

The State of Authorized Agent Opt Outs Under the California Consumer Privacy Act

BY MAUREEN MAHONEY, GINNY FAHS, AND DON MARTI
FEBRUARY 2021

Table of Contents

I. Introduction	3
II. Study Methods	5
Selecting companies	5
Recruiting consumer volunteers	5
Serving agent requests	5
Notice of results to companies	6
CCPA guidelines for authorized agent opt outs	6
III. Study Results	7
Company Responses	7
Requests Issued	8
IV. Ineffective Opt Outs	8
Flawed or deficient opt-out design	8
Difficulties opting out of cross-context targeted advertising	16
Inadequate opt-out notice and communication	22
V. Recommendations	24
VI. Conclusion	26
VII. Appendix	27

Acknowledgments

Generous support for this study comes from Craig Newmark Philanthropies and Omidyar Network as part of a broader initiative to advance consumer privacy and strengthen data rights in the United States.



OMIDYAR NETWORK™

Craig Newmark Philanthropies

I. Introduction

On January 1, 2020, the California Consumer Privacy Act (CCPA) went into effect, giving California consumers important new privacy rights, including the right to access, delete, and stop the sale of their information.¹ The CCPA is the first comprehensive commercial privacy law in the United States. But, many of the rights provided by the CCPA place responsibility on the consumer to submit requests. Because consumers interact with hundreds, if not thousands of companies—for example, there are over 400 data brokers on the California data broker registry alone²—it could practically be a full-time job to adequately protect one’s privacy. Consumer Reports has found that consumers experience significant difficulty exercising their rights under the CCPA.³ Many data brokers’ opt-out processes are so onerous that they have substantially impaired consumers’ ability to opt out. By design, the CCPA has an “authorized agent” provision that allows a consumer to designate a third party to perform requests on their behalf, allowing for a practical option for consumers to exercise their privacy rights under the CCPA.⁴

At Consumer Reports, we want to help consumers meaningfully exercise their data rights, and are currently working to help consumers navigate the new digital marketplace by exploring the authorized agent provision of the CCPA. To kick off this project, we began an exploratory study to submit “Do Not Sell” (“DNS” or “opt-out”) requests on behalf of consumers to 21 companies. During the course of this study, we ran into problems in pursuing opt-out requests on behalf of consumers at nearly every company, including:

- Flawed or deficient opt-out design;
- Difficult to opt out with respect to targeted advertising; or
- Ineffective communication with authorized agents, including inability to explain how to submit opt-out requests.

Some companies threw up significant roadblocks to authorized agents seeking to opt out. For example, agents encountered online interfaces that were difficult, if not impossible, to navigate. In addition, some companies claimed to not sell consumer information, even though they explained in their privacy policies that consumers’ personal information was shared with other companies in order to deliver interest-based advertising. And company disclosures and customer service personnel often failed to provide effective direction to agents seeking to submit these requests.

¹ Cal. Civ. Code § 1798.100 et seq.

² State of California Department of Justice, Office of the Attorney General, Data Broker Registry (last visited Jan. 28, 2021), <https://oag.ca.gov/data-brokers> [hereinafter Data Broker Registry]. The registry shows 190 “Complete Registrations” and over 260 “Incomplete Registrations” pending payment for 2021 fees.

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

⁴ Cal. Civ. Code § 1798.135(c); §1798.140(y).

At the very least, companies need to ensure that the authorized agent process works appropriately, so that consumers can better exercise their preferences. The AG should vigorously enforce the CCPA and its implementing regulations. But the AG should also promulgate additional common-sense rules to make sure that opt outs are quick and simple, even when submitted by an authorized agent:

- Clarify that data shared for cross-context targeted advertising is a sale and tighten the restrictions on service providers;
- Prohibit dark patterns as outlined in the Third Set of Proposed Modifications to the CCPA Regulations;⁵
- Require companies to notify agents when the opt-out request has been received and when it has been honored; and
- Make clear that if an agent inadvertently submits a request incorrectly or through an incorrect channel, the company should either accept it or inform the agent how to submit it appropriately.

Authorized agent services will be an important supplement to other CCPA-compliant privacy tools—but only if they work effectively. Consumer Reports is also supporting the Global Privacy Control (GPC), an effort by privacy researchers, advocates, and publishers to create a “Do Not Sell” specification designed to work with the CCPA.⁶ (The CCPA regulations require websites to respect a “user-enabled global privacy control” set by a web browser as a CCPA opt out.⁷) This is a key tool which will also help make the CCPA opt out more workable for consumers, since the GPC can convey DNS signals to companies with which the consumer directly interacts.

