney  
Electronic Frontier Foundation  
815 Eddy St. | San Francisco, CA 94109  
[REDACTED] [REDACTED]  
Pronouns: he/him/his





October 20, 2020

BY EMAIL (PrivacyRegulations@doj.ca.gov)

**Re: EFF comments on proposed Cal DOJ regulations on “dark patterns”**  
(OAL File No. 2019-1001-05)

Salutations:

The Electronic Frontier Foundation (EFF) writes in support of the proposed regulations from the California Department of Justice (DOJ) to protect against what are commonly called “dark patterns.” These are manipulative user experience designs that businesses use to trick consumers into surrendering their personal data. Specifically, we support the proposed regulations at Section 999.315(h), within the third set of proposed modifications of CCPA regulations, which the California DOJ published on October 12.

The California Consumer Privacy Act (CCPA) created a right of consumers to opt-out of the sale of their personal data. Businesses might use dark patterns to hamstring this CCPA right. The proposed DOJ regulations will secure this right by stopping dark patterns. Among other things, the proposed regulations would:

- Require opt-out processes to be “easy” and “require minimal steps.”
- Ban opt-out processes “designed with the purpose or having the substantial effect of subverting or impairing a consumer's choice to opt-out.”
- Limit the number of steps to opt-out to the number of steps to later opt back in.
- Ban “confusing language” such as “double negatives” (like “don’t not sell”).
- Ban the necessity to search or scroll through a document to find the opt-out button.

For more on EFF’s opposition to dark patterns, please see:  
[eff.org/deeplinks/2019/02/designing-welcome-mats-invite-user-privacy-0](https://eff.org/deeplinks/2019/02/designing-welcome-mats-invite-user-privacy-0).

For the DOJ’s proposed regulations, please see:  
[oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-third-set-mod-101220.pdf](https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-third-set-mod-101220.pdf)

Sincerely,

Adam Schwartz  
Senior Staff Attorney



**From:** [Zoe Vilain](#)  
**To:** [Privacy Regulations](#)  
**Cc:** [Pierre Valade](#)  
**Subject:** To the attention of Deputy Attorney General Kim - Comments with regards to CCPA  
**Date:** Tuesday, October 27, 2020 9:06:48 AM  
**Attachments:** [20201027 - 2121 Atelier Inc - comments 3 on CCPA to California GA.pdf](#)

---

*To the attention of Deputy Attorney General Kim*

Dear Deputy Attorney General Kim,

Please find attached a letter to your attention containing our comments regarding the third set of proposed modifications to the CCPA regulation.

I am available for any queries,

Best regards,

Zoé Vilain

Jumbo Privacy

[www.jumboprivacy.com](http://www.jumboprivacy.com)



**Jumbo Privacy**  
**2121 Atelier Inc.**  
32 Bridge Street, 2<sup>nd</sup> Floor  
Brooklyn, NY 11201  
USA

**Lisa B. Kim**  
**Deputy Attorney General**  
California Department of Justice  
Consumer Law Section – Privacy U.  
300 South Spring Street, 1<sup>st</sup> Floor  
Los Angeles, CA 90013  
USA

October 27<sup>th</sup>, 2020

*By email ([privacyregulations@doj.ca.gov](mailto:privacyregulations@doj.ca.gov))*

**Subject: Written comments regarding the proposed CCPA regulations**

Dear Deputy Attorney General Kim,

We write to you concerning the third set of proposed modifications to the California Consumer Privacy Act (“CCPA”) made on October 12<sup>th</sup>, 2020.

As mentioned in our previous letters to you dated respectively February 25, 2020, and March 27<sup>th</sup>, 2020, 2121 Atelier Inc. d/b/a Jumbo Privacy<sup>1</sup> has been acting as registered Authorized Agent in California for California residents, thanks to the introduction of such a role in the CCPA on Feb 1, 2020. Jumbo Privacy notably represents California consumers who request deletion of their personal information from consumer-selected businesses falling under the scope of the CCPA. Requests sent to a business by Jumbo Privacy on behalf of a consumer all contain the identification of the consumer and a signed mandate executed through and stored by a trusted third-party certifier, authorizing Jumbo to act on behalf of the consumer.

As of the date of this letter, 73% of businesses we are sending Requests to, are refusing to comply with our Requests based on the argument that such businesses refuse to comply with third-party requests to delete the personal information and/or require the consumer to take further action directly. Jumbo Privacy has therefore been pushing back against such refusals by quoting sections 1798-135 of the CCPA and § 999.315.e of the California Attorney General text of Regulations and indicating that such refusals are a restriction of consumer’s rights.

We are concerned that proposed modifications to the CCPA might highly restrict the efficiency and opportunity for consumers to mandate an Authorized Agent. Therefore, we are addressing once

---

<sup>1</sup> Available at <https://www.jumboprivacy.com/>

Jumbo Privacy  
32 Bridge Street, 2<sup>nd</sup> Floor  
Brooklyn, NY  
11201

again our suggestions and comments to the proposed rulemakings of the California Attorney General regarding provisions related to the concept of “Authorized Agent”.

Specifically, our experience has demonstrated that every business falling under the scope of the CCPA should implement a dedicated communication channel with Authorized Agents, preferably an email address for the purpose of simplicity, to facilitate the management of requests made on behalf of consumers they represent. Indeed, if businesses force Authorized Agents to use web forms or postal mail, then Authorized Agents will not be able to manage privacy requests on behalf of their mandators efficiently. We also read proposed amendments to Section 999.326(1) and (3) to place unnecessary hurdles between Authorized Agents and the effective and efficient consumer control of private information.

Consumers that mandate Jumbo Privacy as Authorized Agent to submit their requests are doing so to avoid having to manage such requests themselves, notably to avoid receiving numerous emails from businesses to confirm the validity of their requests or their identity. We believe that allowing a business to contact the consumer directly for additional identity verification after receipt of a request by mandate through an Authorized Agent, that has already verified the identification of the consumer, would lead to additional heavy processes and unnecessary delays to the processing of the original request.

Security of personal information and verification of identity are a priority for Jumbo Privacy when acting as an Authorized Agent. We understand the importance of ensuring the validity of received requests to know or requests to delete. However, we would like to emphasize that providing an option for business to require the consumer verification of identity or request made through an agent might highly impair consumer rights by restraining the practicality to mandate an Authorized Agent.

We believe from requests we have made so far on behalf of consumers, that businesses may be tempted to use the presently proposed revisions to bypass an Authorized Agent’s authority to act on behalf of said consumers. Therefore, we would suggest these additions to ensure that businesses may verify a consumer’s identity only if the business can establish that the Authorized Agent has not provided reasonable proof of such consumer’s identity or the existence of a valid mandate. These additions would prevent any unnecessary verification by the business, ensuring respect of the consumer’s privacy rights.

Regarding Article § 999.326 - Authorized Agent, please find below our proposed amendments highlighted in yellow below:

« (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:

~~(1) Provide the authorized agent signed permission to do so.~~

*(2)(1) Verify their own identity directly with the business in case the authorized agent has not provided reasonable proof that the authorized agent has previously verified the consumer's identity.*

*(3)(2) Directly confirm with the business that they provided the authorized agent permission to submit the request in case the authorized agent has not provided reasonable proof of the existence of the signed mandate.*

*(b) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4121 to 4130.*

*(c) An authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer's information.*

*(d) An authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purposes other than to fulfill the consumer's requests, verification, or fraud prevention. »*

We remain of course at your disposal for any query,

Sincerely,

Zoé Vilain



Chief Privacy and Strategy Officer  
Jumbo Privacy

Cc: Stacey Schesser, Supervising Deputy Attorney General  
Privacy Regulations Coordinator, California Department of Justice

**From:** [Eric Ellman](#)  
**To:** [Privacy Regulations](#)  
**Subject:** Third Set of Proposed Modifications  
**Date:** Tuesday, October 27, 2020 5:40:24 PM  
**Attachments:** [image001.png](#)  
[image002.png](#)  
[image003.png](#)  
[CCPA Regulations Comment Letter Third Set of Modifications.pdf](#)

---

To Whom It May Concern,

On behalf of the Consumer Data Industry Association, please find attached CDIA's comment on the Department of Justice's [Third Set of Proposed Modifications](#) to CCPA Regulations.

Respectfully submitted,  
Eric J. Ellman

.....  
Eric J. Ellman | [Senior Vice President, Public Policy and Legal Affairs](#) | Consumer Data Industry Association | Direct: [REDACTED] | [REDACTED] | 1090 Vermont Ave., NW, Suite 200, Washington, DC 20005, USA | CDIA: Empowering Economic Opportunity | Founded in 1906 | Please visit our blogs, [Federal Review](#), [Judicial Review](#), and the [Background Screening Information Center \(BaSIC\)](#)





Consumer Data Industry Association  
1090 Vermont Ave., NW, Suite 200  
Washington, D.C. 20005-4905

P 202 371 0910

Writer's direct dial: [REDACTED]

[CDIAONLINE.ORG](http://CDIAONLINE.ORG)

October 28, 2020

*Via Electronic Delivery to [privacyregulations@doj.ca.gov](mailto:privacyregulations@doj.ca.gov)*

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

**RE: Third Set of Modifications to California Consumer Protection Act Regulations**

Dear Ms. Kim,

The Consumer Data Industry Association submits this comment letter in response to the California Office of the Attorney General's Third Set of Proposed Modifications to the California Consumer Privacy Act ("CCPA") Regulations.

The Consumer Data Industry Association ("CDIA") is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others.

CDIA is the voice of the consumer reporting industry, representing consumer reporting agencies, including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity all over the world, helping ensure fair and safe transactions for consumers, facilitating competition, and expanding consumers' access to financial and other products suited to their unique needs.

CDIA members have been complying with laws and regulations governing the consumer reporting industry for decades. Members have complied with the Fair Credit Reporting Act ("FCRA"), which has been called the original federal consumer privacy law. The FCRA governs the collection, assembly, and use of consumer report information and provides the framework for the U.S. credit reporting system. In particular, the FCRA outlines many consumer rights with respect to the use and accuracy of the information contained in consumer reports. Under the FCRA, consumer reports may be accessed only for permissible purposes, and a consumer has the right to dispute the accuracy of any information included in his or her consumer report with a consumer reporting agency ("CRA").

CDIA members have been at the forefront of consumer privacy protection. Fair, accurate, and permissioned use of consumer information is necessary for any CDIA member client to do business effectively.

CDIA appreciates the thorough work of the Department of Justice (“Department” or “DOJ”) in finalizing the CCPA regulations. However, CDIA has serious concerns regarding the second grouping of proposed changes in this third set of modifications, specifically the changes to section 999.315(h) relating to opt-out requests. As we describe in greater detail below, the “illustrative examples” actually impose restrictions that do not implement any particular provision in the CCPA or the implementing regulations and exceed the law’s authorization for the Department to adopt regulations “necessary to further the purposes of” the law. See Cal. Civ. Code § 1798.185(b)(2) (emphasis added).

Additionally, imposing new requirements and restrictions with little notice makes compliance with those requirements very difficult from an operational standpoint. CDIA therefore respectfully requests at least 6 months of delayed enforcement on any changes the DOJ adopts.

To assist your office in promulgating clear and effective regulations that allow businesses to best support customers and consumers, CDIA offers the following comments on proposed section 999.315(h).

\* \* \*

In this third set of proposed modifications to the CCPA regulations, the Department proposes to require that the methods for opting out must be “easy for consumers to execute and . . . require minimal steps to allow the consumer to opt-out.” The proposal also would prohibit use of a method designed with the purpose or that has the substantial effect of subverting or impairing a consumer’s choice to opt out.

The proposal then sets out what it refers to as “illustrative examples” of these two principles. However, the “illustrative examples” do not read as examples of methods that would or would not be easy to execute and require minimal steps to effective. Instead, the “examples” read as new requirements and restrictions not contemplated by the statute, that are not “necessary to further the purposes of the statute,” and that are otherwise problematic to the goals of the CCPA.



**1. The proposed restriction that the number steps to opt out may not exceed the number of steps to opt in.**

First, the proposal includes an illustrative example providing that a business's opt out method may not require more steps than the business's opt in process. The example also provides specifics as to how to count the steps to compare the two processes.

ISSUES: This proposal is not just an illustrative example but a strict limitation on how a business may set up its opt out and opt in processes, demonstrated by the strict guidance on how to "count" how many steps a process has. This is a specific restriction on the form businesses may use to receive verifiable consumer requests not contemplated in the statute or current regulations.

Additionally, this restriction conflicts with existing regulation section 999.315(b), which provides that businesses must consider the methods by which they interact with consumers *along with* ease of use for the consumer. Businesses that deal in sensitive consumer information, like CDIA members, have established systems by which they interact with consumers, and a requirement to minimize the number of steps in submitting a request conflicts with the requirement to consider both ease of use *and* the normal methods of interaction.

PROPOSED SOLUTION: Replace the limitation on the number of steps a business may use in its opt out process with an instruction that for purposes of section 999.315(b), "ease of use by the consumer" includes considering the number of steps an opt out process takes.

**2. The restriction that the opt-out method may not use double negatives or other "confusing language."**

The second proposed illustrative example provides that a business may not use "confusing language, such as double-negatives" in the opt out process.

ISSUES: Banning "confusing language" is an overbroad prohibition lacking authorization in the statute.

Additionally, other than noting that double negatives are confusing, this illustrative example provides no guidance as to what is or could be "confusing" to consumers. Prohibiting an undefined category of language thus raises due process concerns. Similarly, prohibiting an undefined category of speech also raises serious First Amendment concerns.

PROPOSED SOLUTION: Strike this section.

**3. The restriction that a business may not require consumers to click through or listen to reasons not to opt out.**

The third illustrative example prohibits business from requiring consumers to click through or listen to reasons not to opt out.

ISSUES: This is a prohibition on content a business may include in its opt out flow, not an illustrative example of “ease of use.” The CCPA opt out right only applies to certain data, for example, and a business should be able to educate a consumer about what effect an opt out does, and does not, have. Additionally, consumers might not understand the nature of the right, such as confusing the CCPA “opt out” with the FCRA’s prescreen opt out, which applies to data to which the CCPA opt out does not apply. If a consumer was seeking to exercise their federal right to opt out of prescreened solicitations, for example, CDIA members should be permitted to explain to a consumer that exercising their CCPA opt out right would not have the same effect. Without specific definitions or limitations, this prohibition could discourage businesses from including helpful, explanatory language that could help consumers navigate their choices under the CCPA.

Furthermore, as a content restriction without any guidance on what it means by “reasons not to opt out,” this prohibition also raises serious due process and First Amendment concerns.

PROPOSED SOLUTION: Strike this section.

**4. The restriction that the business may not require a consumer to provide personal information not necessary to implement the request.**

The fourth illustrative example provides that a business may not require in its opt out process that the consumer provide personal information “not necessary to implement the request.”

ISSUES: The CCPA does not restrict what information a business can request in order to effectuate a consumer’s opt out, so this restriction exceeds the scope of the statute. The CCPA already prohibits, at Cal. Civ. Code § 1798.130(a)(7), a business from using personal information obtained for verification of a request for any purpose other than verification.

Additionally, CDIA has due process concerns with this restriction, as there is no guidance on how a business is expected to assess whether a particular data point is or is not necessary to implement a request on an individual, let alone a global, scale.

Finally, businesses have to endeavor to match opt out requests to data on a particular consumer, and imposing a restriction on required data points complicates that mandate because matching is not always a straightforward task, given the variety of data that companies may collect and the variety of fields that data may contain. A business may be able

to improve its ability to match if it requests more data points. Without guidance as to what information the AG considers to be "not necessary" for this process, however, there is no way for a company to assess whether they comply with this standard.

PROPOSED SOLUTION: Strike this section.

5. The restriction that the business may not require a consumer to search or scroll through the text of a "privacy policy or similar document or webpage" to locate the opt-out mechanism.

The fifth illustrative example provides that a business may not require a consumer to search or scroll through the text of "a privacy policy or similar document or webpage" to exercise an opt out.

ISSUES: This proposal is confusing, as it is not clear what counts as "a privacy policy or similar document or website." The CCPA statute and current regulations already provides guidance on the placement of the Do Not Sell My Personal Information link.

Furthermore, prohibiting the inclusion of information alongside the opt out mechanism raises serious due process and First Amendment concerns. Without clarity as to what the AG finds objectionable, businesses are not equipped to comply with this restriction.

PROPOSED SOLUTION: Strike this section.

\* \* \*

Thank you for the opportunity to share its views on the proposed regulations. Please contact us if you have any questions or need further information based on comments.

Sincerely,



Eric J. Ellman  
Senior Vice President, Public Policy & Legal Affairs

**From:** [MacGregor, Melissa](#)  
**To:** [Privacy Regulations](#)  
**Subject:** SIFMA Letter to California AG re CCPA 3rd Amendments  
**Date:** Wednesday, October 28, 2020 7:11:47 AM  
**Attachments:** [SIFMA Letter to California AG re CCPA 3rd Amendments.pdf](#)

---

Please see the attached letter regarding the third proposed amendments to the CCPA regulations.

Please let me know if you have any questions.

Thanks.



October 28, 2020

VIA EMAIL TO: [privacyregulations@doj.ca.gov](mailto:privacyregulations@doj.ca.gov)  
The Honorable Xavier Becerra  
Attorney General, State of California  
1300 I Street  
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

**Re: Proposed 3<sup>rd</sup> Amendment to California Consumer Privacy Act Regulations**

Dear Attorney General Becerra,

The Securities Industry and Financial Markets Association ("SIFMA")<sup>1</sup> appreciates this opportunity to comment on the third set of proposed modifications to the text of the California Consumer Privacy Act ("CCPA") regulations. SIFMA commends your office for closely reviewing comments and making necessary changes when warranted. SIFMA previously submitted comments on the proposed CCPA regulations last December.<sup>2</sup>

While SIFMA commends the additional clarity in § 999.315, we believe that subsection (H)(1) is potentially confusing and subjective. We appreciate the principle that it must be equally easy to opt-in or out-out of the sale of personal information, but by including the language "opt-in to the sale of personal information after having previously opted out," the Department may be inadvertently creating confusion. We request that the language be simplified to only address customers' opt-in or opt-out actions and be consistent throughout the paragraph. Additionally, it is difficult to identify the "first indication by the

---

<sup>1</sup> SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate for legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).

<sup>2</sup> SIFMA Comment Letter to The Honorable Xavier Becerra dated December 6, 2019 (available at <https://www.sifma.org/resources/submissions/proposed-california-consumer-privacy-act-regulations-ccpa-rules/>).

consumer to the business of their interest to opt-in.” We request that the Department remove this language and replace it with “a request to opt-in is measured from when the consumer clicks to consent to opt-in.” This would bring the opt-in language in line with the opt-out language and remove the ambiguity around “first indication...of their interest” as that can be judged in multiple ways.

SIFMA greatly appreciates the consideration of these issues and would be pleased to discuss these comments in greater detail. If you have any questions or need any additional information, please contact me at [REDACTED].

Sincerely,

Melissa MacGregor  
Managing Director & Associate General Counsel

cc: Kimberly Chamberlain, Managing Director & Associate General Counsel, SIFMA

**From:** [Maureen Mahoney](#)  
**To:** [Privacy Regulations](#)  
**Subject:** CR comments on third set of proposed modifications to the CCPA regs  
**Date:** Wednesday, October 28, 2020 9:52:03 AM  
**Attachments:** [CR Comments on 3rd Set of Modifications to CCPA Regs.pdf](#)  
[CR CCPA-Are-Consumers-Digital-Rights-Protected\\_092020\\_vf.pdf](#)

---

Dear Ms. Kim,

Attached, please see Consumer Reports' comments on the third set of modifications to the proposed CCPA regulations. I've also attached CR's recent report, *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?* which I'd like to submit to the record as well.

Please let me know if you need any additional information, and thank you for your help -

Best,  
Maureen

--

Maureen Mahoney, Ph.D.  
Policy Analyst

o

m

[CR.org](#)



PLEASE NOTE: My email address has changed. Please begin using  
[REDACTED] for all future correspondence.

\*\*\*

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.

\*\*\*



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 Reports<sup>1</sup> 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.<sup>2</sup> 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.<sup>3</sup> Consumer Reports has recently documented that some consumers are finding it very difficult to opt out of the sale of their information.<sup>4</sup> 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

---

<sup>1</sup> 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.

<sup>2</sup> 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>.

<sup>3</sup> *Id.* at §999.315(h)(1)-(5).

<sup>4</sup> 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](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.”<sup>5</sup> 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.<sup>6</sup> 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.<sup>7</sup>

---

<sup>5</sup> § 999.315(h).

<sup>6</sup> *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>.

<sup>7</sup> 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.<sup>8</sup> 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.<sup>9</sup> 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.<sup>10</sup> Similarly, in late 2016, the FTC took action against Ashley Madison for using fake profiles to trick consumers into upgrading their membership.<sup>11</sup> 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.<sup>12</sup> 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.<sup>13</sup> 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

---

<sup>8</sup> 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.

<sup>9</sup> 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.

<sup>10</sup> 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](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.

<sup>11</sup> 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.

<sup>12</sup> 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.

<sup>13</sup> § 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.”<sup>14</sup> 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.

---

<sup>14</sup> § 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.<sup>15</sup> 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.<sup>16</sup> 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.”<sup>17</sup> 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.

---

<sup>15</sup> § 999.315(h)(5).

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

<sup>17</sup> 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.<sup>18</sup> 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.<sup>19</sup> 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.

---

<sup>18</sup> 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>.

<sup>19</sup> § 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.”<sup>20</sup> 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.<sup>21</sup> 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.<sup>22</sup> Some companies claim that because data is not necessarily transferred for money, it does not constitute a sale.<sup>23</sup> 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.<sup>24</sup>

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,<sup>25</sup> 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

---

<sup>20</sup> § 999.315(g)

<sup>21</sup> 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>.

<sup>22</sup> 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](https://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496&ref_=footer_privacy#GUID-8966E75F-9B92-4A2B-BFD5-967D57513A40__SECTION_FE2374D302994717AB1A8CE585E7E8BE).

<sup>23</sup> 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/>.

<sup>24</sup> 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).

<sup>25</sup> 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.<sup>26</sup>

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.

---

<sup>26</sup> *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](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.<sup>27</sup> 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.<sup>28</sup>

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.<sup>29</sup> And, the AG currently has the authority under the CCPA to issue rules with respect to financial incentives.<sup>30</sup> 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.<sup>31</sup> 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,<sup>32</sup> further highlighted by the creation of a Federal Trade Commission task force to monitor these trends.<sup>33</sup> The AG should exercise its authority to put reasonable limits on these programs in consolidated markets.

---

<sup>27</sup> 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](https://hoofnagle.berkeley.edu/wp-content/uploads/2018/12/hoofnagle_facebook_google_data_brokers.pdf).

<sup>28</sup> Cal. Civ. Code §§ 1798.125(a)(2) and .125(b).

<sup>29</sup> *Id.* at § 1798.125(b)(4).

<sup>30</sup> *Id.* at § 1798.185(a)(6).

<sup>31</sup> 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/>.

<sup>32</sup> *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>.

<sup>33</sup> *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.<sup>34</sup> 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.<sup>35</sup> 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 signal<sup>36</sup>—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

---

<sup>34</sup> § 999.315(c).

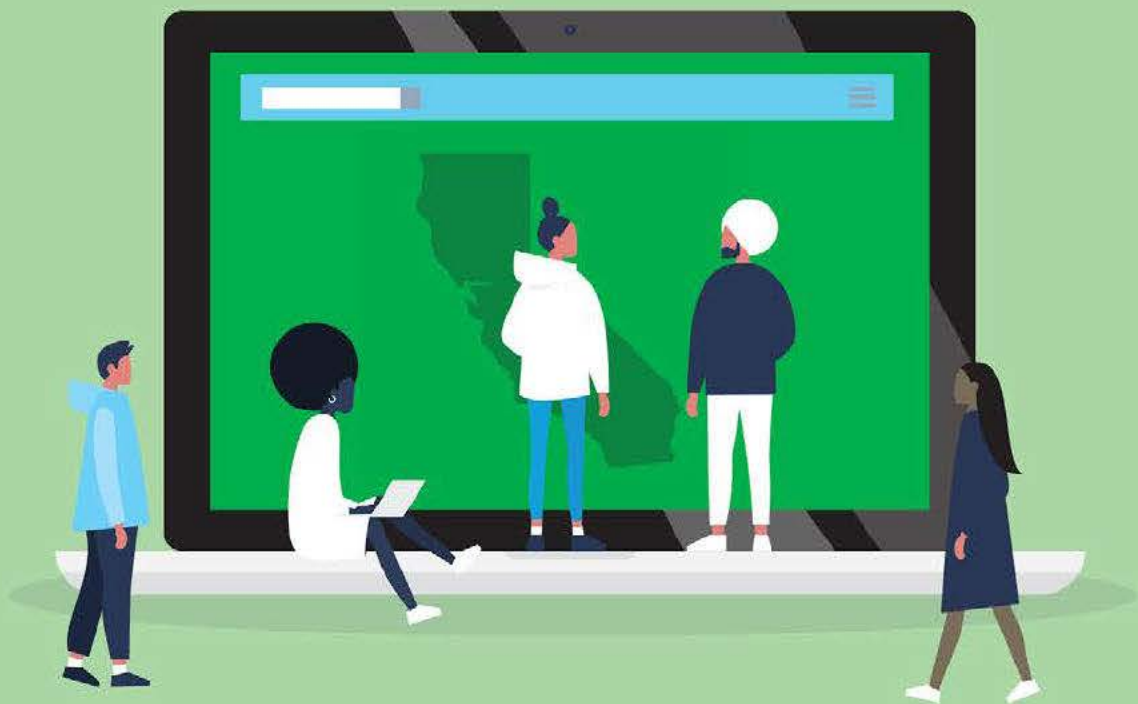
<sup>35</sup> Lara O'Reilly, *Apple's Latest iPhone Software Update Will Make It A Lot Harder for Advertisers to Track You*, BUS. INSIDER (Sept. 10, 2016), <http://www.businessinsider.com/apple-ios10-limit-ad-tracking-setting-2016-9>.

<sup>36</sup> 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



# California Consumer Privacy Act: Are Consumers' Digital Rights Protected?

MAUREEN MAHONEY

OCTOBER 1, 2020

## Table of Contents

Acknowledgments	3
Executive Summary	4
Introduction	6
Companies' Responsibilities Under the CCPA	8
Methodology	10
Findings	13
Policy Recommendations	44
Conclusion	48
Appendix	49

## Acknowledgments

This report is the result of a team effort. Thanks especially to Ben Moskowitz and Leah Fischman for shepherding us through this project, and to Justin Brookman, who provided invaluable assistance throughout. Devney Hamilton, Tom Smyth, and Jill Dimond at Sassafras Tech Collective deserve much of the credit for their work in devising the research study, building the testing tool, and analyzing the results. Kimberly Fountain, Alan Smith, and Daniela Nunez helped us recruit volunteers to participate in the study. Kaveh Waddell made countless contributions and Jennifer Bertsch offered crucial troubleshooting. Karen Jaffe, Camille Calman, Heath Grayson, David Friedman, and Cyrus Rassool improved the report through their review and support. Tim LaPalme and the creative team at Consumer Reports designed the report and helped us present the results more clearly. Finally, our deepest gratitude to the volunteer testers, without whom we would not have been able to conduct this study.

## Executive Summary

In May and June 2020, Consumer Reports' Digital Lab conducted a mixed methods study to examine whether the new California Consumer Privacy Act (CCPA) is working for consumers. This study focused on the Do-Not-Sell (DNS) provision in the CCPA, which gives consumers the right to opt out of the sale of their personal information to third parties through a "clear and conspicuous link" on the company's homepage.<sup>1</sup> As part of the study, 543 California residents made DNS requests to 214 data brokers listed in the California Attorney General's data broker registry. Participants reported their experiences via survey.

## Findings

- Consumers struggled to locate the required links to opt out of the sale of their information. 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.
  - 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 do 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. This also raises concerns about compliance, since companies are required to post the link in a "clear and conspicuous" manner.
- Many data brokers' opt-out processes are so onerous that they have substantially impaired consumers' ability to opt out, highlighting serious flaws in the CCPA's opt-out model.
  - Some DNS processes involved multiple, complicated steps to opt out, including downloading third-party software.
  - Some data brokers asked consumers to submit information or documents that they were reluctant to provide, such as a government ID number, a photo of their government ID, or a selfie.
  - Some data brokers confused consumers by requiring them to accept cookies just to access the site.

---

<sup>1</sup> Cal. Civ. Code § 1798.135(a)(1).

- Consumers were often forced to wade through confusing and intimidating disclosures to opt out.
  - Some consumers spent an hour or more on a request.
  - At least 14% of the time, burdensome or broken DNS processes prevented consumers from exercising their rights under the CCPA.
- At least one data broker used information provided for a DNS request to add the user to a marketing list, in violation of the CCPA.
- At least one data broker required the user to set up an account to opt out, in violation of the CCPA.
- Consumers often didn't know if their opt-out request was successful. Neither the CCPA nor the CCPA regulations require companies to notify consumers when their request has been honored. About 46% of the time, consumers were left waiting or unsure about the status of their DNS request.
- About 52% of the time, the tester was "somewhat dissatisfied" or "very dissatisfied" with the opt-out processes.
- On the other hand, some consumers reported that it was quick and easy to opt out, showing that companies can make it easier for consumers to exercise their rights under the CCPA. About 47% of the time, the tester was "somewhat satisfied" or "very satisfied" with the opt-out process.

## Policy recommendations

- The Attorney General should vigorously enforce the CCPA to address noncompliance.
- To make it easier to exercise privacy preferences, consumers should have access to browser privacy signals that allow them to opt out of all data sales in one step.
- The AG should more clearly prohibit dark patterns, which are user interfaces that subvert consumer intent, and design a uniform opt-out button. This will make it easier for consumers to locate the DNS link on individual sites.
- The AG should require companies to notify consumers when their opt-out requests have been completed, so that consumers can know that their information is no longer being sold.
- The legislature or AG should clarify the CCPA's definitions of "sale" and "service provider" to more clearly cover data broker information sharing.
- Privacy should be protected by default. Rather than place the burden on consumers to exercise privacy rights, the law should require reasonable data

minimization, which limits the collection, sharing, retention, and use to what is reasonably necessary to operate the service.

## Introduction

California consumers have new rights to access, delete, and stop the sale of their information under the landmark California Consumer Privacy Act, one of the first—and the most sweeping—online privacy laws in the country.<sup>2</sup> However, as the CCPA went into effect in January 2020, it was unclear whether the CCPA would be effective for consumers. Though the CCPA was signed into law in June 2018, many companies spent most of the 2019 legislative session working to weaken the CCPA.<sup>3</sup> Early surveys suggested that some companies were dragging their feet in getting ready for the CCPA.<sup>4</sup> And some companies, including some of the biggest such as Facebook and Google, declared that their data-sharing practices did not fall under the CCPA.<sup>5</sup> We suspected that this disregard among the biggest and most high-profile entities would filter down to many other participants in the online data markets, and decided to further explore companies' compliance with the CCPA.