But authorized agents will help address data sharing that GPC cannot. Since a fair amount of data has already been collected and sold, the authorized agent can help consumers exercise their preferences with respect to companies, like data brokers, with which the consumer does not have a direct relationship. Authorized agents can also prospectively stop offline data sharing, which the GPC is not designed to do.⁸ Further, the authorized agent will be important in processing access and deletion requests on behalf of consumers, for which there is not an analogous tool similar to the GPC.

Below, we explore the challenges faced in the course of the authorized agent study and how companies and the AG can help address these problems.

⁵ California Attorney General, California Consumer Privacy Act Regulations, Text of Modified Regulations at § 999.315(h)(1)-(5) (Oct. 12, 2020), <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-third-set-mod-101220.pdf>.

⁶ Global Privacy Control, <https://globalprivacycontrol.org> (last visited Jan. 28, 2020).

⁷ Cal. Code Regs. tit. 11 § 999.315(c).

⁸ The GPC could be construed as a request to also stop offline data sharing if a website has access to identifiers such as email address or phone number.

II. Study Methods

In line with Consumer Reports' efforts to help consumers meaningfully exercise their data rights, we launched a lightweight pilot to act as an authorized agent on behalf of a handful of CR members based in California. The purpose of the pilot was to work with consumers and perform authorized agent services to quickly and simply opt out of the sale of their information by various companies.

Selecting companies

We selected 21 companies to participate in the authorized agent Do Not Sell pilot. A list of companies selected can be found in Appendix 2A. We selected a mix of well-known brands likely to have the personal information of many California consumers, data brokers registered with the state of California, and companies known for creative or high-impact use of personal information. Notably, nearly all of these 21 high-profile companies had implementation problems with respect to the authorized agent opt out, demonstrating the need for more work to better ensure that this a viable option for consumers to exercise their rights under the CCPA.

One month before the study, Consumer Reports wrote to the companies selected to inform them of the study ([Appendix 2B](#)). CR asked companies to specify how they would like requests submitted and offered them the opportunity to ask questions and instruct our team about request submission. Ten companies (48%) responded to this correspondence.

Recruiting consumer volunteers

Consumer Reports emailed 1079 of our members in California and invited them to join the authorized agent Do Not Sell pilot. To enroll in the study, consumers had to submit a short web form with their contact information, confirm email and phone number, then digitally sign a permission letter designating Consumer Reports to act as their authorized agent ([Appendix 2C](#)). In total, 124 consumers completed the sign-up process and enrolled successfully. Over the course of the study, participating consumers received a weekly informational newsletter from CR with articles of interest and encouragement to forward communications they received from participating companies to our team at datarightsstudy@cr.org.

Serving agent requests

Consumer Reports manually served 210 agent requests, 10 to each of the 21 companies we selected for the study. Where companies were registered as data brokers on the California Data Broker Registry,⁹ we referred to opt-out instructions from their entry. We also checked "Do Not Sell" links on web sites and links and addresses on privacy policy pages and page footers to learn how companies preferred for requests to be submitted. Opt outs were sent by the method

⁹ Data Broker Registry, *supra* note 2.

that appeared most reliable and up to date, and included email, dedicated opt-out forms, general contact forms, and postal mail.

All 210 requests were served to companies beginning the week of October 19. The requests consisted of 1) an opt-out letter including the consumers' contact information, 2) a signed permission letter from the consumer designating Consumer Reports to act as their authorized agent, and 3) a Certificate of Information or Certificate of Good Standing respecting Consumer Reports' eligibility to conduct business in California. See [Appendix 2D](#) for a sample opt-out request.

Notice of results to companies

We contacted all the companies in this report to give them an opportunity to provide additional information. We heard back from all but six of them, which were Equifax, Gap, Intuit, Spy Dialer, Starbucks, and Trader Joe's.

CCPA guidelines for authorized agent opt outs

A key protection of the CCPA is that consumers have the right to direct a company to stop the sale of their personal information to third parties—and to authorize someone to opt out on their behalf.¹⁰ The CCPA has an inclusive definition of personal information and a broad definition of sale to cover transfers of data for targeted advertising purposes.¹¹ In addition, the opt-out is designed to be simple and easy for consumers or their agents to navigate: companies that sell consumers' personal information are required to place a "Do Not Sell My Personal Information" link on their homepage, which directs the consumer or their authorized agent to a website where they can opt out. The consumer cannot be required to set up an account to opt out.¹² And all personnel who are responsible for handling inquiries about privacy practices or compliance with the CCPA must be informed about how to instruct consumers (and presumably, by extension, their authorized agents) how to opt out.¹³

The authorized agent opt-out provision is fleshed out in the Attorney General's regulations implementing the CCPA. Under the CCPA regulations, companies are required to describe in their privacy policies how an authorized agent may submit a request on behalf of a consumer.¹⁴ The regulations permit the authorized agent to submit opt-out requests without the consumer's direct involvement: the authorized agent may submit opt-out requests on the consumer's behalf if the agent has written permission signed by the consumer to do so. A business may deny the

¹⁰ Cal. Civ. Code § 1798.135(c).

¹¹ 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).

¹² *Id.* § at 1798.135(a)(1).

¹³ *Id.* § at 1798.135(a)(3).

¹⁴ Cal. Code Regs. tit. 11 § 999.308(c)(5)(a).

authorized agent’s request absent that signed permission.¹⁵ Upon receiving the request to opt out, companies have no more than 15 business days to comply with the request.¹⁶

The regulations specifically state that opt-out requests need not be verified; meaning, that the company does not need to confirm the identity of the person submitting the opt-out request—giving authorized agents greater leeway in submitting opt-out requests, including through consumer interfaces. The business may deny the request if they have a “good faith, reasonable, and documented belief” that it is fraudulent, and must provide notice of that denial.¹⁷

Businesses are also required by CCPA regulations to provide two or more methods of opting out, and one of which must be through an interactive form, accessible through the “Do Not Sell” link on the company’s homepage or app.¹⁸

III. Study Results

To assess the effectiveness of the Do Not Sell authorized agent, we examined (1) whether companies confirmed that they had stopped the sale of at least some of the consumer’s data and (2) whether companies had developed a seamless authorized agent opt-out process. As the authorized agent DNS pilot was a small-scale study, these results are a snapshot in time and not necessarily representative of industry writ large.

Company Responses

Consumer Reports issued authorized agent Do Not Sell requests to 21 companies and found the following:

- 12 of 21 companies (57%) ultimately confirmed that they stopped the sale of at least some data in response to all of the opt-out submissions.
- 5 of 21 companies (24%) claimed not to sell consumer data and dismissed the opt-out requests.
- 3 of 21 companies (14%) did not provide confirmation that all of the opt outs had been processed.
- 1 of 21 companies (5%) requested non-standard information that we had not collected from consumers, so we did not complete the opt-out process.

Of companies who responded to Consumer Reports’ agent-submitted opt out requests, the average time to respond was 7 business days.

¹⁵ *Id.* at § 999.315(f).

¹⁶ *Id.* at § 999.315(e).

¹⁷ *Id.* at § 999.315(g).

¹⁸ *Id.* at § 999.315(a).

Requests Issued

It's difficult to quantify the impact of the requests we issued, especially because companies are not required to notify the agent when a request has been received and when it has been honored. One company reported back to CR when a request did not match up with information in its customer database, but most companies did not follow up in this way. Some companies confirmed when opt-out requests had been processed successfully, others did not.

Consumer Reports found that:

- Companies had a functioning process to accept 197 of the 210 opt-out requests sent by the CR agent.
- In 121 cases, the company sent a confirmation that the opt out had been processed.
- In 50 cases, the companies dismissed or disregarded the requests, claiming that they do not sell consumer data.

In the likely case that companies did not report to us every action that they took in response to our requests, the accuracy of our results above is thrown into question. Our results would likely be more precise with improved communication between companies and agents, which we explore in more detail in our recommendations.

IV. Ineffective Opt Outs

Some authorized agent opt outs did not proceed smoothly. We identified three key issues that prevented the authorized agent from effectively stopping the sale of consumers' information:

- Flawed or deficient opt-out design;
- Difficult to opt out with respect to cross-context targeted advertising; and
- Ineffective communication with authorized agents, including inability to explain how to submit opt-out requests.

Below, we explore each in more detail.

Flawed or deficient opt-out design

Several companies' opt-out processes made it difficult for agents and consumers seeking to opt out. For example, online interfaces were difficult to navigate, some consumers seeking to opt out were directed to an access rather than an opt-out request form, and at least one authorized agent opt-out process required some consumer involvement.