The CCPA's opt-out model is inherently flawed; it places substantial responsibility on consumers to identify the companies that collect and sell their information, and to submit requests to access it, delete it, or stop its sale. Even when companies are making a good-faith effort to comply, the process can quickly become unmanageable for consumers who want to opt out of data sale by hundreds if not thousands of different companies. Given that relatively few consumers even know about the CCPA,<sup>6</sup>

---

<sup>2</sup> Cal. Civ. Code § 1798 et seq.; Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (Jun. 28, 2018), <https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html>.

<sup>3</sup> Press Release, Consumer Reports et al., Privacy Groups Praise CA Legislators for Upholding Privacy Law Against Industry Pressure (Sept. 13, 2019), [https://advocacy.consumerreports.org/press\\_release/joint-news-release-privacy-groups-praise-ca-legislators-for-upholding-privacy-law-against-industry-pressure/](https://advocacy.consumerreports.org/press_release/joint-news-release-privacy-groups-praise-ca-legislators-for-upholding-privacy-law-against-industry-pressure/).

<sup>4</sup> *Ready or Not, Here it Comes: How Prepared Are Organizations for the California Consumer Privacy Act?* IAPP AND ONETRUST at 4 (Apr. 30, 2019), [https://iapp.org/media/pdf/resource\\_center/IAPPOneTrustSurvey\\_How\\_prepared\\_for\\_CCPA.pdf](https://iapp.org/media/pdf/resource_center/IAPPOneTrustSurvey_How_prepared_for_CCPA.pdf) (showing that “[M]ost organizations are more unprepared than ready to implement what has been heralded as the most comprehensive privacy law in the U.S. ever.”)

<sup>5</sup> Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously—The Attorney General Needs to Act*, MEDIUM (Jan. 9, 2020), <https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb>

<sup>6</sup> *Report: Nearly Half of U.S.-Based Employees Unfamiliar with California Consumer Privacy Act (CCPA)*, MEDIAPRO (Apr. 30, 2019), <https://www.mediapro.com/blog/2019-eye-on-privacy-report-mediapro/>.



participation is likely fairly low. Anecdotally, those that are aware of the CCPA and have tried to exercise their new privacy rights have struggled to do so.<sup>7</sup> Through this study we sought to get better insight into the challenges faced by consumers trying to exercise their rights under the CCPA's opt-out model.

This study also seeks to influence the regulations implementing the CCPA, to help ensure that they are working for consumers. The CCPA tasks the California Attorney General's office with developing these regulations, which help flesh out some of the responsibilities of companies in responding to consumer requests.<sup>8</sup> For example, with respect to opt outs, the regulations clarify how long the companies have to respond to opt-out requests<sup>9</sup> and outline the notices that need to be provided to consumers.<sup>10</sup> On August 14, 2020, the AG regulations went into effect.<sup>11</sup> The CCPA directs the AG to develop regulations as needed to implement the CCPA, consistent with its privacy intent,<sup>12</sup> and the AG has signaled that they plan to continue to consider a number of issues with respect to opt outs.<sup>13</sup>

The AG is also tasked with enforcing the CCPA, and this study is also intended to help point out instances of potential noncompliance. Despite efforts of industry to push back the date of enforcement,<sup>14</sup> the AG has had the authority to begin enforcement since July 1, 2020.<sup>15</sup> Already, the AG's staff has notified companies of potential violations of the CCPA.<sup>16</sup>

---

<sup>7</sup> Geoffrey Fowler, *Don't Sell My Data! We Finally Have a Law for That*, WASH. POST (Feb. 19, 2020), <https://www.washingtonpost.com/technology/2020/02/06/ccpa-faq/>.

<sup>8</sup> Cal. Civ. Code § 1798.185(a).

<sup>9</sup> Cal. Code Regs. tit. 11 § 999.315(e) (2020).

<sup>10</sup> *Id.* at § 999.304-308.

<sup>11</sup> State of California Department of Justice, CCPA Regulations (last visited Aug. 15, 2020), <https://www.oag.ca.gov/privacy/ccpa/regs>.

<sup>12</sup> Cal. Civ. Code § 1798.185(b)(2).

<sup>13</sup> Cathy Cosgrove, *Important Commentary from Calif. OAG in Proposed CCPA Regulations Package*, IAPP (Jul. 27, 2020), <https://iapp.org/news/a/important-commentary-from-calif-oag-in-proposed-ccpa-regulations-package/>.

<sup>14</sup> See, e.g. Andrew Blustein, *Ad Industry Calls for Delayed Enforcement of CCPA*, THE DRUM (Jan. 29, 2020), <https://www.thedrum.com/news/2020/01/29/ad-industry-calls-delayed-enforcement-ccpa>; Association of National Advertisers, *ANA and Others Ask for CCPA Enforcement Extension* (Mar. 18, 2020), <https://www.ana.net/blogs/show/id/rr-blog-2020-03-ANA-and-Others-Asks-for-CCPA-Enforcement-Extension>.

<sup>15</sup> Cal. Civ. Code § 1798.185(c).

<sup>16</sup> Cosgrove, *Important Commentary*, *supra* note 13; Malia Rogers, David Stauss, *CCPA Update: AG's Office Confirms CCPA Enforcement Has Begun*, JD SUPRA (Jul. 14, 2020), <https://www.jdsupra.com/legalnews/ccpa-update-ag-s-office-confirms-ccpa-55113/>.

Our study revealed flaws in how companies are complying with CCPA and with the CCPA itself. Many companies are engaging in behavior that almost certainly violates the CCPA. But even if companies were complying completely in good faith, the CCPA makes it incredibly difficult for individuals to meaningfully exercise control over the sale of their personal information. Indeed, the conceit that consumers should have to individually opt out of data sale from each of the hundreds of companies listed on the California data broker registry—let alone the hundreds or thousands of other companies that may sell consumers' personal information—in order to protect their privacy is absurd. Over half of the survey participants expressed frustration with the opt-out process, and nearly half were not even aware if their requests were honored by the recipient. The Attorney General should aggressively enforce the current law to remediate widespread noncompliant behavior, but it is incumbent upon the legislature to upgrade the CCPA framework to protect privacy by default without relying upon overburdened consumers to understand complex data flows and navigate heterogeneous privacy controls.

## **Companies' responsibilities under the CCPA**

Under the CCPA, companies that sell personal information (PI) to third parties must honor consumers' requests to opt out of the sale of their PI.<sup>17</sup> The CCPA has a broad definition of personal information, which includes any data that is reasonably capable of being associated with an individual or household—everything from Social Security numbers, to biometric information, or even browsing history. This also covers browsing history or data on a shared computer (in other words, not data that can be exclusively tied to a single individual)<sup>18</sup>—further highlighting that opt outs need not be verified to a particular individual. The CCPA's definition of sale covers any transfer of data for valuable consideration,<sup>19</sup> intended to capture data that is shared with third parties for behavioral advertising purposes.<sup>20</sup>

---

<sup>17</sup> Cal. Civ. Code § 1798.120(a).

<sup>18</sup> *Id.* at § 1798.140(o)(1).

<sup>19</sup> *Id.* at § 1798.140(t)(1).

<sup>20</sup> California Senate Judiciary Committee, SB 753 Bill Analysis at 10 (Apr. 22, 2019), [https://leginfo.ca.gov/faces/billAnalysisClient.xhtml?bill\\_id=201920200SB753](https://leginfo.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201920200SB753). The analysis excerpts a letter from the sponsors of AB 375, Californians for Consumer Privacy, opposing SB 753, legislation proposed in 2019 that would explicitly exempt cross-context targeted advertising from the CCPA: "SB 753 proposes to amend the definition of 'sell' in Civil Code Section 1798.140 in a manner that will break down th[is] silo effect . . . . As a result, even if a consumer opts-out of the sale of their data, this proposal would allow an advertiser to combine, share and proliferate data throughout the advertising

The CCPA places certain responsibilities on these companies to facilitate the opt outs. They are required to provide a “clear and conspicuous link” on their homepage so that consumers can exercise their opt-out rights.<sup>21</sup> The CCPA pointedly creates a separate process for exercising opt-out rights than it does for submitting access and deletion requests—the latter requires verification to ensure that the data that is being accessed or deleted belongs to the correct person.<sup>22</sup> In contrast, for opt outs, verification is not required.<sup>23</sup> Importantly, companies may not use the information provided by the opting out consumer for any other purpose.<sup>24</sup> The CCPA also directs the AG to design and implement a “Do Not Sell” button to make it easier for consumers to opt out.<sup>25</sup>

The AG's regulations outline additional requirements. Companies must post a prominent link labeled “Do Not Sell My Personal Information,” which must lead the consumer to the required interactive form to opt out.<sup>26</sup> (The AG declined to finalize a design to serve as an opt-out button.)<sup>27</sup> CCPA regulations clarify that “A request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request[,]” and the company, if it declines a request for that reason, is required to notify the consumer and provide an explanation.<sup>28</sup> Companies must honor consumers' requests to opt out within 15 business days<sup>29</sup> (in contrast to 45 days for deletion and access requests).<sup>30</sup>

---

economy. The proposed language will essentially eliminate the silo effect that would occur pursuant to the CCPA, which allows for targeted advertising but prevents the proliferation of a consumer's data throughout the economy.”

<sup>21</sup> Cal. Civ. Code § 1798.135(a)(1).

<sup>22</sup> *Id.* at § 1798.140(y).

<sup>23</sup> *Id.* at § 1798.135.

<sup>24</sup> *Id.* at § 1798.135(a)(6).

<sup>25</sup> *Id.* at § 1798.185(a)(4)(C).

<sup>26</sup> Cal. Code Regs. tit. 11 § 999.315(a) (2020).

<sup>27</sup> State of California Department of Justice, Final Statement of Reasons at 15 (June 1, 2020), <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor.pdf> [hereinafter FSOR].

<sup>28</sup> *Id.* at § 999.315(g).

<sup>29</sup> *Id.* at § 999.315(e).

<sup>30</sup> Cal. Civ. Code § 1798.130(a)(2).

## Methodology

In this section, we describe our sample, the research exercise, survey, and method of analysis.

### Selecting Companies to Study

To select the companies to study, we used the new California data broker registry,<sup>31</sup> which lists companies that sell California consumers' personal information to third parties, but do not have a direct relationship with the consumer.<sup>32</sup> Reining in data brokers—which profit from consumers' information but typically do not have a direct relationship with them—was a primary purpose of the CCPA. Through the opt out of sale, the authors of the CCPA sought to dry up the pool of customer information available on the open market, disincentivize data purchases, and make data brokering a less attractive business model.<sup>33</sup>

The data broker registry was created in order to help consumers exercise their rights under the CCPA with respect to these companies. Companies that sell the personal information of California consumers but don't have a relationship with the consumer are required to register with the California Attorney General each year.<sup>34</sup> The AG maintains the site, which includes the name of the company, a description, and a link to the company's website, where the consumer can exercise their CCPA rights.<sup>35</sup> The data broker registry is particularly important because many consumers do not even know which data brokers are collecting their data, or how to contact them. Without the data broker registry, exercising CCPA rights with respect to these companies would be near impossible.

For many consumers, data brokers exemplify some of the worst aspects of the ad-supported internet model, giving participants in the study a strong incentive to opt out of the sale of their information. Nearly everything a consumer does in the online or even physical world can be collected, processed, and sold by data brokers. This could

---

<sup>31</sup> State of California Department of Justice, Data Broker Registry (last visited August 10, 2020), <https://oag.ca.gov/data-brokers> [hereinafter DATA BROKER REGISTRY].

<sup>32</sup> Cal. Civ. Code § 1798.99.80(d).

<sup>33</sup> 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>.

<sup>34</sup> DATA BROKER REGISTRY, *supra* note 31.

<sup>35</sup> *Id.*

include location data picked up from apps, purchase history, browsing history—all combined to better understand and predict consumer behavior, and to guide future purchases. Data brokers can purchase information from a variety of sources, both online and offline, including court records and other public documents. The inferences drawn can be startlingly detailed and reveal more about a consumer than they might realize. Consumers can be segmented by race, income, age, or other factors.<sup>36</sup> The information collected can even provide insight whether a consumer is subject to certain diseases, such as diabetes, or other insights into health status.<sup>37</sup> All of this data might be used for marketing, or it could be used to assess consumers' eligibility for certain opportunities, either due to loopholes in consumer protection statutes such as the Fair Credit Reporting Act, or because of a lack of transparency and enforcement.<sup>38</sup>

## Sampling

We randomly sampled from all of the 234 brokers in California's data broker registry as of April 2020. In the final analysis, we included three sample requests for each of 214 brokers, totaling 642 DNS requests made by 403 different participants. Though we did not have enough testers to ensure that every company on the data broker registry received three tests, a sample of 214 of 234 companies in the database is more than sufficient to represent the different types of processes for all companies. In our initial investigation into DNS requests, in which we submitted our own opt-out requests, we found that three requests were generally enough to uncover the different processes and pitfalls for each company. However, in order to analyze and generalize success rates of DNS requests depending on different processes, a follow-up study should be conducted toward this end. In cases in which testers submitted more than three sample requests for a company, we randomly selected three to analyze.

Participants were not representative of the general population of California. As this initial study was designed to understand the landscape of different data brokers and their DNS request processes, we decided to use a convenience sample. Participants were

---

<sup>36</sup> *Data Brokers: A Call for Transparency and Accountability*, FED. TRADE COMM'N at 24 (May 2014), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

<sup>37</sup> *Id.* at 25.

<sup>38</sup> *Big Data, A Big Disappointment for Scoring Consumer Credit Risk*, NAT'L CONSUMER LAW CTR. at 26 (Mar. 2014), <https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf>; *Spokeo to Pay \$800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA*, FED. TRADE COMM'N (June 12, 2012), <https://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed>.

recruited through CR's existing membership base, promotion by partner organizations, and through social media outreach. Participation was limited to California residents. Therefore, participants were likely better informed about the CCPA and digital privacy rights than the general population. The study was conducted in English, excluding those not fluent in English. Participation in the study was not compensated.

## **Research Exercise**

In the study exercise, participants were randomly assigned a data broker from the registry using custom software, and were emailed with instructions to attempt making a DNS request to that data broker. Participants could, and many did, test more than one data broker. On average, participants performed 1.8 test requests. For each request, the participant was given a link to the data broker's website and its email address. They were instructed to look for a "Do Not Sell My Personal Info" (or similar) link on the broker's site and to follow the instructions they found there, or to send an email to the email address listed in the data broker registration if they did not find the link. Participants then reported their experience with the DNS process via survey immediately after their first session working on the request. Participants were prompted by email to fill out follow-up surveys at one week and 21 days (approximately 15 business days) to report on any subsequent steps they had taken or any updates on the status of their request they had received from the data broker. (See Appendix, Section A for a diagram of the participant experience of the exercise).

## **Survey Design**

The survey aimed to capture a description of a participant's experience in making a DNS request. We approached the design of this study as exploratory to understand the DNS process and as a result, asked mixed qualitative and quantitative questions. The survey branched to ask relevant questions based on what the participant had reported thus far. These questions involved mostly optional multi-select questions, with some open-ended questions. Because the survey included optional questions, not all samples have answers to every question. We omitted from the analysis samples in which there was not enough applicable information for the analysis question. Participants were encouraged to use optional "other" choices with open-ended text. We also offered participants the ability to send in explanatory screenshots. Where participants flagged particularly egregious behaviors, we followed up by having a contractor collect screenshots, or we followed up ourselves to collect screenshots.



## Data Analysis

We used both quantitative and qualitative methods for analysis. To answer the questions of time spent and ability to find the DNS request link, we aggregated the responses. To understand the result of request processes, we relied on answers to both open-ended text questions and multi-select questions related to status in order to code and tally the results.

For open response text, we used a qualitative thematic analysis approach where we read the text and coded inductively for themes.

## Limitations

This was an exploratory study designed to uncover different DNS processes. As such, our results are not experimental and cannot conclusively establish the efficacy of these DNS processes. Some questions in the survey were meant to capture the participants' experiences, such as "Did the [broker] confirm that they are not selling your data?" For example, a confirmation email could have been sent to the consumer's junk mail folder—so the consumer may not have been aware of the confirmation, even if the company had sent one. Also, consumers may not have understood brokers' privacy interfaces, and conflated DNS requests with other rights; for example, some consumers may have submitted access or deletion requests when they meant to submit opt-out requests. That said, given that the CCPA is designed to protect consumers, consumers' experiences have value in evaluating the CCPA. In addition, because of our convenience sample, it is likely that the broader population may generally drop off from these processes earlier (or not engage at all) due to constraints such as time or lack of technology skill.

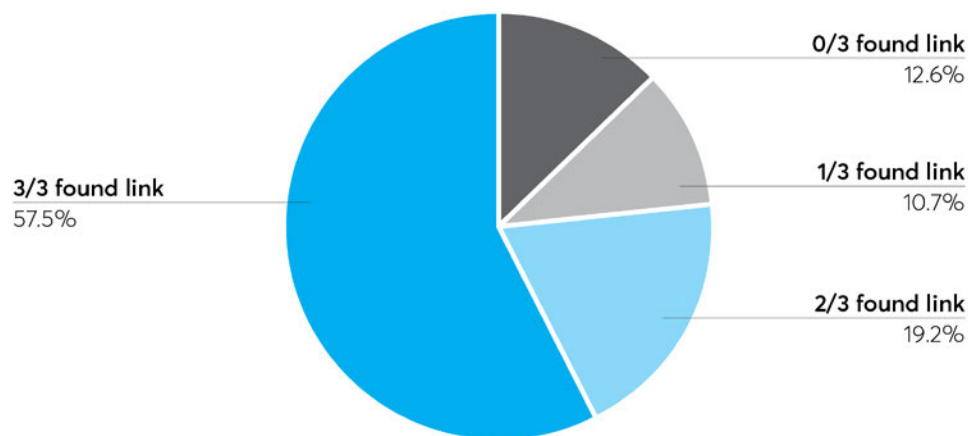
## Findings

CCPA opt outs should be simple, quick, and easy. However, we found that many companies failed to meet straightforward guidelines—posing significant challenges to consumers seeking to opt out of the sale of their information. Below, we explore the challenges consumers faced in opting out of the sale of their information from data brokers.

**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.**

Consumers often found it difficult to opt out of the sale of their information, in large part because opt-out links either weren't visible on the homepage or weren't there at all. Nearly half the time, at least one of three of our testers failed to find the link, even though they were expressly directed to look for it. This suggests that either the link wasn't included on the homepage, or that it was not listed in a “clear and conspicuous” manner, both of which are CCPA requirements.

### Brokers by number of testers who found DNS link



Companies on the California data broker registry by definition sell customer PI to third parties and should have a Do Not Sell link on their homepage in order to comply with the CCPA. Under California law, every data broker is required to register with the California Attorney General so that their contact information can be placed on the registry.<sup>39</sup> A data broker is defined as a “business that knowingly collects *and sells* to third parties the personal information of a consumer with whom the business does not have a direct relationship.”<sup>40</sup> [emphasis added] The definitions of “sell,” “third parties,”

---

<sup>39</sup> Cal. Civ. Code §1798.99.82.

<sup>40</sup> *Id.* at § 1798.99.80(d).



and “personal information” all mirror those of the CCPA, which helps to ensure that the registry effectively aids consumers in exercising their CCPA rights with respect to these entities.<sup>41</sup>

While it is true that some data brokers may enjoy certain exemptions from AB 1202, companies selling customer information still are obligated to put up Do Not Sell links. In response to requests to the AG during the rulemaking process to “Amend [the CCPA rules] to explain that businesses must provide notice of consumer rights under the CCPA only where such consumer rights may be exercised with respect to personal information held by such business. Consumer confusion could result from explanation of a certain right under the CCPA when the business is not required to honor that right because of one or more exemptions[,]” the AG responded that “CCPA-mandated disclosures are required even if the business is not required to comply with the consumers’ exercise of their rights.”<sup>42</sup>

The homepage means the first, or landing, page of a website. It is not sufficient to place a link to a privacy policy on the first page, that leads to the DNS link—the link on the homepage must be labeled “Do Not Sell My Personal Information.”<sup>43</sup> The CCPA clarifies that “homepage” indeed means “the introductory page of an internet website and any internet web page where personal information is collected.”<sup>44</sup> The AG further explains that a link to a privacy policy is not sufficient to constitute a Do Not Sell link: “The CCPA requires that consumers be given a notice at collection, notice of right to opt out, and notice of financial incentive. These requirements are separate and apart from the CCPA’s requirements for the disclosures in a privacy policy.”<sup>45</sup>

The CCPA does note that a company need not include “the required links and text on the homepage that the business makes available to the public generally[,]” if it establishes “a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for

---

<sup>41</sup> *Id.* at § 1798.99.80(e)-(g).

<sup>42</sup> State of California Department of Justice, Final Statement of Reasons, Appendix A, Response #264 (June 1, 2020), <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf> [hereinafter “FSOR Appendix”].

<sup>43</sup> Cal. Civ. Code § 1798.135(a)(1).

<sup>44</sup> *Id.* at § 1798.140(l).

<sup>45</sup> FSOR Appendix, *supra* note 42, Response #105.

California consumers and not the homepage made available to the public generally.”<sup>46</sup> We limited our outreach to participants who had previously told us they were California residents, though we cannot say for sure that they were in California at the time they completed our survey. Occasionally California employees supplemented survey responses by capturing additional screenshots, sometimes from within California, sometimes without. Technically, the CCPA gives rights to Californians even when they are not physically present within the state, though it is possible that data brokers treat users differently based on approximate geolocation derived from their IP address.<sup>47</sup>

If testers are unable to find a DNS link on the homepage even if it is there, that suggests that it may not be placed in a “clear and conspicuous” manner, as required by the CCPA. If testers that have been provided instructions and are looking for an opt-out link in order to complete a survey are unable to find a link, it is less likely that the average consumer, who may not even know about the CCPA, would find it.

Testers that did not find an opt-out link but continued with the opt-out process anyway often faced serious challenges in exercising their opt-out rights. We instructed these testers to email the data broker to proceed with the opt-out request. This considerably slowed down the opt-out process, as a consumer had to wait for a representative to respond in order to proceed. And often, the agent provided confusing instructions or was otherwise unable to help the consumer with the opt-out request. For example, we received multiple complaints about Infinite Media. Infinite Media did not have a “Do Not Sell” link on its homepage (see Appendix, Section B for a screenshot). Further, its representative puzzled testers by responding to their opt-out emails with confusing questions—such as whether they had received any marketing communications from the company—in order to proceed with the opt out.

I am with Infinite Media/ Mailinglists.com and have been forwarded your request below. We are a list brokerage company and do not compile any data. We do purchase consumer data on behalf of some of our clients and we do work with a large business compiler and purchase data from them as well. Can you tell me if you received something to your home or business address? If home address I will need your full address info. If business, then please send your company name and address. Also do you work from home? Lastly who was it that you received the mail piece, telemarketing call or email from? I need to know the

---

<sup>46</sup> Cal. Civ. Code § 1798.135(b).

<sup>47</sup> Cal. Civ. Code § 1798.140(g).

name of the company that contacted you so I can track back where the data came from and contact the appropriate list company and have you removed from their data file so they don't resell your name any longer.

Given the number of unsolicited communications that consumers receive, it was difficult for the testers to answer and frustrated their efforts to opt out. One consumer reached out to us after receiving the message: "I don't know how to reply - since I have not received any marketing item from them, ca[n]'t give them the name of outfit/person they're asking about. Our landline does get an annoying amount of robocalls and telemarketing calls but I can't tell who/what they're from...."

The agent's confusing response itself is a potential CCPA violation, as the CCPA requires companies to "[e]nsure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Section 1798.120 [regarding the right to opt out] and this section and how to direct consumers to exercise their rights under those sections."<sup>48</sup> Instead of directing consumers to the interactive form to opt out, the agent confused and frustrated consumers seeking to exercise their CCPA opt-out rights by asking them questions that they could not answer.

**At least 24 companies on the data broker registry do not have a DNS link anywhere on their homepages.**

Follow-up research on the sites in which all three testers did not find the link revealed that at least 24 companies do not have the required DNS link on their homepage (see Appendix, Section B for screenshots).<sup>49</sup> For example, some companies provide information about CCPA opt-out rights within its privacy policy or other document, but offer no indication of those rights on the homepage. Since consumers typically don't read privacy policies,<sup>50</sup> this means that unless a consumer is familiar with the CCPA or

---

<sup>48</sup> Cal. Civ. Code § 1798.135(a)(3).

<sup>49</sup> These companies are: Admarketplace.com, Big Brook Media, Inc., Blue Hill Marketing Solutions, Comscore, Inc., Electronic Voice Services, Inc., Enformion, Exponential Interactive, Gale, GrayHair Software, LLC, Infinite Media Concepts Inc, JZ Marketing, Inc., LeadsMarket.com LLC, Lender Feed LC, On Hold-America, Inc. DBA KYC Data, Outbrain, PacificEast Research Inc., Paynet, Inc., PossibleNow Data Services, Inc, RealSource Inc., Social Catfish, Spectrum Mailing Lists, SRAX, Inc., USADATA, Inc., and zeotap GmbH.

<sup>50</sup> Brooke Axier et al., *Americans' Attitudes and Experiences with Privacy Policies and Laws*, PEW RESEARCH CTR. (Nov. 15, 2019),

is specifically looking for a way to opt out, they likely won't be able to take advantage of the DNS right.

For example, the data broker Outbrain doesn't have a "Do Not Sell My Personal Information" link on its homepage. The 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.'" Below, we show the opt-out process through screenshots (See pages 20-21):

**STEP 1** The "Privacy Policy" link takes the consumer to the "Privacy Center." Consumers can click on panel 6, "California Privacy Rights," **STEP 2.**

Clicking on "California Privacy Rights" opens up a text box **STEP 3**, that includes a bullet on the "Right to opt-out of the 'sale' of your Personal Information." That section includes a very small hyperlink to "opt out of personalised recommendations."

Clicking on that link takes the consumer to another to a page titled "Your Outbrain Interest Profile," **STEP 4.** (The consumer can also reach this page by clicking on "Interest-Based Ads" on the homepage.)

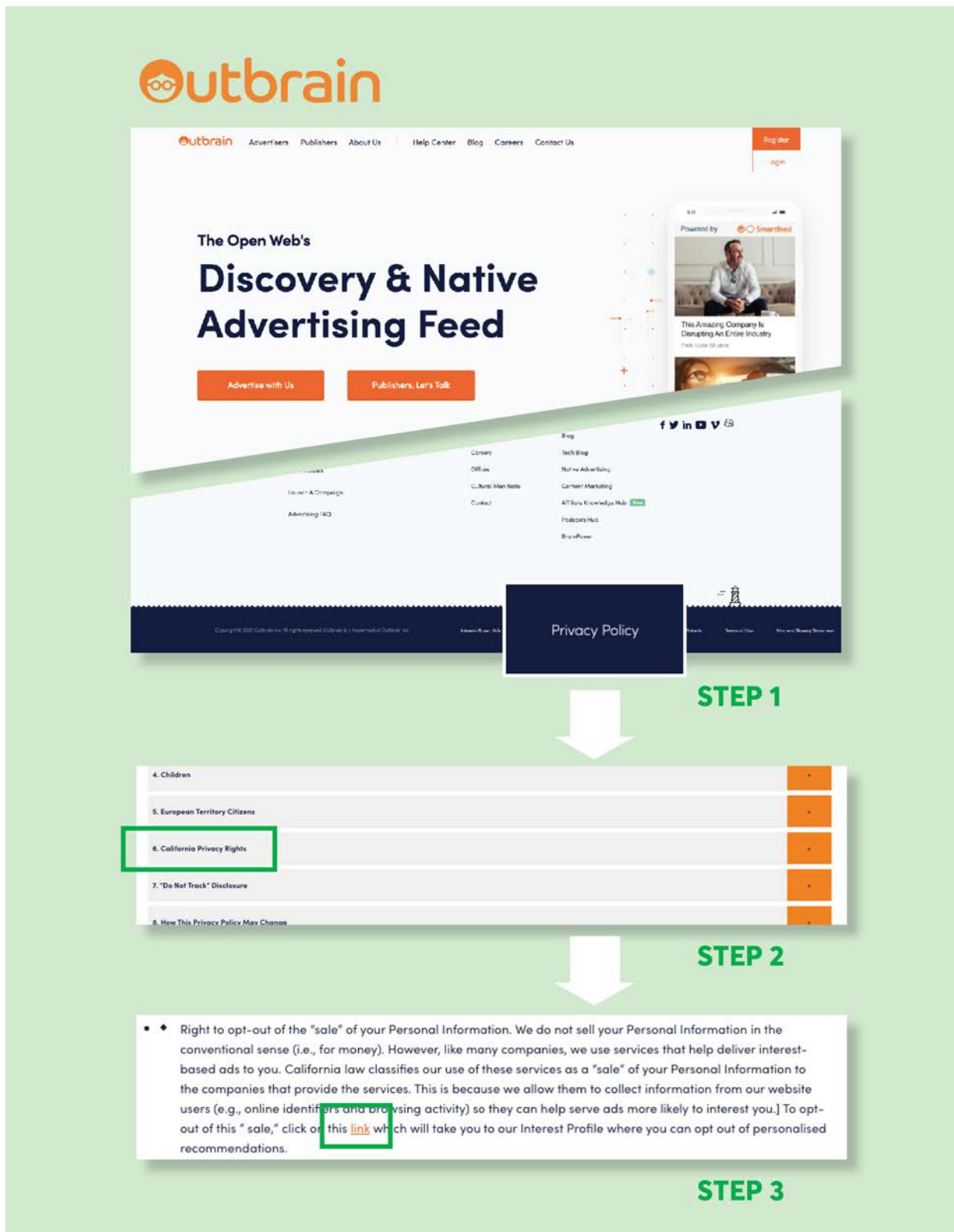
The consumer can then click on "View My Profile," which takes them to a new page that provides a breakdown of interest categories. In the upper right-hand corner, there is a small, gray-on-black link to "Opt Out," **STEP 5.**

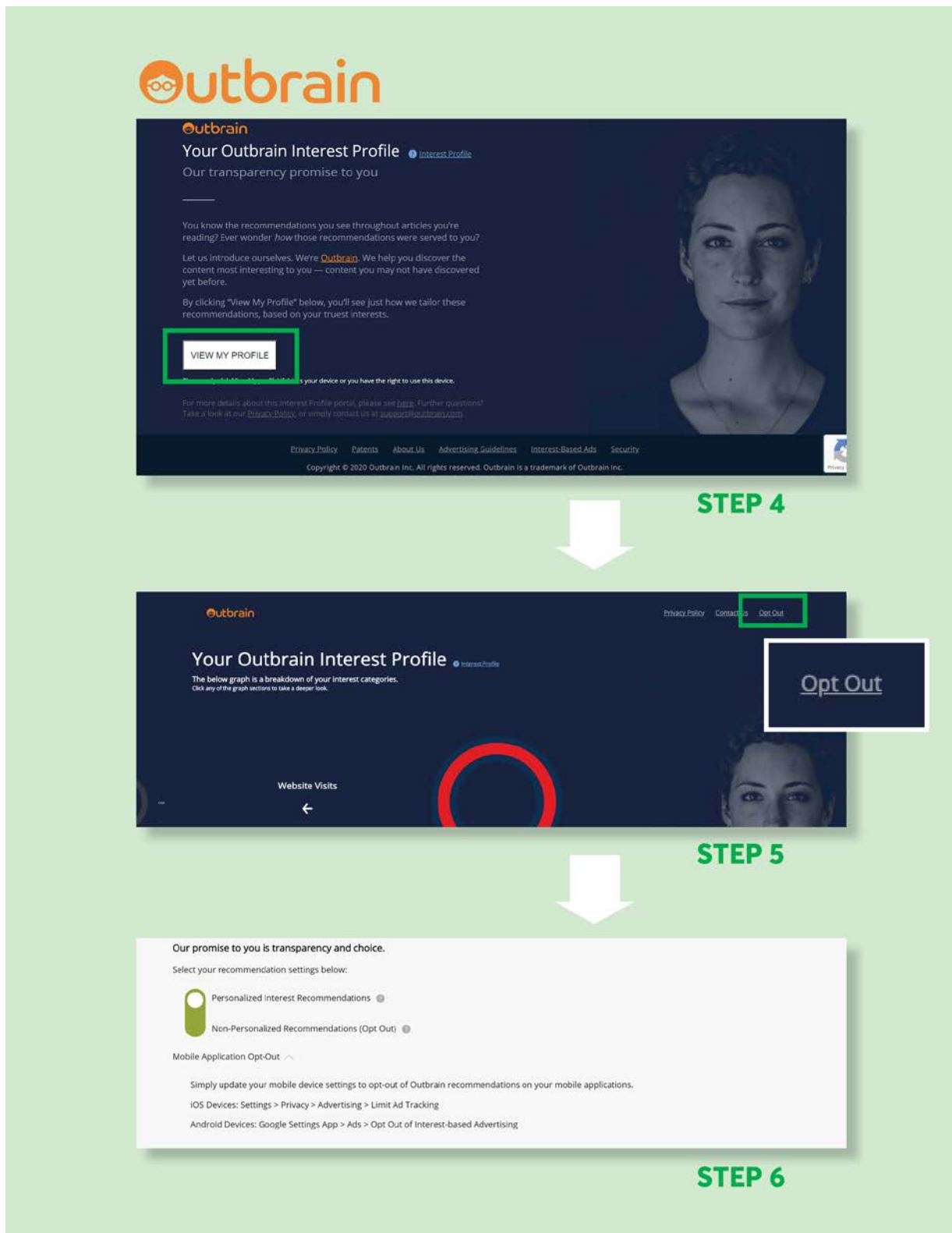
This finally takes the consumer to a page where they can move a toggle to "opt out" of interest-based advertising, **STEP 6**, though it is unclear whether turning off personalized recommendations is the same as opting out of the sale of your data under the CCPA. One tester remarked on the confusion, "There were many links embedded in the Outbrain Privacy Center page. I had to expand each section and read the text and review the links to determine if they were the one I wanted. I am not sure I selected "DO not Sell" but I did opt out of personalized advertising."