Agents submitting opt outs left to navigate deficient design and other hurdles to delivering requests

Axiom's online opt-out process for consumers required the agent to identify, through a drop-down box, the person on whose behalf they were submitting the form: "Myself," "An individual

for whom I have legal guardianship or power of attorney,” or “A deceased member of my family.” There was no option for “Authorized agent.” Since CCPA regulations do not require legal guardianship or power of attorney in order for an authorized agent to submit opt-out requests, but instead require only written permission,¹⁹ this impeded the authorized agent process. (After we notified Acxiom of this issue, they updated their website to provide an option for authorized agents to submit opt-out requests through this portal).

We also tried to submit opt-out requests on behalf of consumers through additional channels, including through a separate online authorized agent flow. Following the flow to submit an authorized agent opt-out request simply took the user back to the consumer opt out. (Acxiom also updated this interface after we shared the findings of the report). Clicking “Do Not Sell My Personal Information” on the homepage took the user to a consumer opt-out page that included the following text:

Acxiom's US Online Opt Out Request Process is intended for individual consumer use. "Authorized Agents" under the California Consumer Privacy Act should adhere to a special process, described [here](#).

Acxiom will accept opt outs from qualified third parties. To obtain a copy of Acxiom's third-party qualification criteria, please send an email to consumeradvo@acxiom.com

Clicking through to pursue the “special process” brought the authorized agent to the next page:

¹⁹ *Id.* at § 999.315(f).

If you have someone else, (which the CCPA calls an “authorized agent”), submit an opt-out request to Acxiom on your behalf, the agent may do so through our online consumer portal found [here](#). Prior to any acceptance of requests through an authorized agent, the authorized agent must complete the minimum requirements described [here](#).

Clicking on the first “here” link led the user to a page called “Acxiom Data Subject Rights Request,” which also had a link to pursue an opt-out request:

To exercise your rights, please select from one of the options below:

- **Opt-Out Request:** If you would like to have your data removed from Acxiom’s US marketing data products.
- **Access Request:** If you would like to receive your Right to Know Consumer Access Report.
- **Deletion Request:** If you would like Acxiom to delete your data from their US marketing data products.



Clicking on the blue “OPT OUT” tab brought the user back to the original consumer opt-out page:

Acxiom's US Online Opt Out Request Process is intended for individual consumer use. "Authorized Agents" under the California Consumer Privacy Act should adhere to a special process, described [here](#).

Acxiom will accept opt outs from qualified third parties. To obtain a copy of Acxiom's third-party qualification criteria, please send an email to consumeradvo@acxiom.com

After multiple attempts, and following up with support staff, we could not complete the Acxiom opt-out process online ([Appendix 4A](#), page 2).

Then, we sent agent opt outs to Acxiom by postal mail ([Appendix 4B](#)). Initially, we did not receive confirmation that those opt-out requests had been processed, but after we provided draft portions of this report to Acxiom for fact-checking, the company notified us that they had honored the mailed opt-out requests.

We also identified problems with Intuit's authorized agent flow for access and deletion requests. On Intuit's website, all privacy actions are locked behind the consumer's account login, which means that an agent cannot submit verifiable consumer requests on behalf of the consumer (Intuit does not honor opt outs because it asserts it does not sell data within the meaning of the CCPA: see *infra*, p. 18).

Clicking on the "Privacy" link on the homepage and pursuing the links to exercise privacy preferences brings the user to an interactive form to submit their personal information:

Data & Privacy
Manage your data

Let's see if we can find you

Enter your info and we'll see what Intuit Accounts or data of yours we can find. The more info you enter, the better chance we'll have of finding your data. [Learn more](#)

Already know you have an Intuit Account? [Sign in](#)

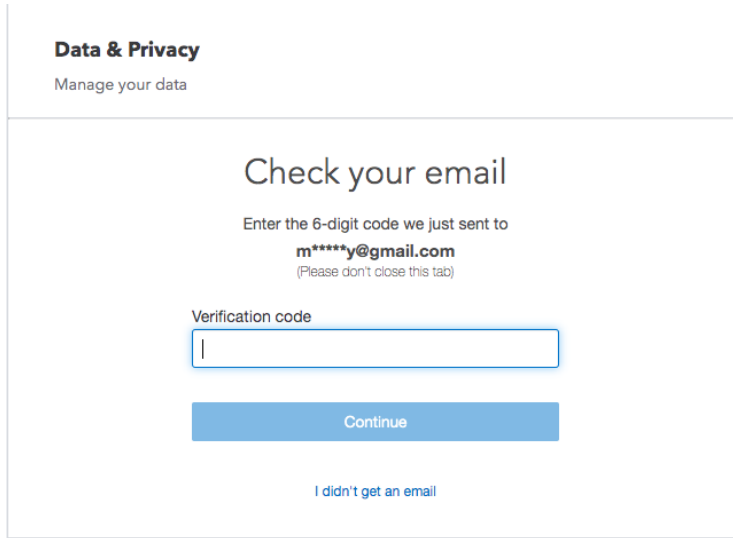
Are you looking for your Credit Karma data? [If so, please contact Credit Karma](#)

* Email address

* Date of birth

* Phone number

The user then encounters an identity verification requirement that only the consumer can fill out; not the authorized agent.