---

<https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/> (Showing that only 9% of adults read the privacy policy before accepting the terms and conditions, and 36% never do.).

---







Even those steps don't opt consumers out for all devices. There are separate instructions for opting out on a mobile device, and for bulk opting out of ad targeting through a voluntary industry rubric (though again, it isn't clear if this is the same as stopping sale under the CCPA).

Instead of leaving consumers to navigate through multiple steps to opt out, Outbrain should have included a link that says "Do Not Sell My Personal Information" on the homepage, and then immediately taken the consumer to a page with the toggle to opt out. The AG's regulations require companies to provide "two or more designated methods for submitting requests to opt out, including an *interactive form* accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information," on the business's website or mobile application."<sup>51</sup> (emphasis added). This suggests that the opt out is intended to involve nothing more than filling out a short form, one that is quickly and easily accessed from the homepage.

**For an additional five companies, all three testers were unable to find the DNS link, suggesting that they may not be listed in a "clear and conspicuous" manner as required by the CCPA.**

All three testers were unable to find the DNS link for an additional five companies (see Appendix, Section C for screenshots).<sup>52</sup> For example, all three testers failed to find the Do Not Sell link for the data broker Freckle I.O.T. Ltd./PlacelQ. First, the website <https://freckleiot.com/>, which is listed on the data broker registry, automatically redirects to <https://www.placeiq.com/>, where consumers are confronted with a dark pattern banner at the bottom of the screen that only offers the option to "Allow Cookies" (the banner also states that "scrolling the page" or "continuing to browse otherwise" constitutes consent to place cookies on the user's device.) If the user does not click "Allow," the banner stays up, and it obscures the "CCPA & Do Not Sell" link (for more on mandating cookie acceptance as a condition of opting out, see *infra*, p. 30).

---

<sup>51</sup> Cal. Code Regs. tit. 11 § 999.315(a) (2020).

<sup>52</sup> These companies are: AcademixDirect, Inc., Fifty Technology Ltd, Freckle I.O.T. Ltd./PlacelQ, Marketing Information Specialists, Inc., and Media Source Solutions. Two of the companies in which all three testers could not find the DNS link did not appear to have a functioning website at all: Elmira Industries, Inc. and Email Marketing Services, Inc.

## California Consumer Privacy Act: Are Consumers' Digital Rights Protected?

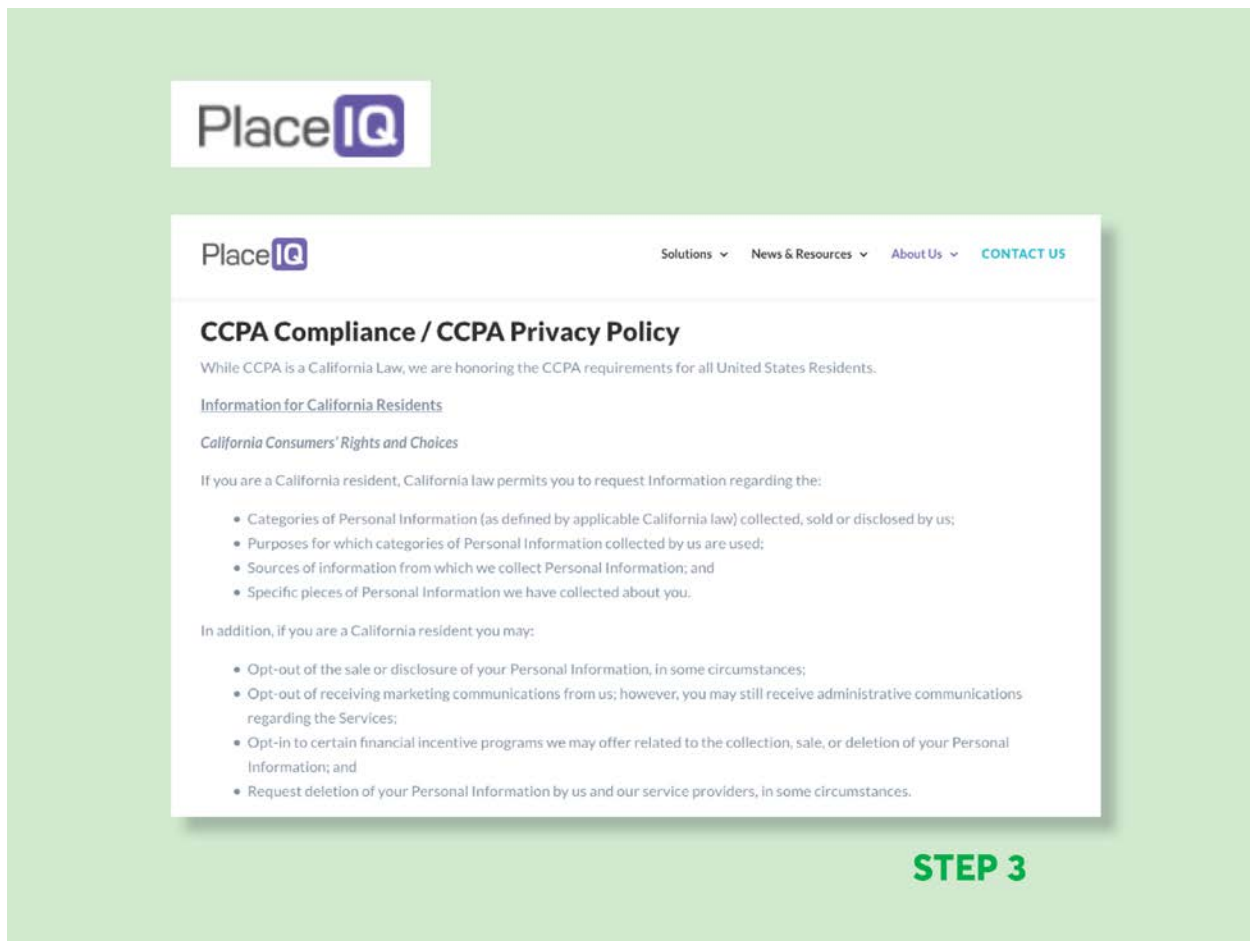
The diagram illustrates the process of finding the CCPA & Do Not Sell link on the PlaceIQ website. It is divided into two main steps:

**STEP 1:** A screenshot of the PlaceIQ website's top navigation bar. The navigation bar includes links for Solutions, News & Resources, About Us, and CONTACT US. Below the navigation bar, there is a green banner with the text: "Check out PlaceIQ's latest COVID-19 research and analysis, and sign up for our weekly newsletter!" and a "LEARN MORE" button. Below the banner, there is a blue banner with the text: "Ten years ago, PlaceIQ invented location intelligence for the marketing and media space. Today, we are the leading data and technology company that helps businesses... insights to connect with...". Below the blue banner, there is a dark blue banner with the text: "We use cookies to ensure that we give you the best experience on our website. If you want to know more or withdraw your consent to all or some of the cookies, please refer to the [cookie policy](#). By closing this banner, scrolling this page, clicking a link or continuing to browse otherwise, you agree to the use of cookies." and a "Allow cookies" button. A white arrow points from the "Allow cookies" button to the next step.

**STEP 2:** A screenshot of the PlaceIQ website's footer. The footer is divided into several sections: PlaceIQ (with address: 5 Bryant Park, 18th Floor, New York, NY 10018, sales@placeiq.com), PRIVACY PARTNERS (with logos for NAES, MMA, IAB, DPAA, and others), NEWS & INSIGHTS (with links for Blog, News & Events, Case Studies, Resource Library), SOLUTIONS (with links for Audiences, Measurement, Dashboards, Data Licensing), and COMPANY (with links for Who We Are, Careers, Contact Us). Below the COMPANY section, there is a "Consumer Options:" link, which is highlighted with a green box. A white arrow points from the "Consumer Options:" link to the next step.

**STEP 3:** A screenshot of the "Consumer Options:" page. The page lists "Privacy Policy" and "CCPA & Do Not Sell" as options. The "CCPA & Do Not Sell" link is highlighted with a green box.





After clicking “Allow Cookies,” revealing the full homepage, then, the user must scroll all the way down to the bottom of the homepage to get to the CCPA & Do Not Sell link (also note that the link is not labeled “Do Not Sell My Personal Information” as required by the CCPA).

Since users must accept cookies to remove the pop up and reveal the link, and the link was buried at the very bottom of the page, it is not surprising that none of the consumers testing the site were able to find the opt-out link, even though they were looking for it. This shows how confusing user interfaces can interfere with consumers' efforts to exercise their privacy preferences, and how important it is for companies to follow CCPA guidance with respect to “clear and conspicuous” links. Without an effective mechanism to opt out, consumers are unable to take advantage of their rights under the law.

**Some DNS processes involved multiple, complicated steps to opt out, including downloading third-party software, raising serious questions about the workability of the CCPA for consumers.**

While companies might need to collect some information from consumers in order to identify consumer records—for example, data brokers typically sell records by email<sup>53</sup>—some companies asked for information that was difficult to obtain, or required consumers to undergo onerous processes in order to opt out. There were a variety of formats for making DNS requests such as instructions to download a third-party app, instructions to send an email, or no instruction or clearly visible opt-out link at all (we instructed our participants to send an email to the email address in the registry if they could not find the opt-out link).

The most common type of DNS process involved filling out a form with basic contact information such as name, email, address, and phone number. However, several companies, such as those tracking location data, asked consumers to provide an advertising ID and download a third-party app to obtain it. This was confusing and labor intensive for many testers.

Companies that defaulted to pushing consumers to install an app to obtain the ID discouraged some consumers from opting out—downloading a separate app to their phone was a step too far. One tester of data broker Freckle I.O.T./PlacelQ reported, “Too technically challenging and installing an app on your phone shouldn't be required.” The consumer further notes that the Freckle I.O.T./PlacelQ opt-out process would be impossible for consumers without a mobile phone. “The process also could not be completed on a computer, so anyone without a smartphone would not be able to complete the request this way.” In nearly half (8 out of 20) of cases, consumers declined to provide an advertising or customer ID.

Other consumers found themselves unable to submit opt-out requests because the company required an IP address. For example, four testers reported that they could not complete their request to Megaphone LLC because they were asked to provide their IP address. In this case, it was likely that testers declined to proceed further because they could not figure out how to obtain their IP address. The screenshot on page 25 shows that Megaphone’s opt-out form includes a required question, “What is your IP address?”

---

<sup>53</sup> For example, TowerData claims that clients can obtain “data on 80% of U.S. email addresses.” TowerData (last visited Sept. 13, 2020), <http://intelligence.towerdata.com/>.

**Megaphone**

Modern podcast technology for publishers and advertisers.

**Do not sell my personal information**

**STEP 1**

**CCPA Request**

California residents may use this form to submit a request to opt out of the "sale" of their personal information to third parties.

The only personal information that Megaphone collects is a user's IP address and user agent, which is information about the user's device, browser, and platform of origin. We require California residents to submit their IP address and the platform from which they download podcasts because, without that information, we have no way to act on their requests.

Name

Email address

What is your IP address?

What is your user agent?

- Select -

☐ I'm not a robot

**SUBMIT**

**STEP 2**

**Some data brokers asked consumers to submit information that they were reluctant to provide, such as a photo of their government ID.**

Some companies asked consumers to verify their identities or residence, for example by providing their government ID number, an image of their government ID, or a “selfie.” Testers reported that a few asked knowledge-based authentication questions, such as previous addresses or a home where someone has made a payment.

The histogram on page 27 shows the relative frequency of types of information testers were asked for and steps they were asked to take as part of their DNS request.<sup>54</sup>

---

<sup>54</sup> All requests are combined in this analysis (rather than broken down by broker), reflecting the overall experience of making DNS requests under the CCPA. For reporting what is asked of testers in the process, we used the answers to multi-select questions about what information testers were asked for and/or refrained from providing, and multi-select questions about actions they were asked to take and/or refrained from taking. As some of the action options were redundant of the information options, we combined a non-repeat subset of the action options with the information options. We also used text answers in these parts of the survey in qualitative analysis about the variety of DNS processes.

## DNS Request Processes



A company needs some personal information in order to process a “Do Not Sell” request—if a data broker sells records linked to email addresses, it needs to know the email address about which it is no longer allowed to sell information. Nevertheless,

companies are not allowed to mandate identity verification to process a DNS request under CCPA, and requesting sensitive information provided friction and led many consumers to abandon their efforts to opt out. See, for example, the Melissa Corporation, which requested consumers to provide “verification of California residency and consumer’s identity.”



The screenshot shows a web form for the Melissa Corporation. At the top is the Melissa logo. Below it is a header for the "California Consumer Privacy Act Notice (Show Details...)". The form contains three unchecked checkboxes: "Right to Know", "Right to Opt-Out of Sale of Personal Information", and "Right to Delete". A section titled "Please provide the information that you want to inquire." contains input fields for First Name, Last Name, Phone, Mobile Phone, Email, Address, Address2, City, State (a dropdown menu set to "CA"), and ZIP/Postal Code. Below this is a section for attaching verification documents, titled "\*Attach verification of California residency and consumer's identity (Supported files: .pdf, .jpg, .jpeg, .gif, .bmp, .png, .tif)". This section contains three "Choose File" buttons, each followed by the text "No file chosen". The entire "Attach verification" section is highlighted with a green rectangular box. At the bottom of the form is a blue "Submit" button.

The CCPA only covers California consumers,<sup>55</sup> and the statute and implementing regulations are ambiguous on how companies may require consumers to prove they are

<sup>55</sup> Cal. Civ. Code § 1798.140(g).

covered by the law. However, asking for proof of residence added difficulty to the opt-out process, especially as other companies achieved this objective by requesting the consumer's name, address, and email.

West Publishing Corporation, part of Thomson Reuters, also asked consumers to submit to identity verification to complete the opt-out process. As shown in the screenshot below, the site requires consumers to submit a photo of their government ID and a selfie, as well as their phone number. Once the phone number is submitted, the site sends a text to help facilitate the capture of these documents through the user's mobile phone.

The screenshot shows a web form for identity verification. At the top, there is a logo for 'the answer company THOMSON REUTERS'. Below this, a text box explains that identity verification is required for privacy protection and that data will be deleted after the transaction. The form contains three main sections: 'Drivers License' with a status of 'Incomplete', 'Facial Similarity Snapshot' with a status of 'Incomplete', and 'Mobile phone' with a text input field containing '(201) 555-0123' and a US flag icon. A green button labeled 'Continue on Mobile' is at the bottom.

While these requests might be appropriate in the case of an access or deletion request, where identity verification is important to make sure that data is not being accessed or

deleted without the consumer's consent, in the case of an opt out, it frustrates consumers' objectives to stop the sale of their personal information and does not provide additional privacy protection.

**Some data brokers led consumers to abandon opt outs by forcing them to accept cookies.**

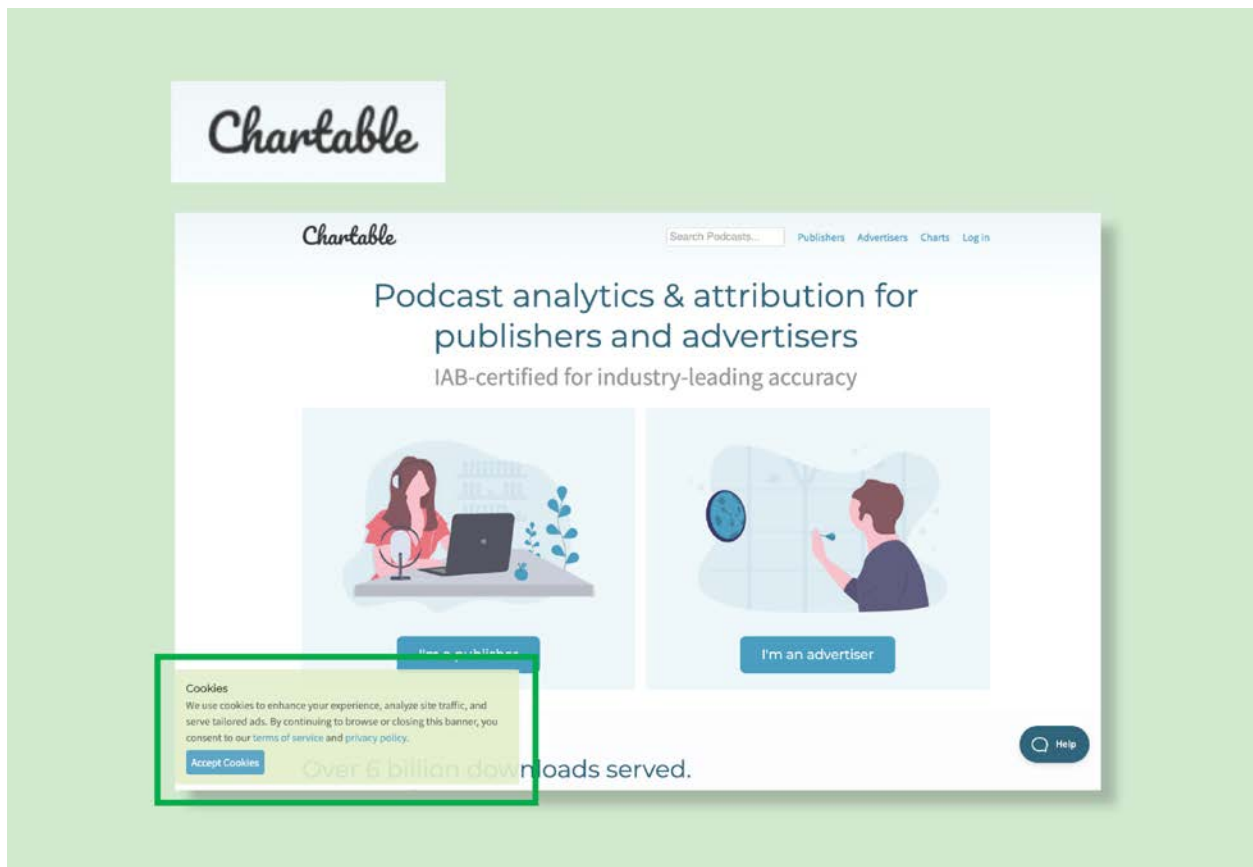
As the CCPA went into effect in January 2020, some California consumers noticed that when they visited websites, they were asked to opt in to the use of cookies—and expressed confusion about what they were being asked to do. These notices have been common in Europe in response to the e-Privacy Directive, and more recently the Global Data Protection Regulation, though privacy advocates have been deeply critical of the practice: companies often use dubious dark patterns to nudge users to click “OK,” providing the veneer, but not the reality of, knowing consent.<sup>56</sup> The expansion of cookie banners in California was borne out in our study. Sixty-six of the 214 brokers had at least one consumer report a request or mandate to accept cookies as part of the DNS process. In some cases, for example if a company only tracks online using cookies, it may be reasonable for a site to set a non-unique opt-out cookie to allow the opt out to persist across multiple sessions. But the examples we saw were confusing to consumers, and did not clearly convey that a cookie was going to be placed for the limited purpose of enabling the opt out of cross-site data selling. And, as previously noted, sometimes the cookie consent banners obscured links to opt-out processes on a company's home page (see discussion of Freckle I.O.T./PlacelQ's interface, *supra* p. 21-22, and *infra* p. 31).

When visiting the website of the data broker Chartable to opt out of the sale of information, visitors are required to accept cookies. Chartable explains that the cookies are used to “serve tailored ads.” The only option is to “Accept Cookies,” and it asserts that by browsing the site users are agreeing to its terms of service and privacy policy.

---

<sup>56</sup> *Most Cookie Banners are Annoying and Deceptive. This Is Not Consent*, PRIVACY INTERNATIONAL (last visited Aug. 28, 2020), <https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent>.





For nine brokers, at least one tester reported refraining from accepting cookies as part of the process. In five of these cases, testers reported that they stopped their request because they felt uncomfortable or did not understand next steps. For example, a Freckle I.O.T./PlacelQ tester described how accepting cookies was implicitly required for making a DNS request:

Their text-box asking to Allow Cookies covers the bottom 20% of the screen and won't go away unless, I assume, you tick the box to Allow. Therefore, I cannot see all my options. Also, I am accessing their site on a PC and they want me to download an app to my phone. Very difficult or impossible to see how to stop them from selling my data.

Another tester reported that the company they tested, Deloitte Consulting, had “two request types—‘Cookie Based’ and ‘Non-Cookie Based’” and that they were “skeptical that most people will be able to decode the techno-babble description of each type.”

**Consumers were often forced to wade through confusing and intimidating disclosures to opt out.**

While our survey did not include direct questions about communications with data brokers, 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.<sup>57</sup> 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.

**Some consumers spent nearly an hour, if not more, to complete a request.**

We also asked consumers about how long they spent to complete a request, and to not include the time spent filling out the survey. While the vast majority of consumers spent less than 15 minutes at a time on requests—and the most common amount of time was less than 5 minutes—some consumers reported that they nearly an hour or more than an hour opting out. A consumer working on the Jun Group reported that they were required to obtain their advertising ID to opt out: “Obtaining my Advertising Identifier was very time consuming and I am not sure how it is used.” The consumer testing Accuity reported: “They make it so hard to even find anything related to my information collected or subscribing or op-out that I had to read through so much boring yet infuriating do to what they collect and every one the will give it to for a price. We, as

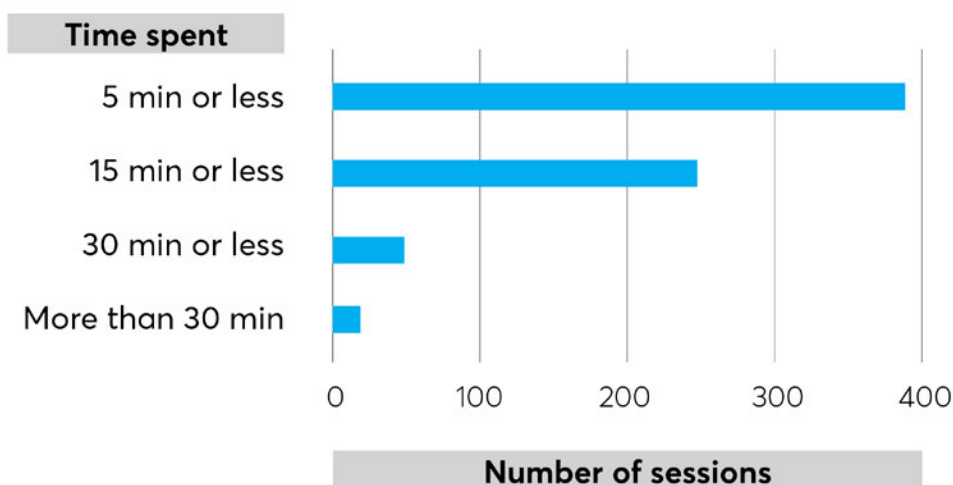
---

<sup>57</sup> ACBJ (last visited Aug. 10, 2020), <https://acbj.com/privacy#X>.

Americans shouldn't have to do this to keep our information out of advertising collectors.”

Even spending five minutes on a single opt-out request could prevent consumers from exercising their CCPA rights. A consumer would have to make hundreds of such requests to be opted out of all data brokers potentially selling their data—not to mention all of the other companies with which the consumer has a relationship.

## Sessions By Time Spent



**At least 14% of the time, burdensome or broken DNS processes prevented consumers from exercising their rights under the CCPA.**

Participants reported giving up in 7% of tests.<sup>58</sup> They reported being unable to proceed with their request in another 7% of tests.<sup>59</sup> These 14% of cases represent a DNS process clearly failing to support a consumer's CCPA rights.

<sup>58</sup> Example responses coded as “giving up” include: “Dead ended, as I am not going to send the info requested” and “Gave up because too frustrating. . . ”

<sup>59</sup> Example responses coded as “unable to proceed” include “the website is currently waiting for me to provide my IDFA number but I’m not sure how to adjust my settings to allow the new app permissions to retrieve;” “I could not Submit my form after several tries;” and “It looks like I did not email them after

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.

**The data broker X-Mode used data submitted as part of a DNS request to deliver a marketing email, a practice that is prohibited by the CCPA.**

X-Mode, a data broker that sells location data, used customer data provided to opt out in order to send a marketing email, in violation of the CCPA. Study participants voiced concerns about handing over additional personal information to data brokers in order to protect their privacy, and it was disappointing to discover that their concerns were warranted. Consumers are particularly sensitive about receiving additional marketing messages. One consumer, for example, shared with us that they began receiving more unsolicited robocalls after submitting the opt-out request. Reflecting these concerns, the CCPA specifically prohibits companies from using data collected to honor an opt-out request for any other purpose.<sup>60</sup>

---

*getting nowhere calling the number on their website that was supposed to handle requests and had no idea what I was talking about."*

<sup>60</sup> Cal. Civ. Code § 1798.135(a)(6).

But X-Mode ignored that requirement. X-Mode is a data broker that pays apps—such as weather and navigation apps—to collect location data from devices that have installed the software.<sup>61</sup> X-Mode makes money by selling insights drawn from that data to advertisers. For example, the Chief Marketing Officer of X-Mode explained, “If I walked by a McDonald’s but walk into a Starbucks, my device knows with the XDK that I passed a McDonald’s but I actually went into Starbucks.”<sup>62</sup> X-Mode also sells personal information to third party applications and websites.<sup>63</sup> And it has also shared anonymized location data with officials in order to help track compliance with stay-at-home orders during the COVID-19 crisis.<sup>64</sup> Because it sells such sensitive information, X-Mode should be particularly careful to protect the anonymity of consumer data and respect consumers’ privacy preferences.

After submitting the opt-out request in April 2020, the author received the following email confirming that she had been placed on an “CCPA Opt-out” mailing list:

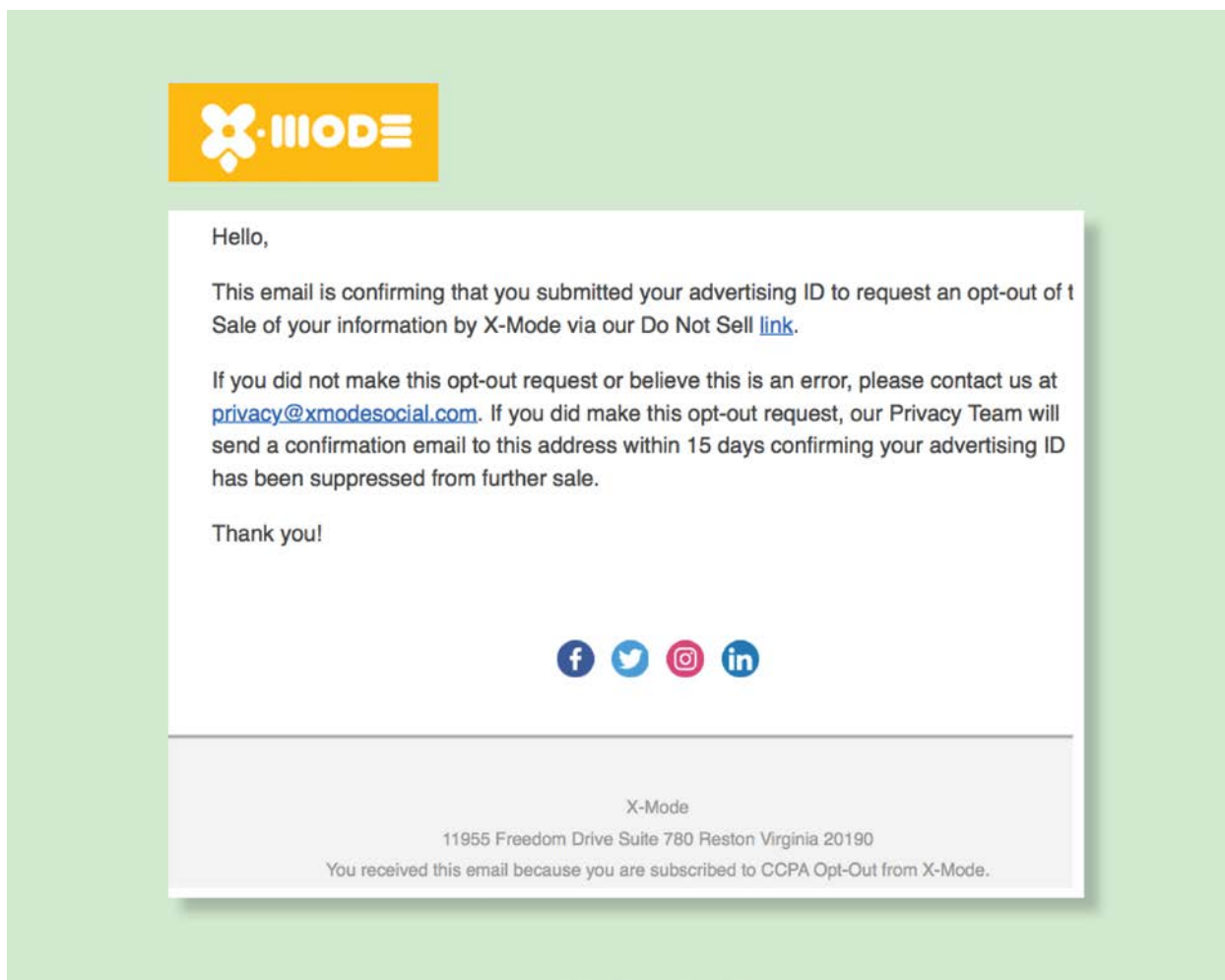
---

<sup>61</sup> Sam Schechner et al., *Tech Firms Are Spying on You. In a Pandemic, Governments Say That’s OK*, WALL ST. J. (June 15, 2020), <https://www.wsj.com/articles/once-pariahs-location-tracking-firms-pitch-themselves-as-covid-sleuths-11592236894>.

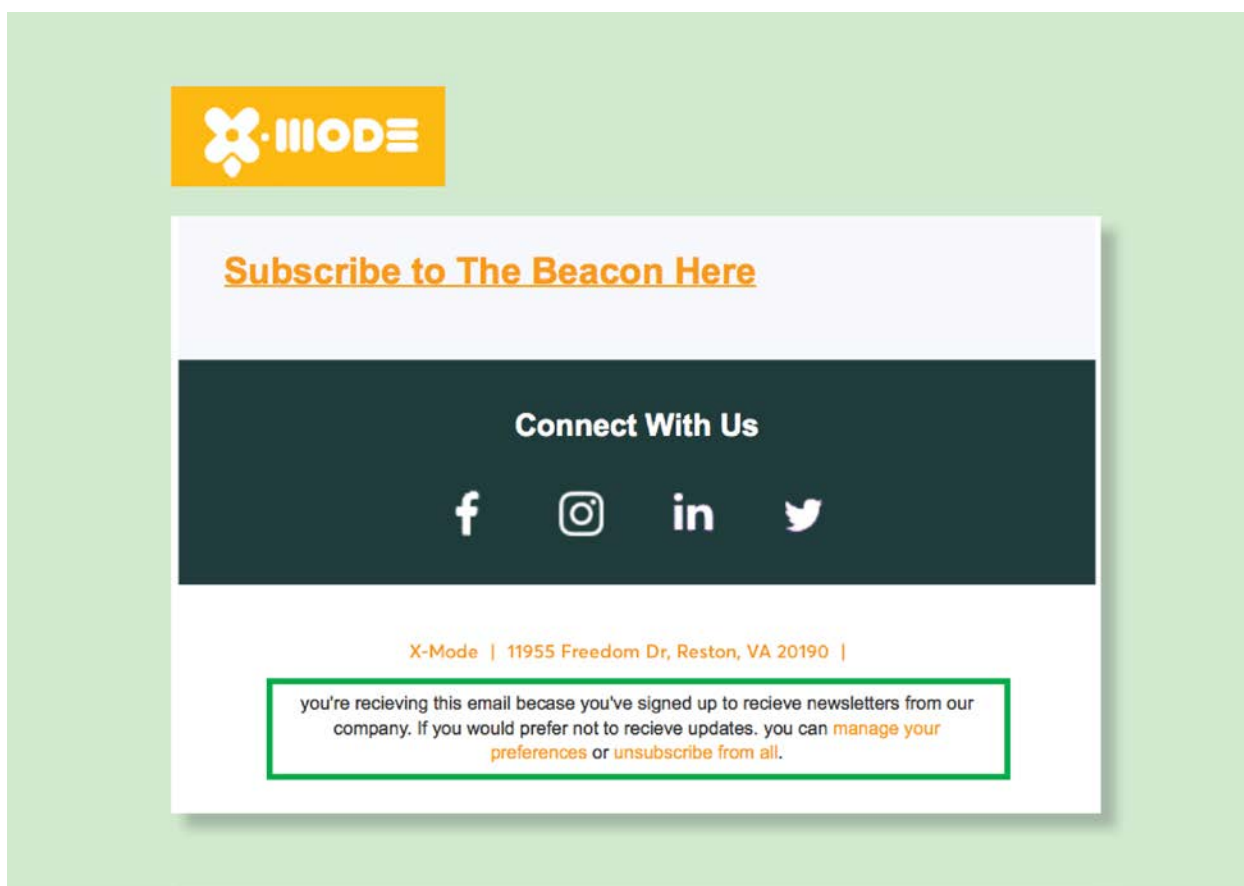
<sup>62</sup> Jake Ellenburg, quoted in Karuga Koinange, *How Drunk Mode, An App for the Inebriated, Became Data Location Company X-Mode Social*, TECHNICALLY (Feb. 27, 2020), <https://technical.ly/dc/2020/02/27/how-drunk-mode-app-became-data-location-company-x-mode-social/>.

<sup>63</sup> ZenLabs LLC, Privacy Policy (last visited Aug. 28, 2020), <http://www.zenlabsfitness.com/privacy-policy/>.

<sup>64</sup> Schechner et al., *Tech Firms Are Spying on You*, *supra* note 61.



The following month, the author received an email inviting her to subscribe to X-Mode's newsletter in order to keep up with the business. The fine print explained that the email was sent "because you've signed up to receive newsletters from our company[,]" with the option to unsubscribe.



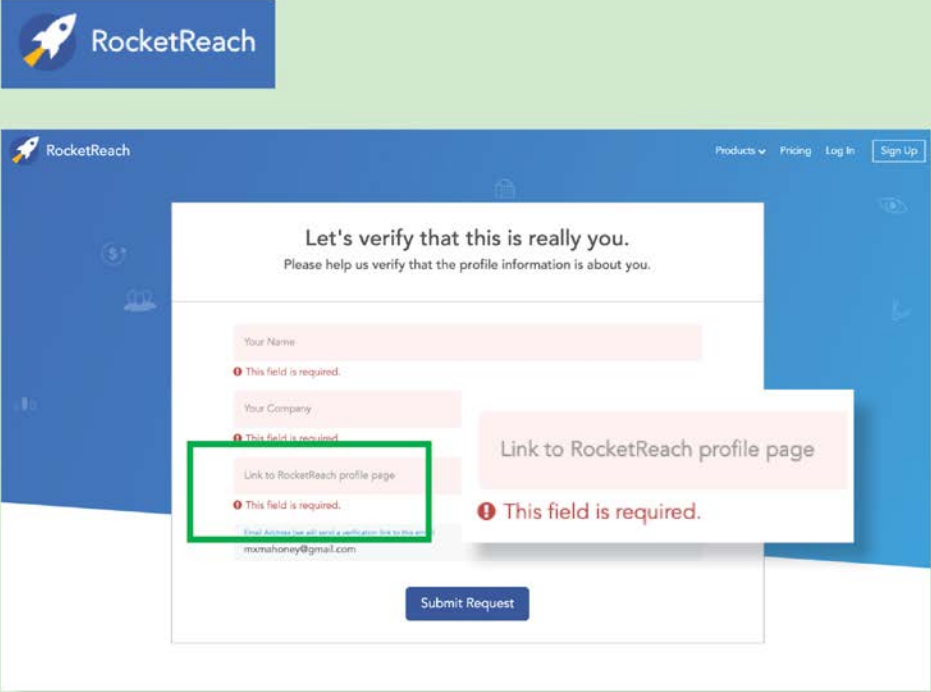
Since the only interaction that the author has had with X-Mode was to opt out—by definition, data brokers do not have relationships with consumers—the only way that she could have “signed up” was through opting out of the sale of her information. This behavior violates the CCPA’s prohibition on reuse of data provided for exercising data rights, and it could have a chilling effect on consumers exercising their rights with respect to other companies, as they are understandably worried about subjecting themselves to even more messages.

**The data broker RocketReach requires the user to set up an account to opt out, which is prohibited by the CCPA.**

RocketReach, a company that helps users find the contact information of potential business leads, requires users to list their RocketReach account in order to opt out of the sale of their information, even though the CCPA explicitly prohibits requiring



consumers to set up an account to opt out.<sup>65</sup> The homepage includes a link that reads “Do Not Sell My Info,” which then takes the consumer to a page that requires them to list their name, company, link to RocketReach profile, and email. If the user enters only name and email, the site does not let the user proceed further.

A screenshot of the RocketReach website's verification page. The page has a blue header with the RocketReach logo and navigation links for Products, Pricing, Log In, and Sign Up. The main content area is white and contains a form titled "Let's verify that this is really you." with the subtitle "Please help us verify that the profile information is about you." The form has four input fields: "Your Name", "Your Company", "Link to RocketReach profile page", and "Email Address". Each field has a red error message below it stating "This field is required." The "Link to RocketReach profile page" field is highlighted with a green rectangular box. Below the form is a blue "Submit Request" button. The background of the screenshot shows a blurred view of the website's interface.

This frustrated testers, one of whom said, “I cannot determine whether they hold any of my information because they require a company and RocketReach account profile in order to honor the do not sell request.”

**About 46% of the time, consumers were left waiting or unsure about the status of their DNS request.**

Neither the CCPA nor the implementing regulations require companies to notify consumers when their opt-out request has been honored, and this left consumers

---

<sup>65</sup> Cal. Civ. Code § 1798.135(a)(1).



confused about whether the company was still selling their information. 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.”

In looking at how often consumers gave up or were unable to complete requests, we found a wide variety of responses from brokers, and variation in how consumers interpreted those responses. Once a DNS request was submitted, broker responses included:

- no response at all;
- acknowledging the request was received but providing no other information;
- acknowledging the request was received and vague language leaving consumers unsure of what was next;
- saying the request would be implemented in a certain timeframe (ranging from 2 weeks to 90 days);
- asking consumers to provide additional information;
- confirming a different type of request (such as Do Not Contact or Do Not Track);<sup>66</sup>
- telling the consumer that the broker is not subject to the CCPA (even though the company was listed on the California data broker registry);
- telling the consumer that the broker has no data associated with them; and
- acknowledging the request was received and confirming that data will no longer be sold.

Consumers' understanding of these responses varied. For example, among participants reporting that the broker said that their request was received and that it would be

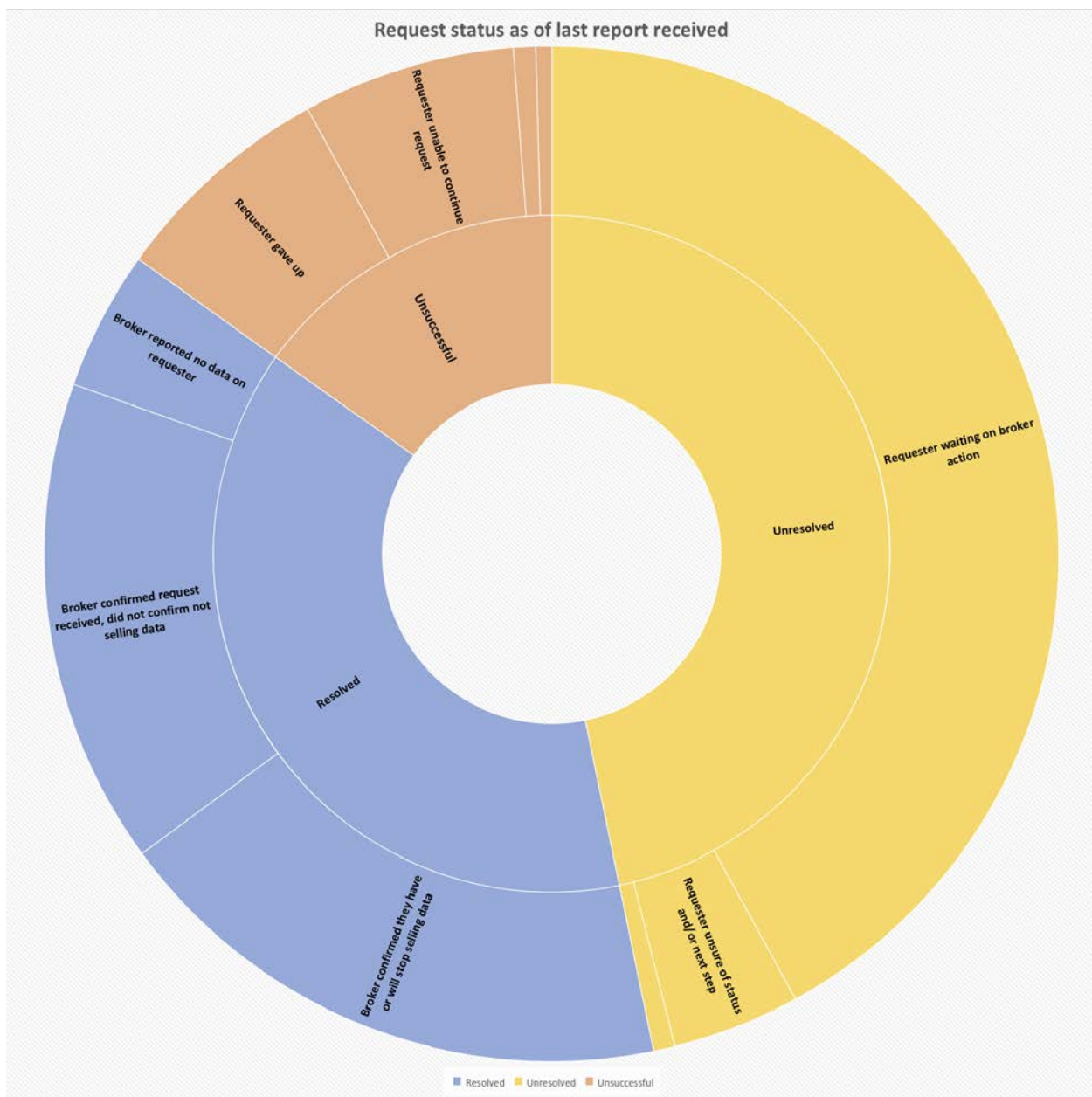
---

<sup>66</sup> Testers' references to “Do Not Contact” likely refer to consumers' right to be added to a company's internal “Do Not Call” list under the Telemarketing Sales Rule, 16 CFR § 310.4(b)(1)(iii)(A). Do Not Track refers to a request to stop tracking information about a consumer's activity across multiple sites. California law requires companies that collect personal information to disclose in the privacy policy whether they honor Do Not Track. See Cal. Bus. Prof. Code § 22575(5).

implemented in a certain time frame, some said the broker was honoring their DNS request but most said they were still waiting or unsure of the status of their request.

Below is a chart and visualization of the proportions of requests with different statuses as of the last report for each request:

Overall Status	Sub Status	Number Requests
Resolved	Broker confirmed they have or will soon stop selling data	107
	Broker confirmed request received, did not confirm not selling data	91
	Broker reported no data on requester	26
Unresolved	Requester waiting on broker action	247
	Requester unsure of status and/or next step	24
	Requester has outstanding follow up	4
Unsuccessful	Requester gave up	42
	Requester unable to continue request	40
	Broker reported not subject to CCPA	4
	Broker confirmed non-DNS request	3



We took a closer look at requests in which participants were “waiting” as of their last report, and found that many were still waiting for the data broker to respond to them after 21 days. Among the 247 requests in which the consumer was waiting for broker action, 81 were waiting after 21 days, 50 were waiting after at least a week but less than 21 days, and 116 of these were within 2 days of initiating a request. Those 116 represent cases where the broker may follow up later. However, the 81 cases in which consumers were still awaiting broker action after 21 days represent a problem with the

CCPA, in which consumers must choose between giving up and staying engaged for weeks at a time in hopes of receiving a clear confirmation from the broker that their DNS request has been completed. In 17 requests, the tester reported in an open-ended answer that they had had no response at all from the broker. Seven of these reports were after 21 days, and another 4 were after at least one week.

**About 52% of the time, the tester was “somewhat dissatisfied” or “very dissatisfied” with opt-out processes.**

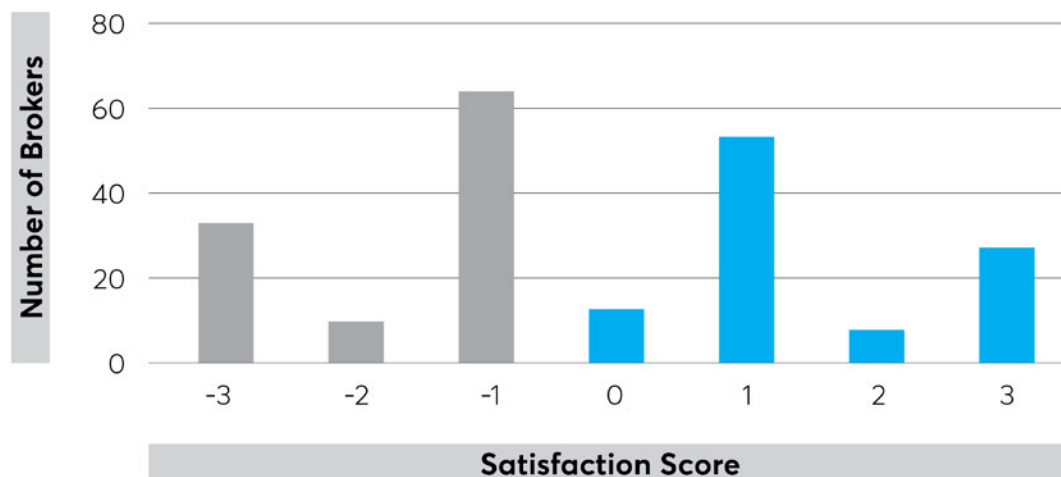
Overall, testers were more often dissatisfied than satisfied with the DNS processes. The survey asked how satisfied testers were with the process by providing four answers: very satisfied, somewhat satisfied, somewhat dissatisfied, very dissatisfied. The question was optional. Of the testers who answered this question, about 52% of the time, the tester was somewhat or very dissatisfied, and about 47% of the time, the tester was very or somewhat satisfied.<sup>67</sup>

We also assigned each broker a satisfaction score. Some companies had consistent satisfaction, others had consistent dissatisfaction, and most had processes leaving consumers mixed in their satisfaction levels. In the satisfaction score, a broker received a positive point for a “very satisfied” or “somewhat satisfied” answer, and a negative point for a “somewhat dissatisfied” or “very dissatisfied” answer. The number of brokers with each score is plotted on the next page.

---

<sup>67</sup> Testers answered this question in 601 tests. Of these tests, in 317 (52%), the respondent was “somewhat dissatisfied” or “very dissatisfied” with the opt-out process, and in 284 (47%) tests, the respondent was “very satisfied” or “somewhat satisfied.” In 41 cases, the tester did not answer the question.

## Tester Satisfaction



**Some data brokers had quick and easy opt-out processes, showing that companies can make it easier for consumers to opt out. About 47% of the time, the tester was “somewhat satisfied” or “very satisfied” with the opt-out process.**

In several cases, consumers reported either a one-step process using an online interface that confirmed their data would no longer be sold, or a prompt and clear confirmation via email from the broker that their data would no longer be sold. For example, one tester of American City Business Journals described the process: “Just had to go to the privacy link at the bottom of the home page. Found the Calif. privacy link then had to scroll to button to turn off ‘sell my info’.” Another shared an email from a DT Client Services, received the same day she submitted her request, that clearly confirmed that they would stop selling her data: “We confirm that we have processed your Request and will not sell your personal information to third parties.” These processes demonstrate an effective standard for implementing DNS requests. Overall, about 47% of the time, the tester was “somewhat satisfied” or “very satisfied” with the opt-out process.

It is also possible for data brokers to post DNS links that are easy to find. For example, for 58% of the brokers, all three testers found the DNS link on the broker’s website, suggesting that these links were posted prominently. Links that were easy to find were



described as “prominent and easy to find,” “at bottom of page, but large,” “bottom of page, bold,” and “prominent at bottom of home page.” Thirty-nine data brokers out of 214 had all three testers report that the DNS link was “very easy” to find. For brokers where three out of three testers found the DNS link, the link was reported “very easy” or “somewhat easy” to find in 65% of cases, and “very difficult” or “somewhat difficult” to find in only 13% of cases.

## Policy recommendations

### **The Attorney General should vigorously enforce the CCPA to address noncompliance.**

The AG should use its enforcement authority to address instances of noncompliance, and to incentivize other companies to comply. While the AG is hamstrung by flaws in the enforcement provisions of the privacy requirements, notably the “right to cure” language that lets companies off the hook if they “cure” the problem within 30 days,<sup>68</sup> taking action will help push companies to get into compliance. Our study showed that a few improvements would go a long way. For example, it was significantly easier to opt out of a data broker site when the company had a link clearly labeled “Do Not Sell My Personal Information” that took consumers directly to the interactive form. Once that element was removed, consumers were often adrift, forced to email customer service staff who may not understand the request, or sent through a maze of sites with confusing disclosures. The AG should make an example of companies that fail to meet these requirements to help bring all of them into compliance.

### **To make it easier to exercise privacy preferences, consumers should have access to browser privacy signals that allow them to opt out of all data sales with a single step.**

At the very least, consumers need access to universal opt-out tools, like browser privacy signals. Requiring consumers to opt out of every company one-by-one simply is not workable. The AG regulations require companies to honor platform-level privacy signals as universal opt outs, if the signal clearly constitutes a “Do Not Sell” command.<sup>69</sup> At the moment, however, there are no platform signals that we are aware of that clearly indicate a desire to out of the sale of data. Browsers are a logical place to start, though consumers need ways to opt out of advertising on devices other than browsers, such as

---

<sup>68</sup> Cal. Civ. Code § 1798.155(b).

<sup>69</sup> Cal. Code Regs. tit. 11 § 999 315(c) (2020).

TVs and phones. The AG should encourage developers to bring to market these solutions as quickly as possible, and should also set up a registry to help identify the signals that must be honored. This would help bring clarity for businesses and consumers.

**The AG should more clearly prohibit dark patterns, which are user interfaces that subvert consumer intent, and design a uniform opt-out button. This will make it easier for consumers to locate the DNS link on individual sites.**

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 a bunch of other links—a 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.”<sup>70</sup> The AG designed an initial draft, but declined to include a design in the final regulations. According to the AG, the proposed opt-out button was “deleted in response to the various comments received during the public comment period. The OAG has removed this subsection in order to further develop and evaluate a uniform opt-out logo or button for use by all businesses to promote consumer awareness of how to easily opt-out of the sale of personal information.”<sup>71</sup> While the original design came under a fair amount of criticism, a uniform button, regardless of what it ends up looking like, will likely have value for consumers seeking to opt out, and the AG should promulgate one as soon as possible.

This will also help address instances in which companies route consumers through multiple, unnecessary steps in order to opt out. For example, Outbrain (*infra*, p. 18) led consumers through multiple steps to opt out, and on nearly every page the consumer had to hunt to figure out which option would lead them to the next step. And after all that, at least one consumer told us that they were not sure they had even opted out. Given that 7% of our testers gave up on the opt outs out of frustration or concern about sharing additional information, confusing interfaces significantly undermined consumers' ability to opt out.

---

<sup>70</sup> Cal. Civ. Code § 1798.185(a)(4)(C).

<sup>71</sup> FSOR, *supra* note 27, at 15.

**The AG should require companies to notify consumers when their opt-out request has been honored.**

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.

Required notification is also important for compliance purposes. For example, the AG regulations require companies to comply with opt outs within 15 business days. Without providing any notification of the opt out completion, there's no way to judge whether or not the company has honored the law and to hold them accountable if not.

**The legislature or AG should clarify the definitions of “sale” and “service provider” to more clearly cover data broker information sharing.**

In response to the CCPA, many companies have avoided reforming their data practices in response to “Do Not Sell” requests by arguing that data transfers either are not “sales,” or that transferees are “service providers” such that opt-out rights do not apply.<sup>72</sup> Certainly, while some sharing with true data processors for limited purposes should not be subject to opt-out requests, many companies' interpretation of the CCPA seems to argue that third-party behavioral targeting practices are insulated from consumer choice.<sup>73</sup> As such, even if a consumer successfully navigates a DNS request from a data broker, in practice exercising opt-out rights may have little to no practical effect. Policymakers should close these potential loopholes to clarify that, *inter alia*, data broker information sharing for ad targeting is covered by CCPA obligations.

**Privacy should be protected by default. Rather than place the burden on consumers to exercise privacy rights, the law should require reasonable data minimization, which limits the collection, sharing, retention, and use to what is reasonably necessary to operate the service.**

---

<sup>72</sup> Mahoney, *Companies Aren't Taking the CCPA Seriously*, *supra* note 5.

<sup>73</sup> 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](https://www.iab.com/wp-content/uploads/2019/12/IAB_CCPA-Compliance-Framework-for-Publishers-Technology-Companies.pdf); Patience Haggin, *Facebook Won't Change Web Tracking in Response to California Privacy Law*, WALL ST. J. (Dec. 12, 2019), <https://www.wsj.com/articles/facebook-wont-change-web-tracking-in-response-to-california-privacy-law-11576175>.



While our study demonstrates that too many companies do not appear to be complying in good faith with the CCPA, any model that relies upon individuals to affirmatively act to safeguard their privacy will be deeply flawed. Given the challenges posed to businesses and consumers with respect to opting out, a better model is to ensure that privacy is protected without the consumer having to take any additional action. Several consumers who signed up for the study expressed shock that they were expected to opt out of the sale of their information. The thought of having to work their way through the entire data broker registry, which had hundreds of companies, was near unimaginable for these participants. Hard-to-find links, if they're even posted at all, confusing opt-out processes, requiring consumers to submit additional personal information, and above all the fact that there are hundreds of data brokers on the registry alone—all suggest that the responsibility needs to be on the company to protect privacy in the first place, rather than placing all the responsibility on the consumer.

This is a particularly important issue for elderly consumers or others who may have difficulty navigating online, several of whom dropped out of our study because it was so challenging to complete a single opt out. While there may be an easier path forward for some consumers who are able to take advantage of browser privacy signals to opt out universally—those are people who are already fairly tech savvy in the first place. Further, such a system only limits the sale of online data or data collected via a platform; it wouldn't stop the sale of data collected, say, in physical stores.

A better model would simply be to prohibit the sale of personal information as a matter of law, and to mandate that companies only collect, share, use, or retain data as is reasonably necessary to deliver the service a consumer has requested. Consumer Reports has supported legislation to amend the CCPA, AB 3119 (2020), that would require just that; Senator Sherrod Brown has introduced similar legislation, the Data Accountability and Transparency Act of 2020, at the federal level.<sup>74</sup> While the CCPA and the California data broker registry law are important milestones that improve transparency and individual agency, ultimately a more robust approach will be needed to truly protect Californians' privacy.

---

<sup>74</sup> The Data Accountability and Transparency Act of 2020, Discussion Draft, <https://www.banking.senate.gov/imo/media/doc/Brown%20-%20DATA%202020%20Discussion%20Draft.pdf>.

## Conclusion

Overall, we found that consumers were too often dissatisfied with CCPA opt-out processes. This study uncovered some cases where the DNS process was short, clear, and satisfactory. It also found that some companies aren't complying with the CCPA, and that consumers were often left frustrated and without confidence that they had successfully exercised their DNS rights. It also reveals that, too often, consumers were unable to make a DNS request or gave up on the process altogether. Policymakers need to adopt crucial reforms in order to ensure that consumers can enjoy their right to privacy under the California Constitution.<sup>75</sup>

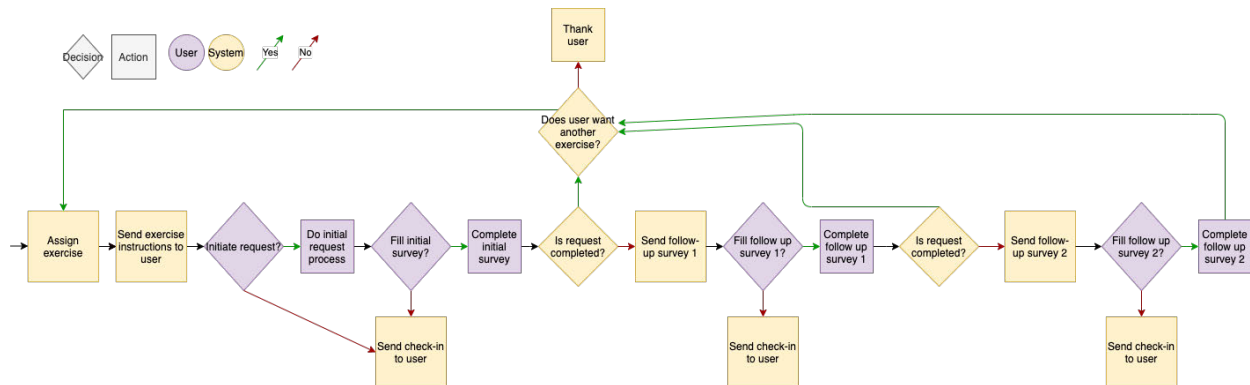
---

<sup>75</sup> Cal. Cons. § 1.

## Appendix

### Section A

Below is a diagram of the participant experience of the exercise. Participants were randomly assigned a data broker from the registry using custom software, and were emailed with instructions to attempt making a DNS request to that broker. Participants then reported their experience with the DNS process via survey immediately after their first session working on the request. Participants were prompted by email to fill out follow-up surveys at one week and 21 days (approximately 15 business days) to report on any subsequent steps they had taken or any updates on the status of their request they had received from the data broker.



## Section B

Below, we include links to screenshots of the homepages of data brokers that did not have the required "Do Not Sell My Personal Information" links on their homepages.

[adMarketplace, Inc.](#)  
[Big Brook Media, LLC](#)  
[Blue Hill Marketing Solutions, Inc.](#)  
[Comscore, Inc.](#)  
[Electronic Voice Services, Inc.](#)  
[Enformion, Inc.](#)  
[Exponential Interactive, Inc. doing business as VDX.tv](#)  
[Gale](#)  
[GrayHair Software, LLC](#)  
[Infinite Media Concepts Inc.](#)  
[JZ Marketing, Inc.](#)  
[LeadsMarket.com LLC](#)  
[Lender Feed LC](#)  
[On Hold-America, Inc. DBA KYC Data](#)  
[Outbrain Inc.](#)  
[PacificEast Research Inc.](#)  
[Paynet, Inc.](#)  
[PossibleNow Data Services, Inc](#)  
[RealSource Inc.](#)  
[Social Catfish LLC](#)  
[Spectrum Mailing Lists](#)  
[SRAX, Inc.](#)  
[USADATA, Inc.](#)  
[zeotap GmbH](#)

## Section C

An additional five companies had “Do Not Sell” links on their homepages, but all three testers were unable to find the DNS link, suggesting that it may not have been posted in a “clear and conspicuous manner” as required by the CCPA. Below, we include links to screenshots of the homepages of these companies.