Further, the company does not provide an email address for U.S. customers to submit privacy questions, which could have been a way for the authorized agent to submit requests. ([Appendix 4C](#)) Intuit provided a phone number for customers to submit questions regarding CCPA requests; however, the agent was unable to answer any questions related to CCPA requests at that number. As a result, there was no effective way for consumers—or agents—to submit questions about the CCPA or other privacy concerns. ([Appendix 4D](#))

LiveRamp’s process also posed challenges for the authorized agent. Upon submitting opt-out requests via the opt-out form for authorized agents on LiveRamp’s website, we received a “Subject Access Request Started” email (despite the fact that our request was to opt out of data sale and not for data access) and an invitation to create a portal account in order to submit documentation.

For Authorized Agent Opt-Out requests in order to proceed, you will need to submit documentation authenticating your right to act as an Authorized Agent. You will receive a follow up email providing you access to LiveRamp's privacy portal where you will be asked to upload the following documents:

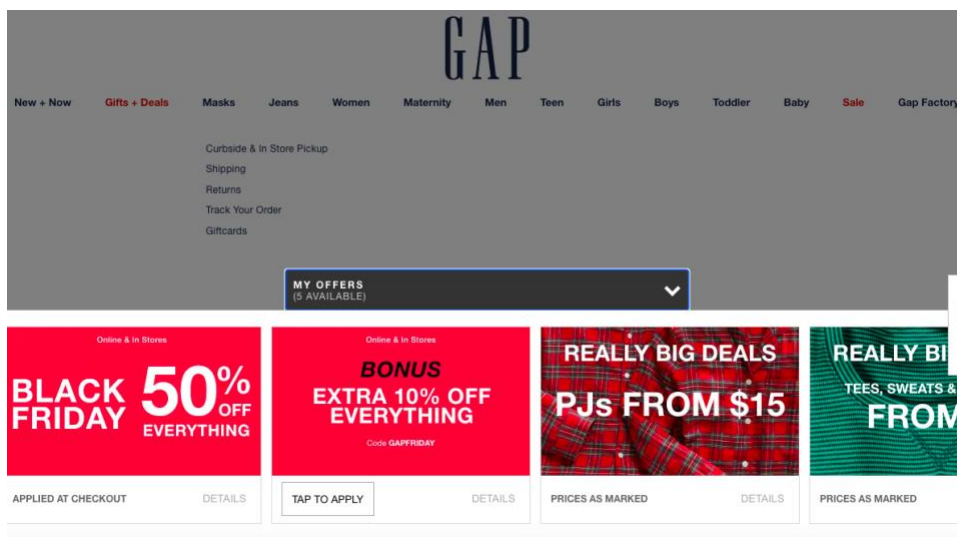
Authorized agents were also given the option to submit the documentation through a one-time sign-in, without creating an account. However, the one-time sign-in portal was broken, and we were unable to submit the documents through that method. We proceeded to create an account, and then LiveRamp sent a confirmation email to finish setting up the account.

Welcome! To continue creating your new account in the Request Portal, please confirm your email.

Confirm Email

Companies are specifically prohibited from requiring consumers to establish an account to exercise their CCPA rights.²⁰ However, after we notified LiveRamp of this issue, they removed the email/password sign-in option. And, further testing revealed that the one-time sign-in is now working correctly.

At Gap.com, pop-up offers for discounts obscure the privacy options at the bottom of the page, including for links to “Do Not Sell My Info,” “Interest Based Ads,” and “Your California Privacy Rights.” Searching the page for “Do Not Sell” using the “find” command provides no results.



Clicking out of the advertising pop-up reveals a “Do Not Sell My Information” link that takes the user to a simple interface that allows consumers to opt out of cookies. Still, this opt out is deficient because the links are hidden below an advertising pop-up. As a result, it places an undue burden on consumers and agents.