[AcademixDirect, Inc.](#)

[Fifty Technology Ltd.](#)

[Freckle I.O.T. Ltd./PlacelQ](#)

[Marketing Information Specialists, Inc.](#)

[Media Source Solutions](#)

**From:** [Kammerer, Susan](#)  
**To:** [Privacy Regulations](#)  
**Cc:** [Merz, Jeremy](#)  
**Subject:** APCIA Comments  
**Date:** Wednesday, October 28, 2020 10:52:22 AM  
**Attachments:** [image003.png](#)  
[CA CCPA Regulations - Third Round - APCIA Comments - Final.pdf](#)

---

To Whom it May Concern:

Thank you for the opportunity to provide comments on the California CCPA regulations.  
Please see APCIA's attached comment letter.

Thank you,

Susan Kammerer  
Administrative Assistant  
APCIA  
1415 L Street, Suite 670  
Sacramento, CA 95814





October 28, 2020

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

VIA Electronic Mail: PrivacyRegulations@doj.ca.gov

Dear Lisa Kim:

The American Property Casualty Insurance Association (APCIA)<sup>1</sup> appreciates the opportunity to provide comments on the Third Set of Proposed Modifications to the California Consumer Privacy Act Regulations (Proposed Revisions). We respectfully provide recommendations for your consideration below.

**999.306(b)(3) – Notice of Right to Opt-Out of Sale of Personal Information.**

The Proposed Modifications in subsection (3) may create compliance uncertainty and consumer confusion in a circumstance where the business separately collects information on-line and off-line. For example, a business may only sell personal information it collects about online website users or from internet-enabled technology devices. Nonetheless, if that business separately collected personal information offline that is not sold, it would be required to notify offline consumers of the sale of online information. This could be confusing for consumers. As such, APCIA recommends changing “collects personal information” to “sells personal information it has collected.” Thus, the requirement and illustrative examples would be appropriately limited to businesses that sell personal information they have collected, either online or offline.

**999.315(h) – Requests to Opt-Out**

Subsection (h) provides a list of illustrative examples that clarify what is considered an easy opt-out procedure that does not subvert or impair consumer choice and utilizes minimal consumer steps. APCIA

---

<sup>1</sup> APCIA is the preeminent national insurance industry trade association, representing property and casualty insurers doing business locally, nationally, and globally. Representing nearly 60 percent of the U.S. property casualty insurance market, APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers. APCIA represents the broadest cross-section of home, auto, and business insurers of all sizes, structures, and regions of any national trade association.

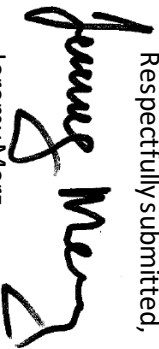
believes the examples are prescriptive and unnecessary. For instance, subsection (1) places an arbitrary requirement that the steps a consumer is required to take for executing an opt-out cannot be greater than those required to opt-in. This does not account for different technological components involved in completing those choices. Further, subsection (h)(3) is contrary to other privacy requirements that a business explain the impacts of a consumer's privacy choice. As an alternative, the illustrative examples should become factors in determining whether an opt-out method is permissible. This is a more flexible approach that will allow companies to meet the requirements without being faced with impossible choices about privacy disclosures or effective technology solutions.

**999.326(a) – Authorized Agent**

The Proposed Revisions are positive in that they promote more choice and flexibility in agent authorization practices, while retaining the ability to require the consumer to verify their identity as necessary.

Thank you for the opportunity to comment. Please let us know if you have any questions or would like additional information.

Respectfully submitted,

A handwritten signature in black ink that reads "Jeremy Merz". The signature is written in a cursive, slightly slanted style.

Jeremy Merz

Vice President, State Government Relations





**From:** [Dale Smith](#)  
**To:** [Privacy Regulations](#)  
**Subject:** CCPA Written Comment on Proposed Regulations Due October 28 (Transmitting)  
**Date:** Wednesday, October 28, 2020 11:51:56 AM  
**Attachments:** [footerNew2.bmp](#)  
[20201028 CCPA Comments.pdf](#)

---

Dear Privacy Regulations Coordinator:

Attached to this email is our .pdf document containing PrivacyCheq's submission of comment for NOTICE OF THIRD SET OF PROPOSED MODIFICATIONS TO TEXT OF REGULATIONS, released October 12, 2020 (comment period closing on October 28).

Thank you for this opportunity to comment.

Dale Smith

DALE R. SMITH, CIPT

*Futurist*



View my blog at: [privacyelephant.com](http://privacyelephant.com)



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

Via Email to: [PrivacyRegulations@doj.ca.gov](mailto:PrivacyRegulations@doj.ca.gov)

Attn: Honorable Xavier Becerra, Attorney General

Re: Comments on NOTICE OF THIRD SET OF PROPOSED MODIFICATIONS TO TEXT  
OF REGULATIONS, Released October 12, 2020

Dear Mr. Becerra:

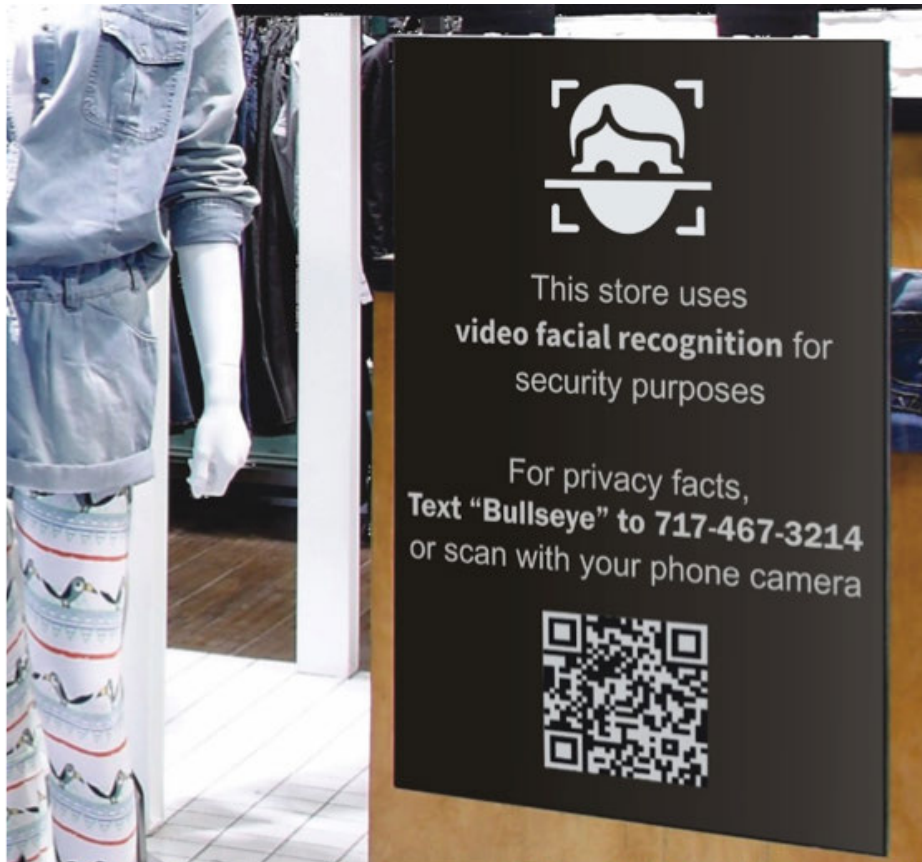
The newly added section §999.306(b)(3)(a) sets forth an illustrative example of how a consumer can be made aware of the right to opt-out in a brick-and-mortar, offline situation. It suggests using a printed paper form and/or by posting appropriate signage.

We are commenting to point out that both of these methods can be operationally enhanced if combined with the use of a QR code<sup>1</sup> and just-in-time notice in conjunction with the paper form or signage. Addition of the QR code technology can bring interactivity between business and consumer even in an offline setting.

---

<sup>1</sup> [https://en.wikipedia.org/wiki/QR\\_code](https://en.wikipedia.org/wiki/QR_code)

A fictitious example can demonstrate how this works. Figure 1 below visualizes one of the many ways a QR code might be deployed for use in an offline retail setting. Here, the content of the signage is static and venue-specific, but the addition of the QR code gives life to a “just-in-time” interactive notice readily available to the consumer.



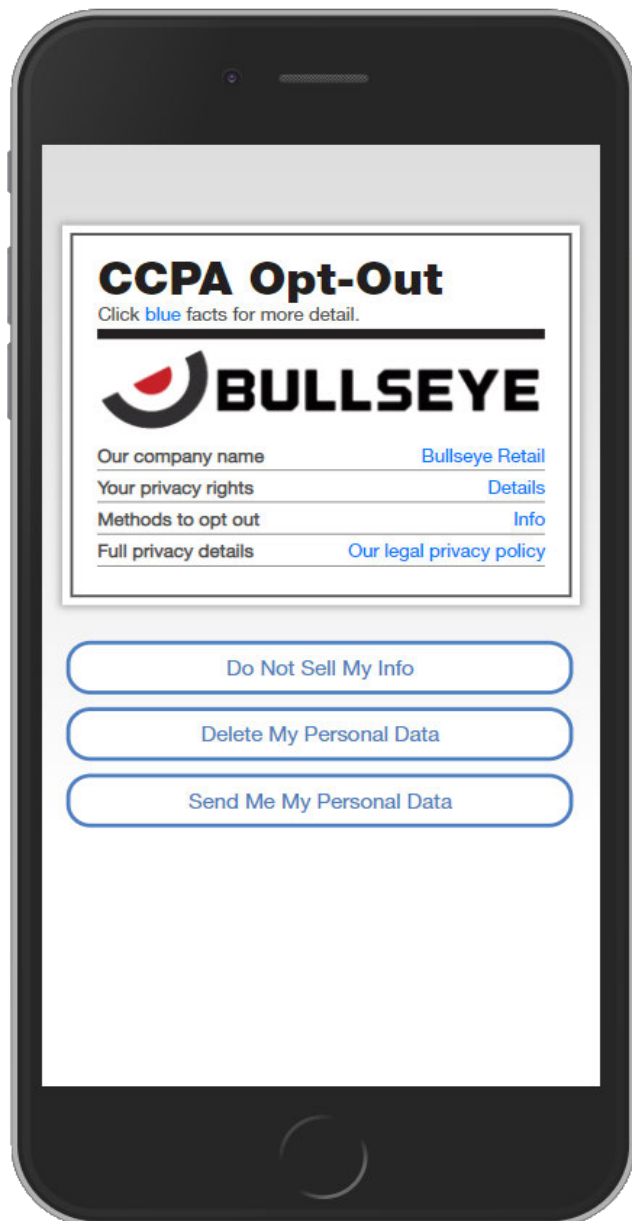
**Figure 1**

Seconds after the consumer “shoots” the QR code on the signage using his smartphone app<sup>2</sup>, a §999.306-compliant notice will appear on the consumer’s phone, ready to interactively inform the consumer of appropriate CCPA rights and choices.

<sup>2</sup>

<https://www.google.com/search?q=smartphone+qr+scanner+app&oq=qr+smaratphone+app&aqs=chrome.1.69i57j0i22i30i457j0i22i30i3j0i8i13i30i2.16643j0j7&sourceid=chrome&ie=UTF-8>

Figure 2 illustrates how that smartphone screen might look.



**Figure 2**

As before, the content of this fictitious screen visualizes several of the many ways an interactive notice can put consumers in the driver's seat regarding their privacy choices. In this example, in addition to presenting drill-down §999.306-specific information, the Do Not Sell, Access, and Deletion rights are set forth as options on the notice's front page.



This scenario demonstrates how the addition of public domain QR technology can transform a retail pamphlet or mall sign into an opportunity for a consumer to interact easily and directly with a business in real time to understand and take advantage of privacy rights provided by CCPA.

**Regarding our specific comment, we suggest that in order to enrich the illustrative examples referenced in §999.306(b)(3), verbiage should be added to §999.306(b)(3)(a) mentioning the utility of the QR code concept as an efficient and practical means of informing consumers in offline environments.**

Use of a QR “trigger” to deliver on-demand, “just-in-time” notices also meets the purpose under §999.305(a) Notice of Collection and §999.307(a) Notice of Financial Incentive.

Additional information on practical CCPA just-in-time 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](#), and [March 27, 2020](#).

Finally, we respectfully reiterate our previous suggestion that the ubiquitous Nutrition Label framework be named within the regulations as an example of a readily adaptable standard and functional implementation of what is called for in §1798.185(a)(4)(C)<sup>3</sup>.

We thank you for these opportunities to comment.

A handwritten signature in black ink, appearing to read 'DRA', with a long, sweeping horizontal line extending to the right.

Dale R. Smith, CIPT  
Futurist



---

<sup>3</sup> §1798.185(a)(4)(C) 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.

**From:** [Emery, Emily](#)  
**To:** [Privacy Regulations](#)  
**Cc:** [Emery, Emily](#)  
**Subject:** MPA Comments on the Third Set of Proposed Modifications to Text of CCPA Regulations  
**Date:** Wednesday, October 28, 2020 1:19:02 PM  
**Attachments:** [MPA Comments on Modifications to CCPA Rulemaking 10.28.2020.pdf](#)

---

Attached, please find comments on the third 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.

Emily Emery  
Director of Digital Policy  
**MPA - The Association of Magazine Media**  
Cell: [REDACTED]  
Office: [REDACTED]  
[REDACTED]

October 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 Third Set of Proposed Modifications to Text of Regulations Implementing the California Consumer Privacy Act (CCPA) 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. MPA represents the interests of all types of magazine media companies, from the largest global companies to the smallest independent journal, and their news, business and finance, lifestyle, and enthusiast brands that appeal to a broad set of interests. Members of our industry connect with more than 90 percent of all U.S. adults through the digital and print magazine titles readers value most.

Having testified 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 third set of proposed modifications to the regulations implementing the California Consumer Privacy Act (“CCPA”).

Almost a full year into implementation of the CCPA, it is extremely important that the third set of proposed modifications not undermine the extensive efforts undertaken and procedures implemented by magazine media companies and others based on previous versions of the rulemaking. Further, consumers have now developed expectations regarding CCPA processes that should not be upended. In the sections below, MPA makes recommendations with respect to the OAG’s proposed modifications to requirements for offline notices, number of allowable steps for opt-out, and requests made through authorized agents. Please note that 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, the offline notice may include a web address that the customer can access to opt-out of the sale of their personal information**

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.

To facilitate that common, expected consumer practice and enhance compliance with the aims of the CCPA, the OAG should confirm that in order 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 recommends that the OAG modify the proposed regulatory text in section 999.306(b)(3) to include an additional illustrative example:

**(c) A business that collects personal information from consumers 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 additional clarification – that the provision of a web address on printed material is an offline notice – would aid in compliance where consumer information is collected from a printed paper form that is then mailed by the consumer. This illustrative example for printed materials sent through the mail is consistent with existing regulation 999.305(b)(3) that offline notices may direct consumers to where the “Do Not Sell My Personal Information” webpage can be found online, and is analogous to the proposed illustrative example 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 in order 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 further clarify in 999.315 on requests to opt-out that two expected, common practices that enhance the consumer experience while promoting the minimal number of steps to opt-out are permitted.**

MPA agrees that the steps for submitting a request to opt-out should be minimal and should not subvert consumer intent. However, MPA is concerned that requiring parity in the number of steps to opt-out and to opt-in could incentivize businesses to add additional steps to both the opt-in and opt-out process that do not enhance the consumer experience or privacy protections but merely ensure technical compliance with the CCPA, or present obstacles for businesses to employ standard identity verification processes that enhance consumer data security.

MPA recommends that the OAG make the following additional modification to the proposed modifications to text in Section 999.315(h)(1):



- (1) The business’s process for submitting a request to opt-out shall not require more steps than that business’ process for a consumer to opt-in to the sale of personal information after having previously opted out. *A business’ process to validate a user’s identity shall not count in the number of steps to opt-in or opt-out.* The number of steps for submitting a request to opt-out is 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 is measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request, *not including identity verification.*

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 indicate 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 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 action if they do not wish to take advantage of the offer.*

**III. The OAG should strike its proposed modified language in Section 999.326(a) on authorized agents and continue to permit a business to exercise direct consumer engagement to effectively make good-faith efforts to respond to suspected threats to consumers’ data security.**

The current CCPA text allows businesses to authenticate right to know and data deletion requests filed by either consumers directly or 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 practices by authorized agents that undermine consumers' data privacy and security. Therefore, MPA is concerned that the proposed language in Section 999.326(a) could impede the necessary steps that businesses would take to effectively respond to instances of suspected consumer fraud by purported authorized agents.

Reducing the avenues available for a business to obtain verification, particularly in instances of suspected fraud, both undermines consumer data security and is counter to the CCPA's authentication requirements found outside the section on authorized agents.

To maximize the protection of consumer data, a business must continue to have the ability to both directly verify identity with the person to whom the request is related, and to confirm that the consumer provided the authorization to the agent submitting the request.

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, the business may require that the consumer:**

**(1) Provide the authorized agent signed permission to do so.**

**(2) Verify their own identity directly with the business.**

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

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

\*\*\*

MPA believes that adopting the additional clarifications proposed above will enhance the ability of businesses, including the magazine media industry, to operationalize consistent privacy-protective practices that comply with the law, enhance reader trust, and preserve the viability of the magazine media brands that consumers enjoy.

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

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:** [Leder, Leslie](#) on behalf of [Mohammed, Shoeb](#)  
**To:** [Privacy Regulations](#)  
**Subject:** Comments to Third Modified CCPA Regulations  
**Date:** Wednesday, October 28, 2020 1:22:01 PM  
**Attachments:** [FINAL CalChamber Comments to Third Modified CCPA Regulations.pdf](#)  
**Importance:** High

---

Ms. Kim,

Attached please find CalChamber's comments to Text of Third Modified CCPA Regulations.

Thank you,

**Shoeb Mohammed**  
Policy Advocate



California Chamber of Commerce  
1215 K Street, 14th Floor  
Sacramento, CA 95814

T [REDACTED]  
F 916 325 1272

Visit [calchamber.com](http://calchamber.com) for the latest California business legislative news plus products and services to help you do business.

*This email and any attachments may contain material that is confidential, privileged and for the sole use of the intended recipient. Any review, reliance or distribution by others or forwarding without express permission is strictly prohibited. If you are not the intended recipient or have reason to believe you are not the intended recipient, please reply to advise the sender of the error and delete the message, attachments and all copies.*

October 28, 2020

SENT VIA EMAIL

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

**Re:** Written Comments to Third 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) Third Set of Proposed Modifications to Text of California Consumer Privacy Act (CCPA) Regulations. As outlined in Section I, we believe this set of proposed modifications to the CCPA violates the APA and should be withdrawn. Sections II-IV outline concerns and substantive edits to the proposed modifications. Recommended revisions are formatted with additions in underline and deletions in ~~strikeout~~. Additionally, requests for clarification are outlined separately in Section V below.

### COMMENTS

#### I. The Third Proposed Modifications Violate the Administrative Procedures Act

We believe the proposed amendments are unlawful and invalid because they violate the procedural requirements of California Government Code (GC) section 11340 et seq, the California Administrative Procedure Act (APA). GC 11346.4(b) provides that a Notice of Proposed Action is valid for one year. The 3rd proposed amendment was published on October 12, 2020, which is more than one year after the original the Notice of Proposed Action, which was dated October 11, 2019. Since 2020 is a leap year, the proposed 3rd amendments were published 367 days after the original Notice of Proposed Action.

The regulations implementing the California Consumer Privacy Act in this rulemaking were first submitted by the Department of Justice (DOJ) to the Office of Administrative Law (OAL) for review on June 3, 2020 (OAL Matter No. 2020-0603-03S). The outcome for this Matter was "Partial Approval, Partial Withdrawal". According to the Notice of Third Set of Proposed Modifications to Text of Regulations "[t]he Department withdrew the following sections from the review of the Office Administrative Law (OAL) pursuant to Government Code section 11349.3, subd. (c): 999.305(a)(5), 999.306(b)(2), 999.315(c), and 999.326(c)." The modified text published on October 12, 2020, proposes to add new regulatory language in sections 999.306(b)(3), 999.315(h), and 999.332(a), and to add and delete language in section 999.326(a). None of the

provisions added or modified in the 3rd amendments modify the subdivisions which were originally withdrawn.

However, even if the 3rd amendments did modify subdivisions originally withdrawn, we believe it would still violate APA requirements. Regulations which are withdrawn during OAL review may be modified and resubmitted, but this must be done within the original one-year Notice period. The APA provides that regulations submitted to OAL may either be disapproved by OAL or withdrawn from OAL at the rulemaking agency's request (GC 11349.3). The process for disapproval is defined by GC 11349.3(b). Withdrawal of a regulation by the rulemaking agency is regulated by GC 11349.3(c). Subdivision (c) provides, in part, that "Any regulation returned pursuant to this subdivision [i.e. a withdrawn regulation] shall be resubmitted to the office for review within the one-year period specified in subdivision (b) of Section 11346.4 or shall comply with Article 5 (commencing with Section 11346) prior to resubmission."

The APA provides that a regulation disapproved by OAL may be resubmitted to OAL within 120 days of the disapproval. A regulation withdrawn by the submitting agency, in contrast, must be resubmitted to OAL, if at all, while the original one-year Notice remains valid. The 120-day extension that the APA provides for disapproved regulations does not apply to withdrawn regulations.

Since the 3rd amendments to the CCPA regulations were published after expiration of the original Notice of Proposed Action, they cannot possibly be "resubmitted to the office [OAL] for review within the one-year period specified in subdivision (b) of Section 11346.4." Under GC 11349.3(c), the only way that these proposed regulations may be lawfully implemented is by "comply[ing] with Article 5 (commencing with Section 11346) prior to resubmission." Article 5 requires, in essence, that a new Notice of Proposed Action be issued, a new 45-day public comment period occur, etc. In summary, to modify a withdrawn regulation, an agency must either resubmit the withdrawn regulation to OAL during the one-year life of the original Notice, or it must start the rulemaking process over from the beginning.

Accordingly, we respectfully request the Department to withdraw this Third Set of Proposed Modifications to Text of California Consumer Privacy Act (CCPA) Regulations and restart a new notice period under the APA.

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

### A. Issue: The requirement to provide notice by an offline method should only apply if information collected offline is sold.

#### 1. Proposed Regulation: 999.306(b)(3)

§999.306(b) requires businesses to provide consumers with an offline method of opting out of the sale of personal information even if the businesses are not selling information that is collected offline. Businesses that do not engage in the practice of selling information shared offline should not be required to post signage implying that the information shared offline is subject to sale. Accordingly, this

section should be narrowed in scope to apply only when businesses are collecting and selling information that is collected offline.

2. Recommended Change: Revise §999.306(b)(3) as follows:

(3) A business that collects personal information in the course of interacting with consumers offline and sells such information shall also provide notice by an offline method that facilitates consumers' awareness of their right to opt-out. Illustrative examples follow:

- a. A business that collects personal information from consumers in a brick-and mortar store and sells such information may provide notice by printing the notice on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the notice can be found online.
- b. A business that collects personal information over the phone and sells such information may provide the notice orally during the call where the information is collected.

B. Issue: The illustrative requirement to post signage in areas where personal information is collected may prohibit signage in more effective and noticeable locations.

1. Proposed Regulation: 999.306(b)(3)(a)

§999.306(b)(3)(a) requires businesses to post signage in the areas where personal information is collected. However, this could be read to prohibit businesses from prominently posting signage in high visibility areas such as store entrances and doorways if personal information is not necessarily collected at these points.

Further, the option to post signage "in the area where the personal information is collected" could be read to require signs at each point of sale or cash register in the state. In many stores, however, points of sale and cash registers are high interaction areas where consumers are not likely to see the notices. For this reason, it would be reasonable to allow businesses more options to post prominent signage.

2. Recommended Change: Revise §999.306(b)(3)(c) to illustrate that signage at the front door or similar prominent area is sufficient to satisfy the rule.

III. SECTION 999.315 – Requests to Opt-Out.

A. Issue: The regulation prohibits businesses from providing essential disclosures of information that could be relevant and informative to users.

1. Proposed Regulation: 999.315(h)

§999.315(h) prohibits businesses from requiring consumers to “click through” or “listen to reasons” why they should not submit a request to opt-out but fails to allow some reasonable degree of notice for the consumer. As drafted, the regulation prohibits additional disclosures of information that could be important, relevant and informative to users.

2. Recommended Change: Revise §999.315(h) to allow businesses to provide a reasonable degree of notice to the consumer.

IV. SECTION 999.326 – Authorized Agent.

A. Issue: Modifications will prohibit businesses from requiring two forms of identity verification when requests to know or delete information come from third parties.

1. Proposed Regulation: 999.326(a)

§999.326(a) requires businesses to choose between one of two forms of identity verification when a consumer uses an authorized agent to submit a request. Businesses should be allowed to use both forms of identity verification when authorizing consumer requests that come from third parties. As drafted, the regulation requires businesses to choose just one.

2. Recommended Change: Restore §999.326(a) to previous draft.

V. Requests for Clarification

A. §999.315(h)(5): Request clarification about how this section aligns with the existing requirements in CCPA §1798.120(b) and §1798.115(d).

B. §999.326(a): Request clarity about what “proof” is sufficient to evidence “signed permission to submit the request”

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:** [Melanie Tiano](#)  
**To:** [Privacy Regulations](#)  
**Subject:** CTIA Comments on CCPA Modified Regulations  
**Date:** Wednesday, October 28, 2020 1:46:07 PM  
**Attachments:** [image003.png](#)  
[10.28.20 CTIA Comments on CCPA Modified Regulations.pdf](#)

---

Hello,

Attached are CTIA's comments in response to the proposed modifications.

Please let me know if you have any questions.

Thank you,

Melanie Tiano



Melanie K. Tiano  
Director, Cybersecurity and Privacy  
1400 16<sup>th</sup> 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](http://www.ctia.org)

October 28, 2020

## TABLE OF CONTENTS

INTRODUCTION .....	1
I.     § 999.306 – Notice of Right to Opt-Out of Sale of Personal Information.....	2
a.     The Department should clarify that the requirement for businesses to provide offline opt-out notices applies only where the information collected offline will be “sold” within the meaning of the CCPA.....	2
II.    § 999.326 – Authorized Agent.....	4
a.     The regulations should allow businesses to require that authorized agents verify their own identities. ....	4
b.     The Department should clarify that the modified regulations permit businesses to require consumers to both verify their own identity and directly confirm that they have provided the authorized agent with permission. ....	5

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”) Third Set of Modified Proposed Regulations (“modified regulations”) to implement the California Consumer Protection Act of 2018 (“CCPA” or “Act”).<sup>1</sup> CTIA recognizes the immense undertaking involved in drafting these regulations and commends the Department’s ongoing efforts to revise and clarify the final regulations.

Nevertheless, CTIA remains concerned about some of the provisions included in the modified regulations, particularly where certain aspects of the modified regulations remain unclear.

CTIA’s concerns pertain to the following sections:

- § 999.306 – Notice of Right to Opt-Out of Sale of Personal Information; and
- § 999.326 – Authorized Agents

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

---

<sup>1</sup> See generally Cal. Civ. Code § 1798.100 *et seq.*

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

- a. The Department should clarify that the requirement for businesses to provide offline opt-out notices applies only where the information collected offline will be “sold” within the meaning of the CCPA.<sup>2</sup>**

Under the modified regulations at subdivision § 999.306(b)(3), any “business that collects personal information in the course of interacting with consumers offline” would be required to provide an offline opt-out notice to consumers. As written, this could be interpreted as requiring a business to provide an offline opt-out notice even where the business never “sells” the personal information it collects offline. Under this interpretation, this provision would have the unintended effect of misleading consumers into believing that their offline-collected personal information is “sold” when it is not, and further that consumers might stop these nonexistent data sales by exercising their CCPA opt-out rights.

For example, consider a major online and brick-and-mortar retail store that sells only the personal information it collects in connection with its online e-Commerce platform. As drafted, the modified regulations could be interpreted as requiring this business to provide an offline opt-out notice to consumers engaging in transactions at the store’s brick-and-mortar locations, provided that the business collects any personal information offline (e.g., loyalty account or payment card information) -- even when that information is not sold. Under this scenario, many offline consumers would reasonably, but mistakenly, believe that their offline-collected loyalty or payment card information will be sold unless they exercise their CCPA opt-out rights.

This interpretation is problematic for several reasons. If a retailer does not sell personal information it obtains offline, there is no need to provide an opt-out notice to the consumer. It is

---

<sup>2</sup> Cal. Civ. Code 1798.140(t)(1) (stating that “‘sell,’ ‘selling,’ ‘sale,’ or ‘sold,’ means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration”).

confusing and misleading to notify the consumer of her right to grant or withhold consent to a transaction -- the sale of information -- that will never take place regardless of her election. CTIA understands that one of the Department's goals in issuing the regulations was to "promote greater transparency to the public regarding how businesses collect, use, and share personal information" and to "make it easier for consumers to exercise their rights."<sup>3</sup> However, as described above, the suggested interpretation serves to obstruct both of these aims. Rather than promoting greater transparency, compliance with this provision would mislead consumers and add unnecessary confusion to the CCPA framework (i.e., consumers would frequently be confronted with offline opt-out notices which counterintuitively pertain only to personal information collected online). Moreover, rather than making it easier for consumers to meaningfully exercise their CCPA rights, it would make it harder for consumers to determine when to exercise those rights and to what information such an opt-out would apply.

CTIA therefore requests that the following clarifying language be inserted into subdivision 999.306(b)(3):

**§ 999.306(b)(3).** *A business that collects personal information in the course of interacting with consumers offline and sells such information shall also provide notice by an offline method that facilitates consumers' awareness of their right to opt-out. Illustrative examples follow:*

*a. A business that collects personal information from consumers in a brick-and-mortar store and sells such information may provide notice by printing the notice on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the notice can be found online.*

---

<sup>3</sup> 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-fsor.pdf>.

*b. A business that collects personal information over the phone and sells such information may provide the notice orally during the call where the information is collected.*

## **II. § 999.326 – Authorized Agent**

### **a. The regulations should allow businesses to require that authorized agents verify their own identities.**

The current and modified regulations recognize the importance of verifying the identity of consumers making CCPA requests, however, they fail to recognize that verifying the identity of a purported authorized agent is equally important.<sup>4</sup> While CTIA appreciates the Department’s recognition in subdivision § 999.326, that to better protect against fraudulent requests related to consumers’ personal information, businesses must be empowered to require agents to directly “provide proof that the consumer gave the agent signed permission to submit the request,” neither the regulations nor the proposed modifications expressly permit businesses to require that an authorized agent verify their own identity, which is an obvious hole in businesses’ ability to guard against fraudulent requests.<sup>5</sup>

Given the relatively short time that the CCPA framework has been in place, it is unclear precisely how malicious actors will try to leverage requests to exploit consumers, but one likely possibility would be through fraudulent authorized agent requests. Accordingly, the CCPA regulations should grant businesses the flexibility to implement anti-fraud measures amid a rapidly changing cybersecurity landscape. One pillar of fraud protection would involve the vetting of authorized agents to confirm that, when a consumer legitimately exercises a CCPA request via an

---

<sup>4</sup> CTIA also reiterates the concerns expressed in its March 27, 2020 comment that the powers of attorney exception in § 999.326(b) poses an unacceptable degree of risk to consumers. § 999.326(b) prevents businesses from deploying antifraud measures when presented with a document which many businesses will be unable to effectively verify.

<sup>5</sup> For example, consider a consumer who has provided her authorized agent, “Agent A”, with authority to make a request on her behalf. Under the modified regulations, a business would be able to verify that, the consumer did in fact provide Agent A with such authorization, but would not be able to verify that the individual purporting to be Agent A, is actually Agent A.

authorized agent, the “agent” itself is, in fact, the authorized party to whom the consumer granted permission to make the request.

Failure to permit businesses to require agents to verify their own identity could result in fraud whereby fraudsters pose as authorized agents to gain access to consumers’ personal information. This is particularly dangerous within the context of requests to know, where fraudsters may seek to exercise CCPA requests in order to acquire sensitive information about consumers for malicious purposes, such as stalking or extortion.

CTIA therefore requests the following language be inserted into § 999.326(a):

**§ 999.326(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 verify their own identity and/or provide proof that the consumer gave the agent signed permission to submit the request.*

- b. The Department should clarify that the modified regulations permit businesses to require consumers to both verify their own identity and directly confirm that they have provided the authorized agent with permission.**

Under the modified regulations, businesses are permitted to **either** (1) verify consumer’s identity, **or** (2) directly confirm with the consumer that they provided the authorized agent with permission. However, businesses are not expressly permitted to do both. Nevertheless, in many contexts, businesses may need to deploy both antifraud measures concurrently in order to effectively protect consumers.

For example, if a business verifies a consumer’s identity, but is prohibited from further confirming that the consumer granted the agent permission to submit a request, the business is unable to adequately assess the validity of the agent’s request. Likewise, if a business verifies that an alleged “consumer” granted an agent permission but is prohibited from verifying that the “consumer” herself is who she says she is, the validity of such permission remains unclear.



Accordingly, businesses should be empowered to take **either or both** steps to adequately protect consumers, as determined by the context and sensitivity of the request.

For these reasons, CTIA requests the following language be inserted into § 999.326(a):

**§ 999.326(a).** . . . *The business may also require the consumer to do either or both 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*

## 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

October 28, 2020

**From:** [Monticollo, Allaire](#)  
**To:** [Privacy Regulations](#)  
**Cc:** [Signorelli, Michael A.](#)  
**Subject:** Joint Ad Trade Comments on Third Set of Proposed Modifications to Text of CCPA Regulations  
**Date:** Wednesday, October 28, 2020 1:53:54 PM  
**Attachments:** [Joint Ad Trade FINAL Comments on Third Set of Modifications to CCPA Regulations.pdf](#)

---

Dear Attorney General Becerra:

Please find attached joint comments from the following advertising trade associations on the content of the third 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, please feel free to reach out to Mike Signorelli at [REDACTED] or by phone at [REDACTED].

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](http://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.  
\*\*\*\*\*



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 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 third set of proposed modifications to the text of the California Consumer Privacy Act ("CCPA") regulations.<sup>1</sup>

As explained in more detail below, the OAG's proposed modifications: (1) unreasonably restrict consumers from receiving important information about their privacy choices, (2) prescriptively describe how businesses must provide offline notices, and (3) unfairly fail to hold authorized agents to the same consumer notice standards as businesses. 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 could stymie the flexibility businesses need to provide effective offline notices to consumers. We consequently ask the OAG to strike or modify the modifications per the below comments.

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.<sup>2</sup> 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 the sections that follow below, the draft regulations implementing the law should be updated to better enable consumers to exercise informed choices and to help businesses in their efforts to continue to provide value to California consumers while also supporting the state's economy.<sup>3</sup>

---

<sup>1</sup> See California Department of Justice, *Notice of Third Set of Proposed Modifications to Text of Regulations* (Oct. 12, 2020), located at <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-third-mod-101220.pdf?>.

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

<sup>3</sup> 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*

Our members are committed to offering consumers robust privacy protections while simultaneously providing 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 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. The most recent modifications to the CCPA regulations set forth a prescriptive interpretation of the CCPA that could limit our members' ability to support California's employment rate and its economy in these unprecedented times. 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 the economy.

## **I. The Data-Driven and Ad-Supported Online Ecosystem Benefits Consumers and Fuels Economic Growth**

The U.S. economy is fueled by the free flow of data. Throughout the past three decades of the commercial Internet, one driving force in this ecosystem has been data-driven advertising. Advertising has helped power the growth of the Internet by delivering new, innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising supports and subsidizes the content and services consumers expect and rely on, including video, news, music, and more. Data-driven advertising allows consumers to access these resources at little or no cost to them, and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the Internet's largest players.

As a result of this responsible advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem*, which was conducted for the IAB by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.<sup>4</sup> This means that the interactive marketing industry contributed \$1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6% of U.S. gross domestic product.<sup>5</sup>

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life, whether through e-commerce, education, free access to valuable content, or the ability to create their own platforms to reach millions of other Internet users. In a September 2020 survey conducted by the Digital Advertising Alliance, 93 percent of consumers stated that free content was important to the overall value of the Internet and more than 80 percent surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers must pay for most content.<sup>6</sup> The survey also found that consumers estimate the personal value of ad-supported content and services on an annual basis to be \$1,403.88, representing an increase of over \$200 in value since 2016.<sup>7</sup> Consumers are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store are used to create an enhanced and tailored

---

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.

<sup>4</sup> John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017), located at <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf>.

<sup>5</sup> *Id.*

<sup>6</sup> Digital Advertising Alliance, *SurveyMonkey Survey: Consumer Value of Ad Supported Services – 2020 Update* (Sept. 28, 2020), located at [https://digitaladvertisingalliance.org/sites/aboutads/files/DAA\\_files/Consumer-Value-Ad-Supported-Services-2020Update.pdf](https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/Consumer-Value-Ad-Supported-Services-2020Update.pdf).

<sup>7</sup> *Id.*

experience, and research demonstrates that they are generally not reluctant to participate online due to data-driven advertising and marketing practices.

Without access to ad-supported content and online services, many consumers would be unable or unwilling to participate in the digital economy. Indeed, as the Federal Trade Commission noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.<sup>8</sup> The ad-supported Internet therefore offers individuals a tremendous resource of open access to information and online services. Without the advertising industry's support, the availability of free and low-cost vital online information repositories and services would be diminished. We provide the following comments in the spirit of preserving the ad-supported digital and offline media marketplace that has provided significant benefit to consumers while helping to design appropriate privacy safeguards to provide appropriate protections for them as well.

## **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."<sup>9</sup> 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 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. 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

---

<sup>8</sup> Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located at [https://www.ftc.gov/system/files/documents/advocacy\\_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400\\_ftc\\_comment\\_to\\_ntia\\_112018.pdf](https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf).

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

impede consumers from receiving important information about their privacy choices, such as information about the vital nature of the ad-supported Internet as described in Section I, 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 “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. . . .”<sup>10</sup> 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, and the regulation is narrowly tailored to serve that interest.<sup>11</sup> 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.

---

<sup>10</sup> *Virginia Pharmacy Board v. Virginia Citizens Consumer Council*, 425 U. S. 748, 770 (1976).

<sup>11</sup> *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).

- ***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.”<sup>12</sup> 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.”<sup>13</sup> 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.”<sup>14</sup> The proposed regulation would do exactly that. Thus, it is a content-based restriction on speech, subject to heightened scrutiny. The OAG should revise the text of the proposed 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.<sup>15</sup> 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,<sup>16</sup> 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 (and, in fact, could incentivize) some agents to give consumers misleading

<sup>12</sup> *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York*, 447 U.S. 557, 564 (1980).

<sup>13</sup> *Id.*

<sup>14</sup> *Sorrell v. IMS Health Inc.*, 564 U.S. 572, 565 (2011).

<sup>15</sup> Cal. Code Regs. tit. 11, § 999.326(a) (proposed Oct. 12, 2020).

<sup>16</sup> *Id.* at § 999.315(h)(3).

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.<sup>17</sup> 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.

The proposed modifications would require businesses that collect personal information when interacting with consumers offline to "provide notice by an offline method that facilitates consumers' awareness of their right to opt-out."<sup>18</sup> 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 brick-and-mortar store, and by reading the notice orally when personal information is collected over the phone.<sup>19</sup> 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."<sup>20</sup> 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

---

<sup>17</sup> Cal. Code Regs. tit. 11, § 999.305(a)(3)(c).

<sup>18</sup> Cal. Code Regs. tit. 11, § 999.306(b)(3) (proposed Oct. 12, 2020).

<sup>19</sup> *Id.*

<sup>20</sup> Cal. Code Regs. tit. 11, § 999.305(a)(3)(c).



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, and inflexible. 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 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

Christopher Oswald  
SVP, Government Relations  
Association of National Advertisers

David LeDuc  
Vice President, Public Policy  
Network Advertising Initiative

Lou Mastria  
Executive Director  
Digital Advertising Alliance

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

David Grimaldi  
Executive Vice President, Public Policy  
Interactive Advertising Bureau

Clark Rector  
Executive VP-Government Affairs  
American Advertising Federation

**From:** [Paul Jurcys](#)  
**To:** [Privacy Regulations](#)  
**Cc:** [Admin Prifina](#); [Markus Lampinen](#)  
**Subject:** Prifina's Comments to CCPA Regulations  
**Date:** Wednesday, October 28, 2020 3:01:39 PM  
**Attachments:** [CCPA-Prifina's comments #3.pdf](#)

---

Dear Ms. Kim,

Please find Prifina's comments.

Sincerely,

Paul

--

Paul Jurcys, LL.M. (Harvard), Ph.D.  
Co-Founder | [Prifina](#)  
1 Market St., San Francisco

**Dr. Paul Juncys and  
Markus Lampinen**

**1 Market Street  
Spear Tower, Suite 3600  
San Francisco, CA 94105  
policy@prifina.com**

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

**Prifina's Comments to the OAG's proposed Third Set of  
Modifications of the CCPA Regulations**

Dear Ms. Lisa B. Kim,

Prifina Inc. is pleased to have the opportunity to provide its responses to the text of modified CCPA Regulations. We would like to thank the Office of the Attorney General for making it possible for various interested parties to express their views on this significant piece of legislation. We admire that the office of the Attorney General has taken a firm stance to protect consumers' rights related to data privacy and ensuring that those rights are given priority in building a more fair and balanced digital market.

We hope that our comments will contribute to the improvement of the legal framework governing data privacy in California.

Sincerely yours,

Paul Juncys and Markus Lampinen

# **Prifina's Comments to the OAG's proposed Third Set of Modifications of the CCPA Regulations**

October 28, 2020

Prifina believes that data privacy is a fundamental human right and we would like to congratulate the Office of the Attorney General for all the hard work that is being done to create a legal environment for more equitable and transparent use of an individuals' personal data. At Prifina, we believe that individual consumers should not only have rights to their data held by third parties but also be able to get value from their personal data. To realize this, we are building tools that help individuals have "master copies" of their personal data, as well as tools for developers to build new types of applications that run on top of the user-held data.

Prifina generally agrees with the most recent proposals to amend the CCPA Regulations and welcomes the OAG's efforts to gather opinions from various stakeholders. In many instances, compliance with the CCPA requires balancing four sets of considerations: data and technology architecture, legal, user experience and interface and numerous issues related to user behavior and psychology. In the following paragraphs, we will provide some insights and suggestions on issues that need to be taken into consideration while improving the text of the Regulations and to facilitate effective implementation.

## **1. Providing Notices to Opt-Out of Sales of Data (S. 999.306(b)(3))**

Providing notices about the possibility of a consumer to opt-out from sales of personal data often depends on the actual circumstances when the data is collected from the consumer. From a practical perspective, it may be questioned what interactions with consumers could be deemed as "offline". For instance, offline interactions in most cases involve collecting data in various formats: making payments via a credit card, offering consumers the ability to check-in by filling in forms on a tablet, signing waivers or having a security camera on the premises of a business already means that data about consumers is being collected. Most businesses also have websites in which customers can be notified about their terms of use, privacy and data collection policies.

**Section 999.306(b)(3)(a).** With regard to brick and mortar businesses, such as theme parks or locations providing physical services, the notification about the opportunity to opt out from sales of personal information could be done at three different instances.

First, information about the possibility to opt-out from sales of data can be provided at the point of entry into a business by placing a notice or an icon displaying data collection practices of the business. Such a notice could be a simple set of words (e.g., “we do not collect your data”, “we do not sell your data” or “we sell your biometric data, ask our staff how to opt-out”, etc.). It is quite possible that businesses could start using certain visual icons to communicate with the consumer about the data collection practices at a given location. At the moment when this comment is submitted, there are no uniform privacy icons to visualize businesses’ data collection and usage practices and communicate them clearly to consumers. However, some businesses as well as researchers have been working on different initiatives to develop icons for data disclosures.<sup>1</sup>

In this regard, the OAG may consider what possible steps it should take to facilitate the creation of icons for data collection and data use and how to ascertain that those data disclosures are easily understandable from an average consumer perspective. The OAG may consider collaborating with businesses and researchers. The OAG may also create a more formal study group consisting of representatives of businesses, academics, researchers, legal experts and designers to develop examples of icons that can be used to communicate consumer options with regard to their personal data. Such icons for data disclosures could be a powerful tool in promoting consumer data literacy both in brick-and-mortar as well as online interactions.

The second instance where notices about the right to opt-out from the sales of data occurs is at the time when the individual consumer has either to sign a waiver (before entering a facility) or making a payment. Again, notifications about the right to opt-out can be made by placing a data disclosure icon, displaying a text message (with or without accompanying instructions), placing a bar code which would lead the consumer who scans the code with her hand-held device to the website where the procedure for opt-out can be completed or by simply checking the box that could mark consumers’ preference to opt-out from the sales of data.

Third, notices about opting out from the sales of data could also be made after visiting brick-and-mortar facility. Provided that the business has the consumer’s contact information (physical address, email address or cell phone number), the business could send instructions on how to opt-out from the sales of data. Similar practices are currently employed by various institutions that offer financial services. Consumers are periodically (usually at the beginning of the year) sent notices about the possibility of opting out of sales of their data.

---

<sup>1</sup> See e.g., Paulius Juncys “Privacy Icons and Legal Design”, available at: <https://towardsdatascience.com/privacy-icons-4ca999a6f2db>, and Zohar Efroni, Jakob Metzger, Lena Mischau, and Marie Schirmbeck, “Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing” (2019) EDPL Vol. 5, p. 352, available at: <https://edpl.lexxion.eu/article/EDPL/2019/3/9>.

From the consumer's point of view, however, the notices about data collection practices and the right to opt-out could become quite disturbing. As a matter of fact, nowadays security camera icons are displayed in almost every shop or venue. Time will show whether the customers' experience and emotions will be affected by notices that their data is being collected, shared with third parties and that they have the right to opt-out. Furthermore, filling in the form before, during or after the experience might be quite time-consuming and contribute to notice fatigue. It may also be questioned whether such a communication about the right to opt-out would be effective (i.e., whether consumers will actually exercise such an option).

**Section 999.306(b)(3)(b).** Similar to brick-and-mortar situations, notifications about the right to opt-out from sales when the interaction with the consumer takes place via the phone is based on the assumption that the business already has some data (at least contact information) about the consumer. Currently, many phone calls are recorded which adds another layer of consideration about how that data is being used and exactly what notices about the right to opt-out from sales should contain. Given California already requires explicit consent of all parties before a call is recorded, a disclosure to opt-out in the same situation may be logical.

From a consumer psychology point of view, notices about the right to opt-out from sales of data are complex. Such notices to opt-out might put the consumer in an uncomfortable position because the consumer may be forced to say something she may not not be comfortable saying in a verbal conversation or that may be perceived to lessen the service she receives. Hence, the OAG might want to consider whether businesses who are collecting and selling consumer data should be required to provide the consumer with directions on how to opt-out from the sales of data after the phone call.

It appears that that Section 999.306(b)(3)(b) is incomplete and should be clarified as follows (our suggestion is highlighted in yellow):

- b. A business that collects personal information over the phone may provide the notice orally during the call what information is collected and sold, and explain to the consumers how to opt-out of sales after the call is over.**

## 2. Requests to Opt-Out (S. 999.315(h))

Prifina believes that offering illustrative examples of practices that businesses should not employ is certainly helpful. Generally speaking, while examples provided in Section 999.315(h) are relevant today, one might wonder if the illustrative list would still be meaningful tomorrow?

Accordingly, it would be reasonable for the OAG to follow the emerging CCPA compliance practices and regularly update the prohibited practices that hinder the consumers' opportunity to opt-out from sales of data.

More specifically, Prifina has noticed that businesses tend to require consumers to provide additional information which is justified by the need to verify the identity of the requestor. We have noticed that in some instances, the verification process ends-up being quite time-consuming and involves multiple steps. This proves to be quite a cumbersome experience for consumers. In practical terms, businesses need to find more efficient ways to structure their data and establish record-keeping practices. To facilitate this, the OAG could provide some non-binding guidelines and recommendations to help businesses transition to more efficient data practices.

### 3. Authorized Agents (S. 999.326(a))

Prifina welcomes the proposed modifications to Section 999.326(a) because they should contribute to making consumer interactions with businesses via authorized agents more smooth. It should be recalled that one of the main incentives for consumers to employ authorized agents is the willingness to reduce the burden and hassle related to dealing with third parties that process consumer's personal information. In practice, balancing security, fraud prevention, transparency and efficiency of communication can be quite challenging. Therefore, the deletion of the possibility for businesses to require authorized agents to provide written permission of the consumer is definitely a positive step forward. The regulator should seek to create an environment where consumer interactions via an authorized agent are frictionless.

Nevertheless, the current version Section 999.326(a) leaves an ample spectrum of possibilities for businesses to delay the fulfillment of requests submitted via an authorized agent, by adding an additional verification step. The possibility which businesses now have to ask the consumer to verify the consumer's identity or confirm that they have authorized the agent to act on their behalf opens the gate for double verification. This could have quite an adverse effect on consumers because the whole point of using authorized agents is to streamline the opt-out process and avoid multiple verifications that are employed by businesses on a case-by-case basis.

More particularly, the consumer's "signed permission to submit request", in principle, should be deemed sufficient unless there are some reasonable grounds to believe otherwise. One possible solution to resolve such an information asymmetry is to create an industry-wide template of a signed permission which should be deemed sufficient for the business to comply



with the request submitted via an authorized agent. This **signed permission template** could be prepared by the OAG (which could then cooperate with industry and consumer representatives). This would help find balance between different regulatory objectives, save time, cost, and would reduce information asymmetries between all parties involved.

In situations where a consumer interacts with businesses via an authorized agent, it is desirable that businesses have a **designated point of contact** with whom authorized agents should be able to interact with. This would facilitate the interaction between the authorized agent and businesses.

Finally, if the AOG decides to keep the proposed structure of Section 999.326(a), we would like to suggest narrowing down the scope of subsections (1) and (2) by adding an additional qualifier which would allow businesses to contact the consumer in cases where the authorized agent has not provided **reasonable proof** of the existence of the signed mandate.

#### 4. The Wording of S. 999.332(a)

We recommend deleting “and” and keeping the text of Section 999.332(a) as following:

**§ 999.332. Notices to Consumers Under 16 Years of Age.**

- (a) A business subject to sections 999.330 ~~and~~<sup>or</sup> 999.331 shall include a description of the processes set forth in those sections in its privacy policy.

**From:** [Courtney Jensen](#)  
**To:** [Privacy Regulations](#)  
**Subject:** TechNet Comment Letter Regarding Third Set of Proposed Modifications to CCPA Regulations  
**Date:** Wednesday, October 28, 2020 3:20:03 PM  
**Attachments:** [TechNet CCPA Regulation Letter 10.28.20.pdf](#)

---

Good Afternoon,

Attached please find TechNet's written comments regarding the third set of proposed modifications to CCPA regulations.

Please do not hesitate to reach out with any questions.

Thank you,  
Courtney

Courtney Jensen  
Executive Director | California and the Southwest  
TechNet | The Voice of the Innovation Economy





**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](http://www.technet.org) | @TechNetUpdate

October 28, 2020

The Honorable Xavier Becerra  
ATTN: Privacy Regulations Coordinator  
300 S. Spring Street  
Los Angeles, CA 90013

Dear Mr. Attorney General Becerra,

TechNet appreciates the opportunity to submit written comments regarding the third 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; 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.

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

- For opt-out notices in an offline setting such as a retail store, TechNet believes that such a notice should only be required if information collected in that offline setting or from an offline transaction is sold, consistent with the rest of CCPA.

**§ 999.315 Requests to Opt-Out.**

- TechNet has concerns with h(3) and h(4) as outlined in the modified regulations and the vagueness, lack of detail and compelled speech these sections present.

- (h)(3) states *"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 optout before confirming their request."* This illustrative examples ties the hands of companies to provide additional information to their consumers. Companies would not be able to provide more disclosures or information that could explain to consumer the implications of their decisions. This does not further the intent of the CCPA which is to promote consumer transparency and information. For example, during an opt out process a business may include information that explains what a data sale is and the impact of opting out. This would not be allowed under (h)(3). We believe providing this information stays true to the spirit of CCPA and simply educates consumers. We believe (h)(3) is especially unnecessary with the inclusion of (h)(1) which ensures ease for consumers. Businesses should be able to explain the impacts and/or drawbacks of opting out, since many consumers may not understand what it means.
- (h)(4) states *"The business's process for submitting a request to opt-out shall not require the consumer to provide personal information that is not necessary to implement the request."* We are concerned with the vagueness and lack of detail given for the new illustrated example. If this new example is to be added, then businesses need more guidance as to what personal information is actually needed versus what is not needed to avoid confusion for both businesses and California resident "consumers."

### **Conclusion**

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 Courtney Jensen, Executive Director, at [REDACTED] or [REDACTED].

Thank you,  
Courtney Jensen  
Executive Director, California and the Southwest  
TechNet

**From:** [Dylan Hoffman](#)  
**To:** [Privacy Regulations](#)  
**Subject:** Internet Association Comments on Third Modified CCPA Regulations  
**Date:** Wednesday, October 28, 2020 3:53:05 PM  
**Attachments:** [IA Comments on Proposed Modified Regulations to CCPA 10.28.20 \(1\).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



Check out [Internet Association's job site](#) with hundreds of internet industry positions now open!



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  
Email: [PrivacyRegulations@doj.ca.gov](mailto: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.<sup>1</sup> 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.<sup>2</sup> 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 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

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 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.

### 999.315 (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

---

<sup>1</sup> IA’s full list of members is available at: <https://internetassociation.org/our-members/>.

<sup>2</sup> 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](https://internetassociation.org/files/ia_privacy-principles-for-a-modern-national-regulatory-framework_fulldoc) / (last accessed November 25, 2019).



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~~is~~ 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~~is~~ 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~~The 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~~Upon~~ 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:** [Jen King](#)  
**To:** [Privacy Regulations](#)  
**Cc:** [Adriana Stephan](#)  
**Subject:** Re: CCPA comments for 10/29/20 rulemaking  
**Date:** Monday, November 2, 2020 11:20:43 AM  
**Attachments:** [CCPA comments October 28 2020 corrected.pdf](#)

---

Greetings,

I realized after submitting our comments last week that the version I sent in was missing our footnotes. Attached is an updated version (the only changes are the inclusion of footnotes that should have been in the submitted copy!). Please let me know if you are able to replace our existing submission with this one.

Sincerely,  
Jen King

Jennifer King, Ph.D (she/her)  
Director of Consumer Privacy  
Center for Internet and Society  
Stanford Law School



<https://cyberlaw.stanford.edu/about/people/jen-king>

[www.jenking.net/publications](http://www.jenking.net/publications)

Google Scholar profile: <https://scholar.google.com/citations?user=O5jENBMAAAAJ&hl=en>

On Oct 28, 2020, at 4:02 PM, Privacy Regulations  
<[PrivacyRegulations@doj.ca.gov](mailto:PrivacyRegulations@doj.ca.gov)> wrote:

Thank you for submitting a public comment on the CCPA proposed regulations. Your email has been received.

Sincerely,  
California Department of Justice

**From:** Jennifer King [REDACTED]  
**Sent:** Wednesday, October 28, 2020 3:55 PM  
**To:** Privacy Regulations <[PrivacyRegulations@doj.ca.gov](mailto:PrivacyRegulations@doj.ca.gov)>  
**Cc:** Adriana Stephan [REDACTED]  
**Subject:** CCPA comments for 10/29/20 rulemaking

Dear Ms. Kim,

Attached please find our comments regarding the

latest revisions to the CCPA.

Best,  
Jen King

**Jennifer King, Ph.D**

*Director of Consumer Privacy - Center for Internet and Society*

**Stanford Law School**



<https://cyberlaw.stanford.edu/about/people/jen-king>

[www.jenking.net/publications](http://www.jenking.net/publications)

Google Scholar profile: <https://scholar.google.com/citations?user=O5jENBMAAAAJ&hl=en>

CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.

October 28, 2020

To Whom It May Concern:

We are pleased to submit comments to the California Attorney General's office regarding the Third Set of Proposed Modifications to CCPA Regulations released on October 12, 2020. We make these comments on behalf of ourselves individually and provide our institutional affiliation for identification purposes only.

In sum, we are heartened by the OAG's decision to further clarify §999.315 - Requests to Opt-Out. From our own experience conducting empirical research on the implementation of "Do Not Sell My Personal Information" links across a variety of websites, we observed a wide discrepancy in how individual companies have implemented this process. We found evidence of so-called "dark patterns"—as defined in Proposition 24, "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice." Whether intentionally designed to thwart Californians' exercise of their Do Not Sell right, or as a result of poor design choices, the end result is the same: unfair barriers to completing these requests. While these design choices may negatively impact all California consumers, they may have disproportionate impacts on vulnerable individuals, such as the elderly, non-English speakers, and individuals with lower written literacy and technology experience.

Our research group reviewed the Do Not Sell (DNS) processes of dozens of websites across a variety of different business types, including: brick and mortar retail stores, car dealerships, theme parks, grocery stores, pharmacies, banks, and newspapers. We observed the following problems, of which we include examples in the attached appendix:

- Do Not Sell flows (the steps by which a consumer initiates a Do Not Sell request up to completion) that included unnecessary steps for making a DNS request, such as:
  - Sending consumers from the DNS link on a company's homepage to the company's privacy policy page (or other indirect routes), rather than directly to a DNS form, thus requiring consumers to hunt through the policy to find the link to the DNS form (see Appendix 1 for an example);
  - Requiring consumers to select a button or toggle embedded within a page to make a request, often without instructions or clear labels, such that it is unclear which option initiates the DNS state (see Appendix 2 for examples);
- DNS forms that asked consumers to provide personal information that appeared extraneous to the DNS request;

- Forms offered only in English by companies that likely have large non-English speaking customer bases (see Appendix 3 for an example);
- DNS landing pages and/or forms that used confusing (e.g., double negatives) or manipulative language (e.g. emotionally charged or guilt-inducing) that attempts to persuade consumers not to exercise their rights (see Appendix 4 for an example);
- DNS landing pages that included copious amounts of text preceding the form that was not directly salient to making a request. Forcing consumers to spend additional time or energy to read extraneous information may decrease the likelihood of completing a DNS request (see Appendix 5 for an example);
- For companies that honor DNS requests only via email, many of these companies provided little or no instruction to consumers about how to complete the request (e.g., what information to include in an email), did not offer automated shortcuts for composing emails (e.g., mailto functionality that can prepopulate an email with the address and subject link when clicked), and provided email addresses that appeared to be non-specific to DNS requests, which may increase the burden on the consumer to engage in continual back-and-forth with the company to make the DNS request.

Consumer Reports, which released a report on October 1st, 2020 entitled “California Consumer Protection Act: Are Consumers’ Digital Rights Protected,” also found many of the same issues we report here, as well as additional concerns.<sup>1</sup>

We are pleased to see the OAG address some of the issues above with additional clarifications to the statute in order to improve what should be a simple and straightforward process for consumers. These clarifications make it less onerous for both consumers to exercise their rights and for companies to comply with the CCPA. By reducing the gray area that forces companies to rely heavily on interpretation, the updated regulations diminish the potential for DNS processes to be designed in ways that are confusing, deceptive, or manipulative to consumers, whether deliberately or by accident.

At the same time, while the clarifications reduce company discretion in designing DNS processes, the current OAG guidelines still leave room for companies to implement DNS processes in ways that subvert consumers’ ability to exercise their rights under the statute.

We would like to see companies and/or policymakers also address the following:

1. Provide forms, rather than email addresses, for consumers to make DNS requests

DNS requests that require consumers to send an email, without outlining the information consumers must provide for the request to be fulfilled, are particularly burdensome on consumers.

2. Offer DNS forms in languages other than English, and also use simple, easy to understand language

Non-English speakers are particularly vulnerable to confusing or misleading language in DNS requests. For businesses that provide essential services and/or have a substantial non-English speaking clientele, company DNS forms should accommodate different languages (see Appendix 3 for examples of English-only privacy policies for companies with large non-English speaking customer populations).

---

<sup>1</sup> Available at: [https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR\\_CCPA-Are-Consumers-Digital-Rights-Protected\\_092020\\_vf.pdf](https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf)

### 3. Avoid crowding DNS forms with extraneous information

DNS forms are not the place for companies to produce treatises on why they think they do not sell information. And while providing references to useful background information on the CCPA may be helpful to consumers (including links to official guidance from the OAG's CCPA website), reproducing hundreds of words of text that is not required reading for exercising one's DNS rights is not helpful and discourages consumers from completing their requests.

4. Provide consumers a streamlined form that does not require them to take extraneous steps to complete a DNS request. For multiple-purpose forms (e.g. forms allowing consumers to also exercise their deletion and access rights), make the selection choices simple and clear.
5. Absent a mandate to respect Global Privacy Control signals, provide a standardized interface for consumers to exercise their DNS rights.

The CCPA presently requires companies to provide “two or more designated methods for submitting requests to opt-out.”<sup>2</sup> The vast majority of companies have elected not to adopt mechanisms such as the Global Privacy Control<sup>3</sup>, which would provide a simple and straightforward means for consumers to communicate DNS preferences with all websites they visit using a browser plug-in or setting. Unfortunately, the original requirement of the statute to develop “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” (§1798.185(4)(C)) was dropped during the review period. While we filed comments in February 2020 urging that the Attorney General (OAG) not adopt the version of the button proposed at that time, we did support the OAG following the advice of the CMU report to create a standardized control.<sup>4</sup> Unfortunately, our research demonstrates that absent a standardized control mechanism, companies are using inconsistent and in some cases, unclear and misleading methods to allow consumers to exercise their DNS rights. Further, executing DNS requests for even a single website requires consumers to repeat these steps using every browser on every device (including mobile devices) they have used to access the website in order to fully ensure that a single company honors their DNS preference. This is, on a practical level, unworkable for consumers, and illustrates the unreasonable burden consumers must shoulder to exercise their CCPA rights.