Next, Spy Dialer’s online form to submit opt outs is arguably a dark pattern.²¹ The page reached by clicking on Spy Dialer’s “Do Not Sell My Personal Info” link on its homepage prominently

²⁰ Cal. Civ. Code § 1798.135(a)(1); § 1798.185(a)(7).

²¹ Dark patterns are deceptive user interfaces designed to trick consumers into doing something they did not intend to do, such as sharing more information than intended. Harry Brignull, *Dark Patterns: Inside the Interfaces Designed to Trick You*, THE VERGE (Aug. 29, 2013), <https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you>.

features an option to use the “Know and Delete Tool” to submit access and deletion requests. To reach the opt-out form, the user has to identify and click on a small, inconspicuous link in the middle of the same page.

Know and Delete Tool

This will allow you to know and delete your information. After this step, you will also have the option to opt-out future sharing of your information. We do not store or otherwise share the information you provide below, except to complete your request and to log your request as required by law. If you only want to opt-out, [click here](#) for our opt-out tool!

Enter Your Information:

Name and at least one address and/or phone number and/or email address is required.

[Why is this required?](#)

[+ ADD NAME](#)

[+ ADD ADDRESS](#)

[+ ADD PHONE NUMBER](#)

[+ ADD EMAIL ADDRESS](#)

All Done? Click the button below and we will check to see if we have your information!

BACK

KNOW MY DATA

It’s likely that users will not see the opt-out link and will either give up or fill out the access and deletion form.

Consumers seeking opt out directed to access request

In some cases, consumers seeking to opt out were sent to an access request interface. For example, after the agent submitted the opt-out request to Oracle on the consumer’s behalf, the company then sent an email to the authorized agent and the consumer, confirming that the request had been honored with respect to offline direct marketing campaigns. ([Appendix 4E](#)).

In the email, consumers were also provided with a link to opt out of online marketing. But the opt-out link in the email took consumers to a section of the page for access requests, not opt-out requests, ([Appendix 4F](#)) requiring the consumer to scroll up or down on the page to reach the opt out. (When we notified Oracle of the issue, they agreed to fix the link so that it now sends the consumer to the opt-out section of the page.)

Want to see your data?

Oracle empowers you to view the online third-party, interest data associated with your browser, computer, or device.

Download PDF 

Oracle also provides a way to [request a copy](#) of your third-party offline personal data used by the Oracle Data Cloud.

For information about opting out and for other information about our practices, please see the [Oracle Marketing Cloud & Oracle Data Cloud Privacy Policy](#).

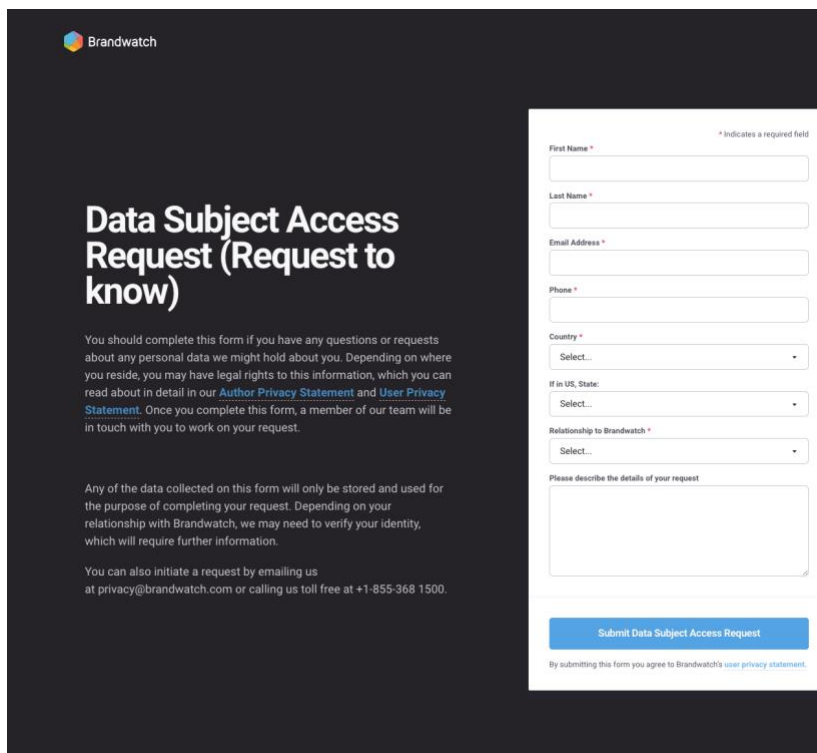
ABOUT ORACLE

[Oracle Data Cloud](#)

RESOURCES

[Opt Out](#)
[Request Your Data](#)
[Privacy Policy](#)

Similarly, following the “Do Not Sell My Personal Data” link on the Brandwatch.com website, or following the link to opt out in Brandwatch’s California data broker registry description, sent the user to a data access request screen. (After we notified Brandwatch of this issue, they updated the page so that it now is clearly marked to allow for both access requests and opt outs.)