Accordingly, we urge California policymakers to mandate the adoption of the Global Privacy Control standard. In the CCPA, §999.315(c) mandates that businesses treat “user-enabled global privacy controls, such as browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request.” The current “process” for making DNS requests on websites where cookies, rather than a user account, are the basis by which consumers are tracked is, as we note above, is highly complicated and likely deeply confusing for most consumers (Please see Appendix 6 for examples.) As the attached examples demonstrate, consumers are expected to either submit opt-out requests on each browser and device they use to visit a company's website, or are asked to allow the site to place a cookie in order to provide a DNS signal (which becomes obsolete if a consumer elects to clear her browser cookies).

The Global Privacy Control could provide consumers with a delegated means of seamlessly providing DNS requests to companies without having to engage in the burden of making independent DNS requests for each

<sup>2</sup> §999.315(a)

<sup>3</sup> <https://globalprivacycontrol.org/>

<sup>4</sup> [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\* \(February 4, 2020\).](#)

website they visit and on each browser and device they use. However, as we note above, businesses can refuse to honor a consumer's privacy-specific preferences if the preferences were set in the software, such as the legacy "Do Not Track" option in web browsers. As of right now, California law dictates that companies must disclose whether they respond to "Do Not Track" requests, ultimately giving them the discretion as to whether or not to honor these requests from consumers.

In closing, while we believe the §999.315 clarifications are a positive development for consumers hoping to exercise their rights under the CCPA, there are still several measures companies should take to ensure that they are not actively undermining DNS processes, particularly for vulnerable populations.

Sincerely,

Jennifer King, Ph.D  
Director of Consumer Privacy  
Center for Internet and Society, Stanford Law School

Adriana Stephan  
M.A. Student  
Cyber Policy, Stanford University

Emilia Porubcin and Claudia Bobadilla  
Undergraduate Students, Stanford University

Morgan Livingston  
Undergraduate Student, University of California, Berkeley



## Appendix 1: 3M Company ([https://www.3m.com/3M/en\\_US/company-us/privacy-policy/](https://www.3m.com/3M/en_US/company-us/privacy-policy/)), visited 10/26/20

Please note that there is no “Do Not Sell” link from the homepage; this page is accessed via the privacy policy link in the footer. Due to the length of this page we have cut it into smaller sections in order to fit it all one printed page. The link in the red circle is the link to the DNS form.

3M Global Privacy Policy

3M is committed to protecting your privacy. This privacy policy describes how we collect, use, and share your information, and how you can control your privacy settings. It applies to all 3M products and services, including our website, mobile applications, and email newsletters. For more information, please visit our website or contact us at 1-800-333-3333.

[View our privacy policy](#)

### Additional Information for California Residents

California residents have certain rights regarding their personal information. This section describes those rights and how to exercise them.

**Right to Know:** You have the right to know what personal information we have collected about you, and how we use it. You can request this information by contacting us at 1-800-333-3333.

**Right to Delete:** You have the right to delete your personal information from our systems. You can request this by contacting us at 1-800-333-3333.

**Right to Opt-Out:** You have the right to opt-out of the sale of your personal information. You can do this by clicking on the “Do Not Sell My Information” link in our website footer.

**Right to Access:** You have the right to access your personal information. You can request this by contacting us at 1-800-333-3333.

**Right to Correction:** You have the right to correct your personal information. You can request this by contacting us at 1-800-333-3333.

**Right to Portability:** You have the right to port your personal information to another system. You can request this by contacting us at 1-800-333-3333.

**Right to Restriction:** You have the right to restrict our use of your personal information. You can request this by contacting us at 1-800-333-3333.

**Right to Non-Discrimination:** You have the right to non-discrimination. We will not discriminate against you for exercising your rights.

**Right to a Fair and Transparent Process:** We will provide you with a fair and transparent process for exercising your rights.

**Right to a Timely Response:** We will respond to your request within 30 days.

**Right to a Free Response:** We will not charge you a fee for exercising your rights.

**Right to a Confidential Response:** We will keep your request confidential.

**Right to a Secure Response:** We will protect your information from unauthorized access.

**Right to a Responsible Response:** We will handle your request in a responsible manner.

**Right to a Compliant Response:** We will ensure our response complies with the law.

**Right to a Satisfying Response:** We will strive to satisfy your request.

**Right to a Fair Response:** We will provide a fair response to your request.

**Right to a Transparent Response:** We will be transparent about our response.

**Right to a Timely Response:** We will respond to your request within 30 days.

**Right to a Free Response:** We will not charge you a fee for exercising your rights.

**Right to a Confidential Response:** We will keep your request confidential.

**Right to a Secure Response:** We will protect your information from unauthorized access.

**Right to a Responsible Response:** We will handle your request in a responsible manner.

**Right to a Compliant Response:** We will ensure our response complies with the law.

**Right to a Satisfying Response:** We will strive to satisfy your request.

**Right to a Fair Response:** We will provide a fair response to your request.

**Right to a Transparent Response:** We will be transparent about our response.

## Appendix 2: Examples of unclear or confusing DNS toggles or buttons

These examples illustrate how companies are using a specific form of interaction design (toggle switches) that neither clearly communicates to consumers what toggling the switch will accomplish, nor whether they have successfully opted out or not. The LA Times (Example 1) is slightly clearer than Examples 2 and 3 given that the switch is grey when arriving at the page (indicating “off”), and when clicked turns green (indicating “on”), as well as providing a “Save” button to confirm the selection. Even so, there are no instructions to follow nor text indicating the switch state. Example 2 offers consumers the choice to “agree” or “disagree”, but with what exactly is unclear (are you agreeing to opt-out? Or not?). Example 3 provides no instruction of what will occur when the toggle is switched; the consumer must deduce that the existing state (blue, presumably “on”) means that one’s data is being sold to third parties, and that toggling it to grey (“off”) will stop the sale.

### Example 1: Los Angeles Times (visited 10/26/20)

#### Opt-Out Tools

To unsubscribe from Los Angeles Times marketing messages, you can adjust your settings here:  
<https://membership.latimes.com/settings>.

If you are a California resident, to opt out of the sale of your personal information (and as a result, opt out of personalized advertising), **you must utilize the following toggle (and all 3 tools below).**

#### Do Not Sell My Info



Save

If you are logged into your Los Angeles Times account, this setting will save your opt out preference to your profile (otherwise your preference will be stored in a browser cookie). Please see the [full disclosure](#) below.


**You must utilize each of the following 3 tools (in addition to the toggle above) to ensure that you are opted out as much as technically possible across the open web.**


1. DAA: <http://optout.aboutads.info/>  
 This tool, created by the Digital Advertising Alliance, will generate a list of participating vendors who are currently collecting data from you for the purposes of targeted advertising. You will be able to see each vendor and must then affirmatively opt out of any or all of their databases.
2. NAI: <http://optout.networkadvertising.org/>  
 This tool, created by the Network Advertising Initiative, will also generate a list of participating vendors who are currently collecting data from you for the purposes of targeted advertising. You will be able to see each vendor and must then affirmatively opt out of any or all of their databases.
3. LiveIntent: <http://d.liadm.com/opt-out>  
 This tool is specific to LiveIntent, which is a vendor we utilize for advertising within our newsletters.

Full disclosure: For many of these tools, your opt-out preferences may be stored in cookies. If your browser blocks cookies, your opt-out preferences may not be effective. If you delete cookies, you may also be deleting your opt-out preferences, so you should visit these pages periodically to review your preferences or to update your choices. The above opt-out mechanisms are browser based and device specific; thus, you must opt-out on each device and on each browser to exercise your rights. The Los Angeles Times does not maintain or control the opt-out mechanisms listed in items 1-3 above and is not responsible for their operation.



**Example 2: Huffington Post/Verizon Media (visited 10/27/20)**





### Continue Sharing under California Law

Verizon Media does not sell information that identifies you on its own, like your name or email address. As outlined in our Privacy Policy, we do share other identifiers with partners for product, service and advertising reasons. Sharing this information enables us to provide our content and services by helping our partners deliver better, more relevant content and advertising and by keeping our services supported by our advertising partners. Under the California Consumer Privacy Act some of this sharing activity may be considered a “sale” that you have a right to opt out of. If you opt out we will stop sharing your data as described above when that activity is selling as defined in the CCPA. As a result, some of our services and content may be impacted or become less relevant or interesting to you. [Learn More](#)

Disagree

☒

Agree

**Example 3: CNN.Com/Warner Media (visited 10/27/20)****WarnerMedia**

✕

**Do Not Sell My Personal Information**

For California Residents Only

Pursuant to the California Consumer Privacy Act (CCPA)

The WarnerMedia family of brands uses data collected from this site to improve and analyze its functionality and to tailor products, services, ads, and offers to your interests. Occasionally, we do this with help from third parties using cookies and tracking technologies.

We respect your right to privacy, and we have built tools to allow you to control sharing of your data with third parties. You can choose to disable some types of cookies and opt to stop sharing your information with third parties, unless it is necessary to the functioning of the website. Click on the different category headings to find out more and to opt-out of this type of data sharing. Note that any choice you make here will only affect this website on this browser and device.

To learn more about how your data is shared and for more options, including ways to opt-out across other WarnerMedia properties, please visit the [Privacy Center](#).

**Manage Consent Preferences****Share my Data with 3rd Parties**

For California Residents Only

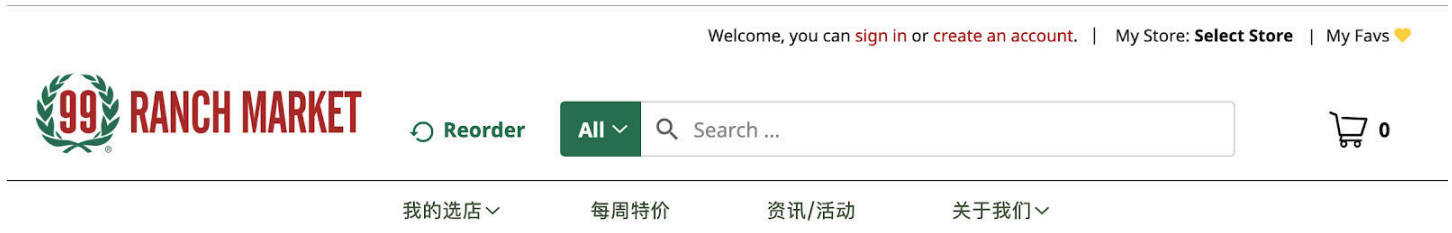
Pursuant to the California Consumer Privacy Act (CCPA)

Some of your data collected from this site is used to help create better, more personalized products and services and to send ads and offers tailored to your interests. Occasionally this is done with help from third parties. We understand if you'd rather us not share your information and respect your right to disable this sharing of your data with third parties for this browser, device, and property. If you turn this off, you will not receive personalized ads, but you will still receive ads. Note that any choice you make here will only affect this website on this browser and device.

## Appendix 3: Examples of English-only privacy policies for companies with large non-English speaking customer populations

### 99 Ranch Market (<https://www.99ranch.com/zh-hans/privacy-policy>), visited 10/26/20

Please note this site does not have a Do Not Sell link on the homepage; this page is accessed via the Privacy Policy link (also only in English), though the site offers an option to set the language to Chinese (simplified or traditional). In this example, the language was set to Chinese (simplified). Please note: this screenshot includes only the top portion of the webpage



### Privacy Policy

Tawa Supermarket, Inc. and our affiliates are committed to protecting your privacy. We recognize that privacy is an important issues for our customers and employees and we want to be transparent about how we collect, use, and disclose your personal information—this Privacy Notice provides you with notice of our processing activities and your rights under the law. Personal Information generally means any information that identifies you as an individual person, along with other information we associate with it. This includes information that is maintained by us in a manner that identifies you or your household. Personal information does not include publicly available information or information that is de-identified or aggregate consumer information.

By using any of our websites and mobile applications in the United States (collectively, "Sites") or otherwise providing Personal Information to us, you agree to this Privacy Policy. This Privacy Notice is intended for individuals in the United States who are over the age of 16. If you live outside of the United States and choose to use the Sites connected with this Privacy Notice, you do so at your own risk and understand that your information will be sent to and stored in the United States.

#### Application

This Privacy Notice applies to Tawa Supermarket, Inc., Tawa Inc. (Retail), Tawa Services, Inc., Welcome Market, Inc., Welcome California Market, Inc., and Welcome Services, Inc.

## Appendix 4: Examples of websites using “guilt-shaming” or other coercive language in their DNS requests.

### Example 1: BuzzFeed.com (visited 10.27/20)

Please note the text on the opt-out button: “this action will make it harder to us [sic] to tailor content for you.”

#### BuzzFeed - Do Not Sell My Personal Information

We, and our partners, use technologies to process personal information, including IP addresses, pseudonymous identifiers associated with cookies, and in some cases mobile ad IDs. This information is processed to personalize content based on your interests, run and optimize marketing campaigns, measure the performance of ads and content, and derive insights about the audiences who engage with ads and content. This data is an integral part of how we operate our site, make revenue to support our staff, and generate relevant content for our audience. You can learn more about our data collection and use practices in our Privacy Policy.

If you wish to request that your personal information is not shared with third parties, please click on the below checkbox and confirm your selection. Please note that after your opt out request is processed, we may still collect your information in order to operate our site.



I want to make a 'Do Not Sell My Personal Information' request. Note: this action will make it harder to us to tailor content for you.

CONFIRM

[Data Deletion](#)

[Data Access](#)

[Privacy Policy](#)

## Example 2: Forever 21 (<https://www.forever21.com/us/shop/info/optout>), visited 10/27/20

Please note the language in this notice that attempts to minimize the effects of cookie tracking (“data contained in these Cookies does not typically identify you,” warns the consumer that avoiding tailored ads “may not be what you want,” and informs consumers that even after they exercise their rights, “we will still continue to share data with our service providers.” Finally, the company uses this notice to argue with the definition of the term “sale” in the CCPA, attempting to delegitimize the regulation.



### Do Not Sell My Info

The CCPA gives California consumers the right to opt-out of the sale of their personal information (“PI”).

The only way you can exercise this right as it relates to the use of cookies and other tracking technologies, is to click on the Do Not Sell My Information Toggle below from each browser and device you use.

However, before you click on the Do Not Sell My Information Toggle below, we hope that you will consider a few more things:

- First, remember that the data contained in these Cookies does not typically identify you by name or other directly identifiable means.
- Second, opting-out of sales of your PI in the digital advertising context (i.e. by means of Cookies) will not stop you from getting ads, but these ads will not be tailored to your interests. This may not be what you want.
- Third, if you opt-out, your experience on our Sites and when you otherwise engage with us will be much less personalized.
- Fourth, even after you opt-out, we will still continue to share data with our service providers who use the data on our behalf.

The CCPA defines “sale” in an unusual way, and with no guidance yet from the State of California as to how broadly the term should be interpreted, a number of differing reasonable interpretations are possible.

Some may argue that when certain third parties place Cookies on the consumer’s device when the consumer engages with our site or app, the PI collected by such Cookies constitutes a “sale” under the CCPA. We do not agree with this interpretation. However, pending a consensus as to what “sale” actually means under the CCPA, we are providing a way for California consumers to opt-out of future Cookie-based “sales” of their PI, by (i) enabling the Google Restricted Processing solution into our use of certain Google products, (ii) using the IAB Tech Lab “do not sell” signal with third parties that we work with and that are participating in the IAB CCPA Compliance Framework, and (iii) disabling other third parties’ Cookies that are not covered by either (i) or (ii) above. The solutions referenced in (i) and (ii) each conveys to the recipient that PI can only be used for restricted purposes, such as providing us services, and cannot be sold by the recipient downstream. We make no guaranty as to how third parties will treat our Do Not Sell signals.



## Appendix 5: Example of opt-out form nested beneath excessive text

Home Depot (<https://www.homedepot.com/privacy/Exercise My Rights>), visited 10/27/20

Please note: this screenshot includes only the top portion of the webpage

[Home](#) / [Exercise Privacy Rights](#)

## The Home Depot & Your Personal Information

### MOST VIEWED

Check Order Status  
Store Finder and Store Hours  
My Account Sign in  
Check Order History  
Order Cancellation  
Shipping and Delivery FAQ  
Pay Credit Card Bill  
**About My Order**  
Check Order Status  
Order Cancellation  
Confirm Order Was Placed  
Shipping and Delivery FAQ  
In-Store Pickup

### Shipping and Delivery

Free Shipping  
Shipping Options  
Buy Online and Pickup in Store  
Buy Online and Ship to Store  
Check Order Status  
Shipping and Delivery FAQs

### Product and Services

Product Availability  
Protection Plans  
Installation Services  
Tools and Truck Rental  
Moving Services  
Pro Services  
How To and Project Guides

Ratings and Reviews  
Seeds Program

### Pricing and Promos

Price Match Policy  
Savings Center  
LocalAd  
Special Buy of the Day  
Credit Center  
Credit Offers  
Rebate Center

### Payments

Payment Methods  
Gift Cards and Store Credits  
Tax Exemptions  
Credit Card Bill Payments

### My Account

Order History  
In-Store eReceipts  
Email/phone Opt-in/out  
Credit Card Payments

### Returns and Recalls

Online Purchase Return Policy  
In-Store Purchase Return Policy  
Recalls

### Policies and Legal

Terms of Use  
Exercise My Privacy Rights  
Privacy and Security Statement  
Manage My Marketing Preferences  
California Rights and Regulations  
Electronics Recycling Programs  
The Home Depot Reviewer Program

### Corporate Information

Careers  
Corporate Information  
Home Depot Foundation  
Government Customers  
Investor Relations  
Suppliers and Providers

The Home Depot values and respects your privacy. Some of the ways we use the information we collect include:



#### CONVENIENCE

To provide you with the best shopping experience through services like eReceipts, home delivery, and in-store pickup.



#### CONSISTENCY

To provide the same customer service experience when you engage with us in our stores, online, or over the phone.



#### COMMUNICATION

To provide the same customer service experience when you engage with us in our stores, online, or over the phone.



#### AWARENESS

To make you aware of the products and services we offer to support your home improvement needs.

You can learn more about how The Home Depot uses the personal information we collect in our [Privacy and Security Statement](#).

## Exercise Your Privacy Rights

Complete the form below to submit your request. When we receive your information, we'll use it to verify your identity and review your request. You can only submit one type of request at a time. Need to make more than one request? Complete a new submission form for each request.

You can:

- Request the personal information we collect about you.
- Ask that we delete the personal information we collect about you.
- Submit an Opt Out of Sale request (while we do not share your personal information with third parties in exchange for money, we disclose certain information in exchange for insights and other valuable services, and California law treats such sharing as a "sale" even if no money is exchanged; click here for more information).

#### IMPORTANT NOTE REGARDING REQUESTS TO OPT OUT OF SALES

When you visit our website, we use cookies and similar tools to automatically make certain personal information available to select third parties who are providing services to us to help us enhance your experience, improve and deliver advertising, learn how you use the website, and achieve the other purposes addressed in the "Tracking Tools We Use" section of our [Privacy and Security Statement](#). Some of those select third parties may use the personal information for their own purposes or to provide services to other businesses. California law treats such sharing as a "sale" even if no money is exchanged.

If you want to opt out of such automatic sharing, use this form to submit an Opt Out of Sale request, and we will place a cookie on your browser to automatically prevent the sharing from happening when you use that browser to visit our website. Because we use a cookie to automatically identify and register your preference, if you disable cookies on your browser or device, the Opt Out of Sale request will no longer work. You can always enable cookies on your browser or device and visit this page again to register your Opt Out of Sale request. We may not recognize you when you use other browsers or devices to visit our website. So, you will need to submit a separate Opt Out of Sale request on each device and browser you use to visit our website. For more information about our tracking tools and how to control them, please click here.

After you submit an Opt Out of Sale request, you may still see advertising regarding our products and services. And some of that advertising may be delivered by third parties or appear on third-party sites or services. This advertising may be general audience advertising or may be delivered by service providers in ways that do not involve sales of your personal information.

When you submit your Opt Out of Sale request using the form below, as indicated above, we will no longer share your information via digital tracking technologies used on homedepot.com. You may need to take other steps for other websites, as described in the privacy policies for those websites. We also will use the information you provide via the form to identify the personal information not involving online tracking technologies that we hold about you so that we can honor your request that such information no longer be sold as well.

Once you submit your request, we will place a cookie on your browser to automatically prevent the sharing from happening when you use the browser to visit our website. However, to fully register your Opt Out of Sale request for information that may be shared via channels other than online tracking technologies, if any, you will need to provide a working email address and respond to the verification request we send you.

#### Making a Request

A working email address is required to complete your request online. Call 1-800-394-1326 to speak to a representative if you don't want to provide an email address.

For each request you submit, we'll send a verification email to the email address you provided. This may take up to 72 hours. Check your spam folder if you don't see it. You'll have 3 days to verify your email before your request expires. If you don't, you'll have to submit another request.

If you are making a request on behalf of another person, please send your request to [myinfo@homedepot.com](mailto:myinfo@homedepot.com) and include the following information about you and the person on whose behalf you are making the request: full name, mailing address, email address, and phone number. You should also provide proof of your authorization to act on the other person's behalf. We will contact you for additional information once your request has been received.

After we process your request to delete your personal information or to Opt Out of Sale, you may still see advertising regarding our products and services. We may deliver advertising to a general audience or place advertising on websites, mobile applications, and connected device applications that relates to our products and services. For example, if you visit a do-it-yourself website, you may see advertising on that website that promotes our products and services related to the do-it-yourself content.

## Submit Your Privacy Request

Select Request Type

☐ Get My Information ☐ Delete My Information ☐ Opt Out of Sale

First Name

Last Name

State of Residence

Email Address

## Appendix 6: Examples of instructions for opt-outs based on cookie tracking

Please note: the BuzzFeed, Los Angeles Times, Verizon Media, and Warner Media examples used in the earlier appendices are also examples of the confusing and multi-step processes consumers must follow to ensure that their DNS requests are respected by companies relying on third party tracking mechanisms. In the examples below, consumers are instructed that they will have to replicate the process for making their requests using every browser on every device they have used to access these websites.

### Example 1: Office Depot cookie example (visited 10/22/20)

#### IMPORTANT NOTE REGARDING REQUESTS TO OPT OUT OF SALES

When you visit our website, we use cookies and similar tools to automatically make certain personal information available to select third parties who are providing services to us to help us enhance your experience, improve and deliver advertising, learn how you use the website, and achieve the other purposes addressed in the "[Tracking Tools We Use](#)" section of our [Privacy and Security Statement](#). Some of those select third parties may use the personal information for their own purposes or to provide services to other businesses. California law treats such sharing as a "sale" even if no money is exchanged.

If you want to opt out of such automatic sharing, use this form to submit an Opt Out of Sale request, and we will place a cookie on your browser to automatically prevent the sharing from happening when you use that browser to visit our website. Because we use a cookie to automatically identify and register your preference, if you disable cookies on your browser or device, the Opt Out of Sale request will no longer work. You can always enable cookies on your browser or device and visit this page again to register your Opt Out of Sale request. We may not recognize you when you use other browsers or devices to visit our website. So, you will need to submit a separate Opt Out of Sale request on each device and browser you use to visit our website. For more information about our tracking tools and how to control them, please [click here](#).

### Example 2: Walmart cookie example (visited 10/22/20)

We respect the privacy of your personal information. The information you provide here will only be used to process your opt out of sale request. To assure the implementation of your request across all devices associated with your account, you should login to your account with each of your devices. If you are not logged in or do not provide accurate account details, you should complete an opt out of sale request on each browser or device that you use to access our websites and mobile services. In addition, if you are not logged into your account while making your request, and you later clear your Walmart cookies, your opt out of sale request will need to be resubmitted. Please note that your request will apply to future sales of your personal information and will not impact sales made prior to your request.

**From:** [Rachel Nemeth](#)  
**To:** [Privacy Regulations](#)  
**Subject:** CTA Letter on Third Set of Proposed Modifications to Proposed CCPA Regulations  
**Date:** Wednesday, October 28, 2020 4:33:28 PM  
**Attachments:** [CTA Letter on Third Set of Modifications to Proposed CCPA Regulations-FINAL.pdf](#)

---

See attached for comment letter from Consumer Technology Association (CTA).

Thank you,  
Rachel

**Rachel Sanford Nemeth**

Sr. Director, Regulatory Affairs  
Consumer Technology Association, producer of CES®

[REDACTED]

d: [REDACTED]

c: [REDACTED]

**Disclaimer**

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by **Mimecast Ltd**, an innovator in Software as a Service (SaaS) for business. Providing a **safer** and **more useful** place for your human generated data. Specializing in; Security, archiving and compliance. To find out more [Click Here](#).



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  
Email: [PrivacyRegulations@doj.ca.gov](mailto:PrivacyRegulations@doj.ca.gov)

Dear Ms. Kim:

Consumer Technology Association (“CTA”)<sup>1</sup> respectfully submits this letter commenting on the third set of modifications to the proposed California Consumer Privacy Act (“CCPA”)<sup>2</sup> regulations.<sup>3</sup> As CTA has previously explained, since the CCPA was signed into law, companies of all sizes have raced to establish processes, policies, and systems to come into compliance. For many, this effort has already been a significant, challenging and expensive initiative.<sup>4</sup>

CTA therefore supported those changes in the initial and second set of modifications that sought to reduce some of the confusion regarding businesses’ regulatory requirements. CTA now recommends changing Proposed Section 999.306—Notice of Right to Opt-Out of Sale of Personal Information—to provide more clarity and predictability for the many businesses that have implemented CCPA requirements in good faith and to avoid consumer confusion.

The Department should clarify that the new offline notice requirement applies when only a business both collects and *sells* data from offline activity. Many businesses do not sell data collected during offline activities such as store visits. For businesses that do not sell data

---

<sup>1</sup> As North America’s largest technology trade association, CTA<sup>®</sup> is the tech sector. Our members are the world’s leading innovators—from startups to global brands—helping support more than 18 million American jobs. CTA owns and produces CES<sup>®</sup>—the most influential tech event on the planet.

<sup>2</sup> Cal Civ. Code § 1798.100 *et. seq.*

<sup>3</sup> See California Department of Justice, Notice of Third Set of Modifications to Text of Proposed Regulations, OAL File No. 2019-1001-05 (Oct. 12, 2020).

<sup>4</sup> See Comments of Consumer Technology Association on Proposed Adoption of California Consumer Privacy Act Regulations (filed Dec. 6, 2019); Comments of Consumer Technology Association on Modifications to Proposed Regulations (filed Feb. 25, 2020); Comments of Consumer Technology Association on Second Set of Modifications to Proposed Regulations (filed Mar. 27, 2020).

Producer of



collected during such offline activities, but sell data collected online, an offline notice will create consumer confusion by falsely implying to consumers that it does. Even if such a notice does not directly cause consumer confusion, an additional offline notice would be redundant and burdensome to businesses that must already provide two forms of opt-out notice.<sup>5</sup>

CTA agrees that a company should offer an offline notice when data that is collected offline may be sold. Accordingly, the Department should make the following targeted edits to Proposed Section 999.306(b)(3):

(3) A business that collects personal information in the course of interacting with consumers offline **and sells such information** shall also provide notice by an offline method that facilitates consumers' awareness of their right to opt-out. Illustrative examples follow:

a. A business that collects personal information from consumers in a brick-and-mortar store **and sells such information** may provide notice by printing the notice on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the notice can be found online.

b. A business that collects personal information over the phone **and sells such information** may provide the notice orally during the call where the information is collected.

CTA appreciates the Department's continued efforts to adopt and implement CCPA regulations in a manner that enhances consumer privacy without being unduly burdensome on businesses, especially startups and other small businesses. With the recent adoption of final regulations in August, CTA encourages the Department to condition any modification to CCPA regulations on providing additional clarity to both businesses and consumers, reducing still-remaining unjustified burdens on businesses, and ensuring that the regulations properly adhere to the requirements of the statute. The above suggested modifications will help accomplish these goals.

Respectfully submitted,

/s/ Michael Petricone

Michael Petricone

Sr. VP, Government and Regulatory Affairs

/s/ Rachel Nemeth

Rachel Nemeth

Senior Director, Regulatory Affairs

---

<sup>5</sup> Cal Civ. Code § 1798.135(1)-(2); Cal. Code Regs. Tit. 11 § 999.306(b)(1)-(2).

**From:** [Javier A. Bastidas](#)  
**To:** [Privacy Regulations](#)  
**Cc:** [Lara L. DeCaro](#)  
**Subject:** Comments to Proposed Modified CCPA Regulations [OAL File No. 2019-1001-05]  
**Date:** Wednesday, October 28, 2020 4:44:16 PM  
**Attachments:** [Comments to Third Set of Proposed Modified CCPA Regulations \(01629220x9C6B5\).pdf](#)

---

Dear Deputy Attorney Kim:

Attached please find our law firm's comments to the Third Set of Proposed Modifications to the CCPA Regulations.

If you have any questions regarding these comments, please do not hesitate to contact us.

Thank you for your time,

Javier Bastidas

**Javier A. Bastidas**

**Leland, Parachini, Steinberg, Matzger & Melnick LLP**

199 Fremont Street, 21st Floor

San Francisco, CA 94105

Telephone: 415.957.1800

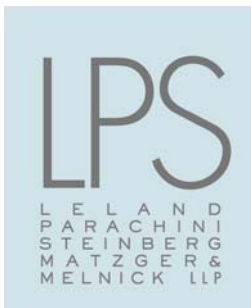
Direct: [REDACTED]

Mobile: [REDACTED]

**Think Green!** Before printing this e-mail ask the question, is it necessary?

**CONFIDENTIALITY:**

*The e-mail is intended solely for the use of the individual to whom it is addressed and may contain information that is privileged, confidential or otherwise exempt from disclosure under applicable law. If the reader of this e-mail is not the intended recipient or the employee or agent of the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please immediately notify us by replying to the original sender of this note or by telephone at 415.957.1800 and delete all copies of this e-mail. It is the recipient's responsibility to scan this e-mail and any attachments for viruses. Thank you.*



LARA L. DECARO  
[REDACTED]  
JAVIER A. BASTIDAS  
[REDACTED]

October 28, 2020

*Sent via electronic mail*

Deputy Attorney General 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: **Comments to the Third Set of Proposed Modified Regulations Concerning the California Consumer Privacy Act ("CCPA")**

Dear Deputy Attorney General Kim:

On behalf of our law firm, Leland, Parachini, Steinberg, Matzger & Melnick, LLP, we respectfully provide the following comments concerning the Third Set of Proposed Modified Regulations for the CCPA (the "Regulations"). We appreciate and applaud the Attorney General's efforts to clarify and improve upon the previous, existing regulations. In this comment round, we focus on only the most important matters to our clients as we recognize the grand task ahead of you.

**A. ENABLING LEGISLATION.**

The Attorney General derives its authority for the proposed Regulations, in part, from California Civil Code Section 1798.185(a), which reads:

(a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

[...]

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.