The screenshot shows the Brandwatch website's "Data Subject Access Request (Request to know)" form. The form is set against a dark background with white text. On the left, there is a heading and explanatory text. On the right, there is a white form with several input fields and a submit button.

Brandwatch

Data Subject Access Request (Request to know)

You should complete this form if you have any questions or requests about any personal data we might hold about you. Depending on where you reside, you may have legal rights to this information, which you can read about in detail in our [Author Privacy Statement](#) and [User Privacy Statement](#). Once you complete this form, a member of our team will be in touch with you to work on your request.

Any of the data collected on this form will only be stored and used for the purpose of completing your request. Depending on your relationship with Brandwatch, we may need to verify your identity, which will require further information.

You can also initiate a request by emailing us at privacy@brandwatch.com or calling us toll free at +1-855-368 1500.

* Indicates a required field

First Name *

Last Name *

Email Address *

Phone *

Country *

If in US, State:

Relationship to Brandwatch *

Please describe the details of your request

Submit Data Subject Access Request

By submitting this form you agree to Brandwatch's [user privacy statement](#).

Process required consumer involvement

With over 400 firms already registered as data brokers, consumers need intermediaries like authorized agents to make CCPA's rights practical and scalable.²² Spending even five minutes to opt out of each one would take more than 33 hours, which would be an unreasonable burden on any consumer. That's why the authorized agent provisions—especially for opt outs, which pointedly do not require verification—are designed to ensure that the consumer need only provide appropriate authorization to the agent.

However, Home Depot's authorized agent process, for example, required some consumer involvement. After the authorized agent opt-out request was received, the company still sent an email directly to the consumer that required them to confirm the validity of the request within 3 days to begin the opt-out process. ([Appendix 4G](#)) This confused consumers and increased the length of time needed to complete the submission.

Difficulties opting out of cross-context targeted advertising

During the course of the study, we encountered difficulties helping consumers opt out of cross-context targeted advertising. Several companies claimed that they do not “sell” personal information as defined by the CCPA, but their privacy policies revealed that they share personal information with other companies in order to deliver targeted ads. Others noted that they sell information, but directed consumers to voluntary industry opt outs to stop cross-context targeted advertising. Still others considered data sharing for interest-based advertising a sale, and provided an in-house cookie-based opt out for consumers to exercise their preferences—a preferable option, but which still points to limitations in the opt-out based law.

Some companies claim that because data is not necessarily transferred for money, it does not constitute a sale.²³ Or, they have developed service provider relationships in order to deliver targeted advertising outside of the opt out.²⁴ But giving consumers the ability to rein in targeted advertising was a primary goal of the CCPA.²⁵ In 2019, California legislators quickly scuttled a bill, SB 753, designed to provide a wholesale exemption in the CCPA for targeted advertising. The bill analysis cited the objections of CCPA sponsor Californians for Consumer Privacy, which noted that by exempting behavioral advertising, “SB 753 would undermine a major right gained

²² Data Broker Registry, *supra* note 2.

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

²⁴ *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.

²⁵ Confessore, *The Unlikely Activists Who Took On Silicon Valley*, *supra* note 11.

through the passage of the CCPA in 2018.”²⁶ While the CCPA places no limits on websites’ abilities to advertise to their own visitors, it does put limits on the tracking of consumer behavior across the web in exchange for consideration in order to show ads.

For many consumers, behavioral advertising is a serious abuse of their personal privacy. Not only does the widespread collection of data involved in this tracking leave consumers potentially more vulnerable to security breaches and inadvertent disclosure of damaging information, but it also reveals more about consumers than they might want to share with others such as their sexual preferences, health issues, and political activities. It can also perpetuate historic inequalities by facilitating differential pricing²⁷ and allowing companies to target job or housing offers to members of specific groups.²⁸ Finally, most people just don’t want their personal information sold to countless strangers without their knowledge,²⁹ and at the very least companies should be required to honor affirmative efforts to opt out of the ad tech ecosystem.