{999/0001/LTR/01629186.DOCX}

199 FREMONT STREET, 21<sup>ST</sup> FLOOR ■ SAN FRANCISCO, CA 94105  
PHONE 415.957.1800 ■ FAX 415.974.1520 ■ WWW.LPSLAW.COM

CCPA\_3RD15DAY\_00152



(4) Establishing rules and procedures for the following:

[...] (C) 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.

[...]

(6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this title and as needed thereafter.

## **B. ANALYSIS OF PROPOSED REGULATIONS.**

### **I. EXCEPTIONS FOR TRADE SECRETS AND INTELLECTUAL PROPERTY RIGHTS**

Thus far, there are no provisions concerning the exceptions mandated by Section 1798.185(a)(3) though previous commentators have noted the deficiency. The Attorney General argued that “the comments fail to show how an exemption for protection of intellectual property rights is necessary” as they “fail to explain how a consumer’s personal information collected by the business could be subject to the business’s copyright, trademark, or patent rights, or how a business could possibly patent, trademark or copyright a consumer’s personal information” (Response 901/Appendix A). The Attorney General’s responses also noted that even if a consumer’s personal information could potentially be considered a trade secret, “neither federal nor state law provides absolute protection for trade secrets” (*Id.* at Response 247/). The Attorney General further concluded that “a blanket exemption from disclosure for any information a business deems could be a trade secret or another form of intellectual property would be overbroad and defeat the Legislature’s purpose of providing consumers with the right to know information businesses collect from them” (*Id.*)

Respectfully, Section 1798.185(a)(3) states nothing about "blanket" exemptions nor are businesses seeking "absolute" protection. It is also not the duty of the public to delineate the specific exceptions contemplated by the above statute. The legislators tasked the Attorney General's office to adopt the appropriate language, after receiving comment from the public. While there is no doubt that the legislature intended to provide consumers with the right to know about the information that businesses collect, it was also the legislature's clear intent to provide some





exceptions in this context, including but not limited to those concerning trade secrets and other intellectual property rights.

For example, we point to the obligation within the Notice of Financial Incentive portion of the Regulations (Section 999.307(b)(5)<sup>1</sup>), requiring businesses to provide a “good-faith estimate of the value of the consumer’s data.” Such disclosure as required by the Regulation may involve proprietary information, which Section 3426.1 of California’s Uniform Trade defines as follows:

(d) “Trade secret” means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

- (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and
- (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

It is reasonable to conclude that companies may wish to keep their proprietary methods for such a calculation a secret. While we agree that a consumer has a right to know what information is collected, where is the authority requiring a company to disclose its formulas for calculating the economic value contemplated by Regulation 999.307(b)(5)? It simply does not exist.

Therefore, the easy fix is to delete Section 999.307(b)(5) from the Regulations and to compose new regulations that address the legislature's concerns over trade secrets, intellectual property rights, and other possible exceptions needed to comply with other State and Federal laws. Once the Attorney General has drafted such new language, then the public can provide meaningful comments regarding the new language in a future comment period.

## II. DEVELOPMENT OF OPT-OUT LOGO OR BUTTON

Again, the Attorney General has failed to develop a "recognizable and uniform opt-out logo or button" as required by Section 1798.185(a)(4)(C) of the Civil Code (see above). While the original proposed regulations had provided for an Opt-Out switch, those provisions were

---

<sup>1</sup> (b) A business shall include the following in its notice of financial incentive... (5) An explanation of why the financial incentive or price or service difference is permitted under the CCPA, including: a. A good-faith estimate of the value of the consumer’s data that forms the basis for offering the financial incentive or price or service difference; and b. A description of the method the business used to calculate the value of the consumer’s data.



deleted from subsequent iterations of the Regulations. Such a logo or button would greatly simplify the Opt-out process and bring clarity to businesses throughout the state and beyond.

Newly proposed Regulation 999.315(h) provides the following:

(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...

(1) The business's process for submitting a request to opt-out 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 is 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 is measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request.

(2) 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 optout.

While we appreciate the Attorney General's attempts to clarify the opt-out rules, we believe that the confusion that exists in this regard can be avoided by propounding the adoption of a uniform opt-out button. We agree the Notice language should be simple to understand, and we support the notion behind subsection (h)(2), but creating a recognizable device for the public to use will eliminate the confusion companies are currently experiencing in figuring out what language is legally sufficient for their requisite Notices. While the new Regulation language provides some helpful guidance, it is still too complicated. There will be no need for measuring the "number of steps" towards opt-out versus opt-in procedures when a recognizable button can accomplish what the legislature intended in just one-step.

### III. ACCESSIBILITY

While our firm of course supports the requirement that all website notices be "reasonably accessible to consumers with disabilities," respectfully, we believe that the Attorney General's office has overstepped its authority by introducing language, in essence new law, concerning the use of "Web Content Accessibility Guidelines" or "WCAG." The United States Department of Justice ("DOJ") has urged that "public accommodations have flexibility in how to comply with the ADA's general requirements of nondiscrimination and effective communication" (see letter dated September 25, 2018, from Assistant General Stephen E. Boyd<sup>2</sup>). Furthermore, in *Robles v.*

---

<sup>2</sup> <https://www.adatitleiii.com/wp-content/uploads/sites/121/2018/10/DOJ-letter-to-congress.pdf>



*Domino's Pizza, LLC* (2019) 913 F.3d 898, the Ninth Circuit held that the ADA was intended to give businesses "maximum flexibility" in meeting the statute's requirements.

"A desire to maintain this flexibility might explain why DOJ withdrew its [Advanced Notice of Proposed Rulemaking] related to website accessibility and 'continue[s] to assess *whether specific technical standards are necessary and appropriate* to assist covered entities with complying with the ADA'." (*Id.* at 908-909, citing 82 Fed. Reg. 60921-01 (December 26, 2017) [emphasis in original]).

Furthermore California Civil Code Section 1798.185(a)(6) states that the Attorney General shall establish rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer. It follows that businesses can provide the requisite notices in a manner that is easily understood if the regulations dictating the requirements were also easily understood.

Here we are in late October 2020, and the Regulations have still not been finalized in reality. How can a company truly be held to all CCPA requirements under such circumstances? Add to that, the fact that, as a result of the on-going Covid-19 pandemic, businesses have been forced to furlough or fire employees who have relevant knowledge and responsibility for CCPA compliance. Businesses have also been forced to reduce their outside counsel due to pandemic-related budget shortfalls.

In this environment, aside from the legislative overstep on the part of the Attorney General, it simply does not make any sense to introduce the new WCAG requirements when such rules complicate the question of what the Regulations require, and create new, substantial costs for all on-line companies. Further, there's no evidence that these WCAG requirements are truly "generally recognized industry standards" for on-line information accessibility. In fact, both the DOJ and the Ninth Circuit hold positions that contradict this proposition.

In the Attorney General's own words (See "Final" Statement of Reasons published on June 1, 2020):

"DOCUMENT INCORPORATED BY REFERENCE The following document is incorporated in the regulations by reference: World Wide Web Consortium, Web Content Accessibility Guidelines (WCAG) 2.1 (June 5, 2018) [as of May 21, 2020]. The document is incorporated by reference because it would be ***cumbersome, unduly expensive, or otherwise impractical*** to publish the document in the California Code of Regulations..." (emphasis added).

In other words, the Attorney General appears to expect companies to follow the voluminous and admittedly "cumbersome" WCAG requirements, even though the CCPA makes no mention of it





and the DOJ strongly advise flexibility in compliance. In short, the WCAG rules, aside from being unconstitutional (as fully explained in our previous comment dated and submitted on February 25, 2020), creates a scenario that makes it practically impossible for companies to successfully achieve CCPA compliance because companies cannot provide "simple" notices when the rules behind them are so terribly complex.

Thank you for your time and consideration of these comments.

Very truly yours,

A handwritten signature in blue ink, appearing to read "LDeCaro", followed by a forward slash and the letter "s".

Lara L. DeCaro  
LELAND, PARACHINI, STEINBERG,  
MATZGER & MELNICK, LLP

A handwritten signature in blue ink, appearing to read "JAB", followed by a forward slash and the letter "s".

Javier A. Bastidas  
LELAND, PARACHINI, STEINBERG,  
MATZGER & MELNICK, LLP

**From:** [Halpert, Jim](#)  
**To:** [Privacy Regulations](#)  
**Subject:** State Coalition -- Final Comments re AG\_s Office CCPA Do Not Sell Notice Rules October 28, 2020.DOCX  
**Date:** Wednesday, October 28, 2020 5:01:08 PM  
**Attachments:** [State Coalition -- Final Comments re AG\\_s Office CCPA Do Not Sell Notice Rules October 28, 2020.DOCX](#)

---

Enclosed are our comments on the latest proposed rules changes.

Thank you for your consideration – Jim Halpert

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](mailto:postmaster@dlapiper.com). Thank you.

# State Privacy and Security Coalition, Inc.

October 28, 2020

Lisa B. Kim, Privacy Regulations Coordinator  
California Department of Justice  
300 Spring Street, 1<sup>st</sup> Floor  
Los Angeles, CA 90013  
[PrivacyRegulations@doj.ca.gov](mailto:PrivacyRegulations@doj.ca.gov)

**Re: Comments Regarding Title 11(1)(20): Third 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 and workable matter 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 agree with the with the proposed additions laid out in § 999.315(h) regarding not creating barriers to the choice to opt out, and suggest one clarification highlighted below. However, we are concerned about the changes proposed in 999.306(b) because of the risk of consumer confusion and therefore oppose these modifications. Only when a business actually sells personal information collected through the offline channel should a notice of the right to opt out be required.

We further oppose the change to § 999.326(a), which would in the case of right to know and data deletion requests bar businesses from both asking the consumer to verify their identity and to confirm that the authorization presented by the authorized agent is actually from the consumer.

### **1. We agree with that businesses should not interfere with user opt-out requests.**

Our Coalition agrees that businesses should not create barriers to consumers executing opt-out requests for actual sales of personal data. We suggest only a minor clarification with regard to the proposed restrictions in § 999.315(h)(3) -- that the business may explain truthfully the effect of an opt-out request (as the First Amendment to the U.S. Constitution would require).

# State Privacy and Security Coalition, Inc.

2. **We urge clarifying that the additions to the notice of the right to opt-out in § 999.306(b)(3) apply only if the information collected through the applicable offline channel (i.e., in a brick or mortar store or over the phone) is in fact sold.**

Providing a notice of the right to opt-out in offline channels should be required only in situations where personal information collected through the offline channel is sold. To do otherwise would, for example, lengthen telephone interactions with consumers and could require notices in stores when the personal information collected through that channel is never sold. This would be confusing and misleading to consumers, as it would be suggesting to them that the information being collected in that channel is in fact to be sold, when in fact it is not.

Furthermore, if the consumer made a “do not sell” request through the offline channel, the business would in most situations be unable to relate that request to the other channel through which personal information collected is being sold without collecting significantly more personal information – a step that Civil Code § 1798.145(k) of the CCPA specifically makes clear that the statute does not require. The end result would be even more confusing and frustrating for consumers.

On the other hand, if personal data collected by a business through the offline channel is sold, then an opt-out notice should be required. In addition, because notice may be provided “at or before the time of collection”, in the brick and mortar store context, we suggest that “at the store entrance” be included as one of the illustrative examples set forth in § 999.306(b)(3)a.

In the brick and mortar store context, personal information can sometimes be collected outside the store anywhere in the parking lot. For this reason, we suggest an illustrative example for collection of personal information outside the store.

Finally, we suggest that, like subdivision 3a (in-store notice), subdivision 3b (telephone notice) similarly refer to the option of directing consumers to where the notice can be found online. This clarification would be consistent with both subdivision 3a. and with § 999.305(b)(3).

For all these reasons, we ask that the final regulations insert the phrase “that it sells” in subdivision (3), as well as clarify subdivisions (3)a. and b. as follows:

**(3) A business that collects personal information in the course of interacting with consumers offline that it sells shall also provide notice by an offline method that facilitates consumers’ awareness of their right to opt-out. Illustrative examples follow:**

- a. **A business that collects personal information from consumers in a brick-and-mortar store may provide notice by printing the notice on the paper forms that collect the personal information or by posting signage directing consumers to where the notice can be found online by the store entrance, or in the area where the personal information is collected, or, if personal information is collected outside the store, in an area that is reasonably visible to consumers directing consumers to ~~where the notice can be found online.~~**

# State Privacy and Security Coalition, Inc.

- b. A business that collects personal information over the phone during the call where the information is collected may provide the notice aurally or aurally direct consumers to where the notice can be found online~~orally during the call where the information is collected.~~

These language additions would clarify when and what sort of notice is in fact required and would alleviate consumer confusion.

3. 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.

The Final Rules rightly impose greater authentication requirements for right to know and data deletion requests because of the security and privacy risks these rights pose if wielded by fraudsters or hackers. The very same reasons counsel strongly against cutting back on business' leeway to authenticate right to know and data deletion requests filed by a purported authorized agent.

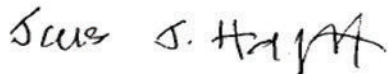
We are unclear about the rationale for shifting the submission of proof of the signed permission authorizing the agent from the consumer to the authorized agent. While the addition of such an option might be workable, allowing a business to do only one (and not both) of further authentication steps risks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

A business should be allowed both to require the consumer to verify their identity with the business *and* to confirm with the business that they provided the authorized agent permission to submit the request. Both are *very important* to prevent fraudulent requests to delete or obtain the contents of a consumer account when a pretexter has established a fake account in the same name as the consumer, thereby making the fake account appear more real.

Respectfully submitted,



Jim Halpert, Counsel  
State Privacy & Security Coalition

**From:** [Aleecia M McDonald](#)  
**To:** [Privacy Regulations](#)  
**Cc:** [Mingya Feng](#); [Zeeshan Sadiq Khan](#); [Bingxuan Luo](#); [Xiaofei Ma](#); [Arjita Mahajan](#)  
**Subject:** Re: NOTICE OF THIRD SET OF PROPOSED MODIFICATIONS TO TEXT OF CCPA REGULATIONS  
**Date:** Wednesday, October 28, 2020 5:01:40 PM  
**Attachments:** [McDonaldEtAl-Comments-to-AG-CCPA-Oct28-Rulemaking.pdf](#)

---

Thank you for the opportunity to provide comments, as enclosed.

Aleecia

Assistant Professor Aleecia M. McDonald // Carnegie Mellon's Information Networking Institute //



Comments from:

Maggie Feng [REDACTED], Zeeshan Sadiq Khan [REDACTED],  
Bingxuan Luo [REDACTED], Xiaofei Ma [REDACTED]  
Information Networking Institute  
Carnegie Mellon University  
4616 Henry Street  
Pittsburgh, PA 15213

Arjita Mahajan [REDACTED],  
Professor Aleecia M. McDonald (corresponding author) [REDACTED]  
NASA Ames Research Center  
Carnegie Mellon University  
Building 23  
Moffett Field, CA 94035

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

Regarding

Sections 999.300 through 999.341  
of Title 11, Division 1, Chapter 20,  
of the California Code of Regulations (CCR)  
concerning the California Consumer Privacy Act (CCPA)

## About the Authors

Maggie Feng is a graduate student at Carnegie Mellon University pursuing her Master's in Information Security. She is currently part of the CCPA browser tool team under Professor McDonald's supervision, worked on the front end, and designed the authentication system.

Zeeshan Sadiq Khan is a graduate student at Carnegie Mellon University pursuing his Master's in Information Security. Inspired by the Do Not Track specification, he has designed a similar specification to signal to the web servers Californian's data privacy preferences for CCPA use.

Bingxuan Luo is a graduate student at Carnegie Mellon University pursuing a Master's degree in Information Technology Mobility. She was a previous intern at Facebook. On the CCPA browser tool, she designed the UI and user interaction flow, and helped integrate the API with the back end.

Xiaofei Ma is a graduate student at Carnegie Mellon University pursuing her Master's in Information Technology. She designed features to send Californian's data privacy preferences to both first-party and third-party companies in the CCPA browser tool.

Arjita Mahajan is a graduate student at Carnegie Mellon University pursuing her Master's in Software Management. She has 5 years of work experience in Software Engineering and has worked on GDPR requirements professionally. She works as Program Manager for the browser tools team and helps engineering team coordination and requirements planning with Professor McDonald.

Aleecia M. McDonald is an Assistant Professor at Carnegie Mellon's Information Networking Institute, based in Silicon Valley. Her *Psst!* Lab focuses on researching the public policy issues of Internet privacy including user expectations, behavioral economics and mental models of privacy, and the efficacy of industry self-regulation. She co-chaired the WC3's Tracking Protection Working Group, a multi-national effort to establish international standards for a Do Not Track mechanism that users can enable to request enhanced privacy online. She presented testimony to the California Assembly including regarding the California Consumer Privacy Act, contributed to testimony before the United States Senate, and presented research results to the Federal Trade Commission. Professor McDonald is a member of the Board of Directors for the Privacy Rights Clearinghouse, and is a member of Carnegie Mellon's CyLab. She was Director of Privacy at the Stanford Center for Internet and Society where she maintains a non-resident Fellow affiliation. She was also previously a Senior Privacy Researcher for Mozilla during the rollout of Do Not Track in the Firefox web browser. A decade of experience working in software startups adds a practical focus to her academic work. She holds a PhD in Engineering & Public Policy from Carnegie Mellon.

Affiliations are for identification and context only. These comments reflect the authors' views alone; we do not speak for any other groups, including Carnegie Mellon University.



## Summary

In this comment we urge the following three courses of action:

1. Adding a new subsection, § 999.315 (h) (6) Opt-out preferences must persist for at least as long as opt-in preferences.
2. Adding a new function for the AG's office to facilitate centralized opt-out for data that is indexed by non-technical PII including name, address, and phone number akin to the FTC's Do Not Call list. The AG's office would therefore become an Authorized Agent under revised § 999.326.
3. Similar to the AG's prior work on *Privacy on the Go: Recommendations for the Mobile Ecosystem* <[https://oag.ca.gov/sites/all/files/pdfs/privacy/privacy\\_on\\_the\\_go.pdf](https://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf)> we call on the AG's office to convene dialogs regarding the technical mechanisms for CCPA rights. We see some current offerings do not yet fulfill legal requirements for children's opt-out consent in § 999.332.

## Table of Contents

<b>Background: Building Tools to Enacting Privacy Choices .....</b>	<b>4</b>
<b>Topic 1: Changes to § 999.315 Requests to Opt-Out .....</b>	<b>4</b>
<b>Topic 2: Creating a Do Not Sell Database within the California AG’s Office.....</b>	<b>4</b>
Recommendation: .....	6
<b>Topic 3: Tools for CCPA Compliance.....</b>	<b>6</b>
Recommendation: .....	9

### Background: Building Tools to Enacting Privacy Choices

Thank you for the opportunity to comment on the proposed rulemaking around the California Consumer Privacy Act (CCPA.) As part of our Practicum course at Carnegie Mellon, this semester a team of five students is currently prototyping *Data Guard*. The Data Guard project is a collection of technical tools and user education to support CCPA rights in an automated way, in order to reduce the user burden of asserting CCPA rights.

During our work on Data Guard we encountered areas we see a role for the California Attorney General’s (AG’s) office to host data that would support realizing Californian’s data privacy rights. In particular, we recommend a structure parallel to the FTC’s hosting of Do Not Call phone numbers *in addition* to other technical measures that are under development. Second, we also note parallel similar efforts from multiple groups, and hope the AG’s office will take a formal interest in tools that meet business’ legal requirements under add legal section here.

### Topic 1: Changes to § 999.315 Requests to Opt-Out

We support the proposed addition of (h) to § 999.315, which contains common-sense requirements to avoid “dark patterns” on the web that discourage user choice. In addition, we propose:

§ 999.315 (h) (6) Opt-out preferences must persist for at least as long as opt-in preferences. For example, if a user is able to opt-in indefinitely without further contact, then a company must not present daily opt-out dialogs.

### Topic 2: Creating a Do Not Sell Database within the California AG’s Office

Under the CCPA, businesses are required to provide a “Do Not Sell My Info” link on their sites. With visible links, consumers can exercise their privacy rights from first parties, but they are often not aware of the data collection from third parties. Indeed, one of the major advantages to an automated header request is that it reaches all parties, including invisible third parties. However, this is of limited use for historic third-party data collection with data still in use.

Data brokers can still collect consumers’ data without any direct interaction. In this case, consumers may not be informed that their data is collected by unknown parties. How to practice their CCPA rights can be unclear.

To solve this problem, CCPA requires all data brokers to register with AG's office and provide information about how to opt out for consumers. Although the data broker listing is accessible to consumers, it's extraordinarily difficult for consumers to follow the instructions and manually opt-out 407 companies.<sup>1</sup>

Californians might like to automatically notify data brokers of one of two things:

1. The user is a child (and therefore must be asked to consent to opt-in to data use)  
*Or*
2. The user is an adult, and hereby opts of data use

There is a technical obstacle to realizing CCPA rights. One might imagine simply sending an HTTP header signal to all data brokers once a year to advise them of childhood or opt-out, but such a system of broadcasting HTTP headers fails to work. Third parties, such as data brokers, can (typically) only read their own cookies when a user happens to visit a first-party website at the same time the third-party website is also part of the communication. With 407 data brokers, it could take quite a while to bump into all of them. During that time, children's data and the data from those who try to opt-out would still be bought, sold, and used.

Large companies run into this issue too. They might have multiple domains (e.g. google.com and youtube.com are both part of the same corporate structure, but have different technical structures.) Major companies such as Warner Media (including cnn.com),<sup>2</sup> Walmart<sup>3</sup>, and Oracle<sup>4</sup> use email as an identifier to assist users with the opt-out process, not just within their own company, but as an identifier they send to third party partners. Other potential (mostly) unique identifiers include telephone number, address, and/or name.

In order to help consumers exercising their CCPA rights with data brokers, we designed a feature in our Data Guard CCPA browser tool. Users of our tool can send requests to all data brokers, identifying the user by email address. A screenshot of the tool can be seen in Figure 1.

---

<sup>1</sup> "Data Broker Registry." State of California - Department of Justice - Office of the Attorney General, 22 Oct. 2020, [oag.ca.gov/data-brokers](https://oag.ca.gov/data-brokers). Accessed 28 October 2020.

<sup>2</sup> "CNN opt-out form." WarnerMedia Privacy Center, [www.warnermediaprivacy.com/do-not-sell/request/](https://www.warnermediaprivacy.com/do-not-sell/request/). Accessed 28 October 2020.

<sup>3</sup> "Walmart opt-out inquiry form." Walmart, [cpa-ui.walmart.com/affirmation](https://cpa-ui.walmart.com/affirmation). Accessed 28 October 2020.

<sup>4</sup> "Oracle opt-out inquiry form." Oracle, [www.oracle.com/legal/data-privacy-inquiry-form.html](https://www.oracle.com/legal/data-privacy-inquiry-form.html). Accessed 28 October 2020.

Data Broker

"Data broker" means a business that doesn't have direct relationship with you but collect your information. Imagine a website you never visit before collecting your information and exchange for profit. **You can ask them stop selling your data.**

By checking the button, we will help you to send "do not sell my data" request to data brokers. To complete the request, we need your additional information for purpose of verification.

Email

abc@hotmail.com

Do Not Sell

Figure 1: A screenshot of our browser tool's setting page. Users will need to enter their frequently used email address in the input field. After filling out the form, users only need to click the "Do Not Sell" button to attempt to opt-out of the sale of all registered data brokers. This is harder in practice than in theory.

Consumers can conveniently exercise their CCPA rights with one click. Compared with complex instructions given by companies in the registry, our tool provides a more understandable and scalable solution since consumers do not need to go to all 407 data brokers.

We notice we essentially reinvented the FTC Do Not Call list.

It would be *substantially better* if the AG's office were to host this information instead of having browser plugins and other attempt to contact data brokers and companies on the user's behalf. On the citizen side, it is better to trust the AG's office to hold PII securely than to trust browser plugins or other technologies. For companies, they would have the advantage of a single centralized list to automate checking against, rather than be pestered by random requests coming in at any time. Further, the AG's office could do a proper job of authenticating users to ensure someone is who they say they are, which benefits both citizens and companies alike. We therefore suggest the AG's office become an Authorized Agent under revised § 999.326 in providing functionality akin to the FTC's Do Not Call list.

### Recommendation:

We recommend the California Attorney General's office create a centralized "Do Not Sell" database similar to the FTC's "Do Not Call" list. The Do Not Sell list would contain non-technical identifiers (such as email address, phone number, mailing address, and name,) for those who choose to join, along with notations for those protected as children.

While technical identifiers like cookies and browser fingerprints will likely be the primary way for companies to re-identify users, we do see reliance on non-technical PII in practice today on an *ad hoc* basis. The CA AG's office stepping in as an Authorized Agent under revised § 999.326 can secure consumers' rights, ease the process of exercising rights at scale, and create an automatable path for companies to ensure they are compliant with the law.

### Topic 3: Tools for CCPA Compliance

Similar to our Data Guard tool, there are a few other mechanisms in development to assist users of California exercise the rights given to them by the CCPA. The most prominent is Global Privacy Control<sup>5</sup>. GPC utilizes an HTTP header to signal to the web server the user is interacting with that

---

<sup>5</sup> "Privacy Badger." Electronic Frontier Foundation, [privacybadger.org/](https://privacybadger.org/). Accessed 28 October 2020.



the user wishes to opt out of sale/share of personal data to other parties. There are several implementations of GPC, some of which we show in the figures below.



Figure 2: Privacy Badger<sup>6</sup>



Figure 3: Blur by Abine<sup>7</sup>

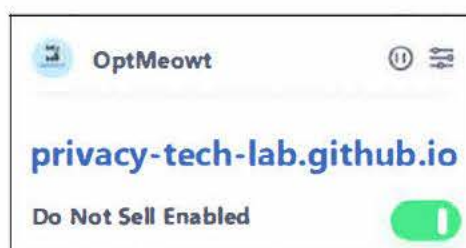


Figure 4: OptMeowt<sup>8</sup>

<sup>6</sup> "Privacy Badger." Electronic Frontier Foundation, [privacybadger.org/](https://privacybadger.org/). Accessed 28 October 2020.

<sup>7</sup> "Remove Your Personal Information From Search Engines." Abine Blur: Passwords, Payments, & Privacy, [www.abine.com/](https://www.abine.com/). Accessed 28 October 2020.

<sup>8</sup> "OptMeowt." Google, [chrome.google.com/webstore/detail/optmeowt/hdbnkdbhglahihjdbodmfefogcjbpgbo](https://chrome.google.com/webstore/detail/optmeowt/hdbnkdbhglahihjdbodmfefogcjbpgbo). Accessed 28 October 2020.

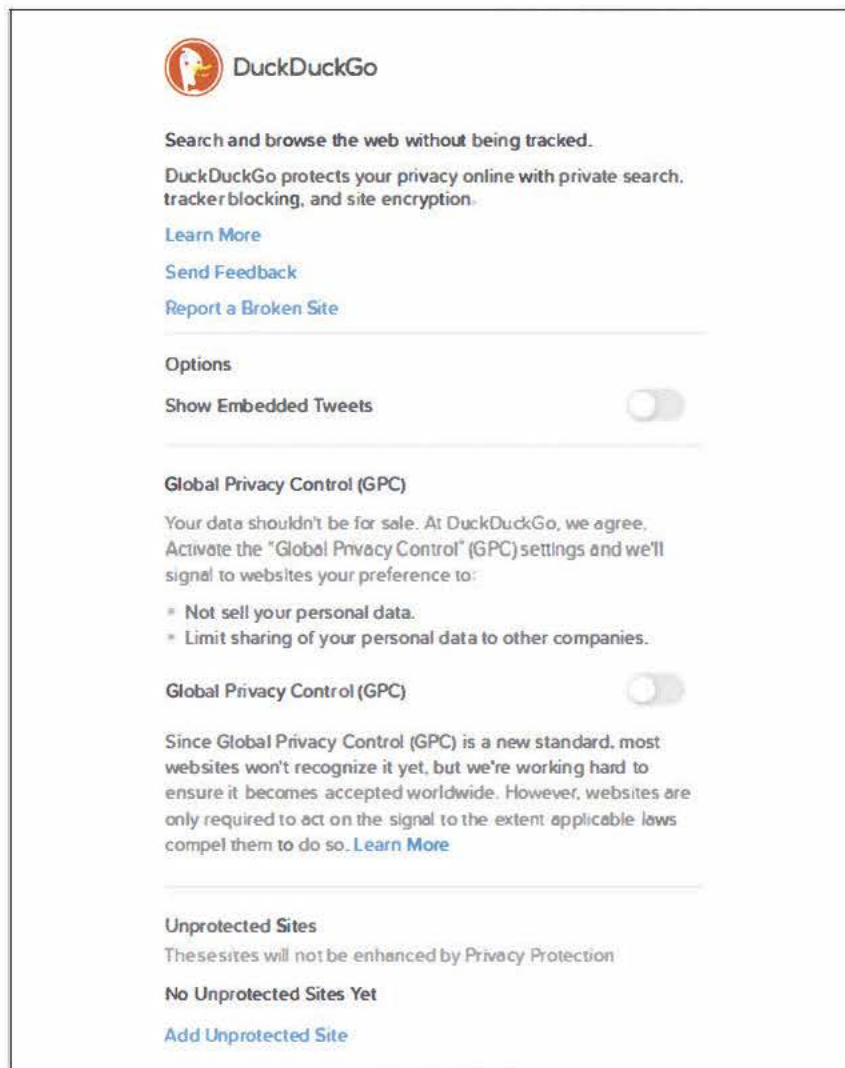


Figure 5: DuckDuckGo<sup>9</sup>

While these are great attempts to allow users to opt-out of sale of their data, there are concerning limitations. None of these tools appears to be responsive to age. The structure of the GPC is built upon users signaling an opt-out for the sale of data, and in the absence of the header it is assumed that they may have opted-in. This does not work for children as they must, by law, be opted out by default, including under the newly revised § 999.332. Our tool is designed to include children and teenagers. While we have great faith in the creators of GPC and assume they plan to add additional functionality later in future work, we are concerned that any early adopters may not realize the current version of GPC does not appear to be legally compliant.

The idea that some tools may be easier to use or faster is not a problem, but rather a marketplace. And indeed, GPC does some things very nicely that we do not do as well. Where we have concerns is that tools may not implement laws correctly.

<sup>9</sup> Settings are enabled as described in “DuckDuckGo Founding Member in Global Privacy Control (GPC) Standards Effort,” DuckDuckGo. <https://spreadprivacy.com/announcing-global-privacy-control/>. Accessed 28 October 2020.

**Recommendation:**

We believe the AG's office has an interest in ensuring tools are, at minimum, legally compliant. One light-touch way to secure that interest is to follow the prior example that led to the publication of *Privacy on the Go: Recommendations for the Mobile Ecosystem*,<sup>10</sup> which included a series of meetings with stakeholders to develop best practice recommendations.

---

<sup>10</sup> "Privacy on the Go: Recommendations for the Mobile Ecosystem," California Office of the Attorney General (January, 2013.) [https://oag.ca.gov/sites/all/files/pdfs/privacy/privacy\\_on\\_the\\_go.pdf](https://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf). Accessed 28 October 2020.