The companies listed in the chart below claimed that they did not sell personal information, either in correspondence with the authorized agent, or in the privacy policy, but also explained in the privacy policy that they provided information to third parties to deliver interest-based advertising. (Amazon provides a browser-based opt out of targeted advertising, but did not explain this when denying our authorized agent opt-out request on the grounds that they do not sell personal information.)³⁰

²⁶ California SB 753 bill analysis at 10 (Apr. 22, 2019), https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201920200SB753.

²⁷ Big Data and Differential Pricing (Feb. 2015), https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf.

²⁸ Noam Scheiber and Mike Isaac, *Facebook Halts Ad Targeting Cited in Bias Complaints*, N.Y. TIMES (Mar. 19, 2019), <https://www.nytimes.com/2019/03/19/technology/facebook-discrimination-ads.html>.

²⁹ Mary Madden and Lee Rainie, *Americans’ Attitudes About Privacy, Security and Surveillance*, PEW RESEARCH CTR. (May 20, 2015), <https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>; Joseph Turow et al., *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation*, Annenberg School for Communication, University of Pennsylvania (Jun. 2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.


³⁰ In other cases, it was less clear whether companies transferred data to other companies for advertising purposes. For example, Trader Joe’s claims that they do not sell personal information. However, according to their Privacy Policy, they use personal information for “[f]acilitating social sharing[.]” <https://www.traderjoes.com/home/privacy-policy>. Facilitating social sharing likely refers to embedding Instagram (owned by Facebook), Pinterest, and YouTube “share” buttons on their website. If they use the standard Facebook code, this allows for secondary use by those companies, and could constitute sharing for commercial purposes. Allen St. John, *How Facebook Tracks You, Even When You’re Not on Facebook*, CONSUMER REPORTS (April 11, 2018), <https://www.consumerreports.org/privacy/how-facebook-tracks-you-even-when-youre-not-on-facebook/>; Matt Burgess, *How to Stop Instagram from Tracking Everything You Do*, WIRED UK (Jun. 14, 2020), <https://www.wired.com/story/how-to-stop-instagram-from-tracking-everything-you-do/>.

Company	Responses/Privacy Policy Language
<p>Amazon</p>	<p>Response to opt-out submission (Appendix 4H): “Amazon is not in the business of selling our customers’ personal information, as we explain in our Privacy Notice. Our practice of not selling customer personal information extends to all customers, regardless of where they might live or whether they have submitted a request to us.”</p> <p>From Amazon Privacy Notice:</p> <p>“Use of Third-Party Advertising Services: We provide ad companies with information that allows them to serve you with more useful and relevant Amazon ads and to measure their effectiveness. We never share your name or other information that directly identifies you when we do this. Instead, we use an advertising identifier like a cookie or other device identifier. For example, if you have already downloaded one of our apps, we will share your advertising identifier and data about that event so that you will not be served an ad to download the app again. Some ad companies also use this information to serve you relevant ads from other advertisers. You can learn more about how to opt-out of interest-based advertising by going to the Advertising Preferences page.” (The Advertising Preferences page allows consumers to stop “interest based ads provided by Amazon.”)</p>
<p>Airbnb</p>	<p>From Airbnb Privacy Policy Supplements: California and Vermont</p> <p>“We do not sell personal information to third parties. We do allow third parties to collect personal information through the Airbnb Platform and share personal information with third parties for the business purposes described in the Privacy Policy, including without limitation advertising and marketing on the Airbnb Platform and elsewhere based on users’ online activities over time and across Airbnb, services, and devices.”</p>
<p>Intuit</p>	<p>From Intuit Privacy Statement:</p> <p>“Sales of personal information to third parties. We do not and will not sell personal information to third parties. We do share personal information with third-parties for the business purposes described in this Statement....”</p> <p>“Advertising and analytics</p> <p>Intuit may use advertising networks and other providers to display advertising on our Intuit Platform or to manage our advertising on other sites. Our advertising partners may place cookies on unaffiliated websites in order to serve advertisements that may be relevant to you based on your browsing activities and interests and determine the effectiveness of such advertisements. You may be able to opt-out of such interest-based advertising by visiting Digital Advertising Alliance's Network Advertising Initiative's, or Your Online Choices.”</p>

Starbucks	<p>Response to opt-out submission (Appendix 4I): “As referenced in our Privacy Policy, Starbucks does not sell personal information.”</p> <p>From Starbucks Privacy Policy:</p> <p>“To Display Ads for Products or Services – We allow some advertising companies to collect this information in order to display ads that are more relevant to you across your different devices and on our own and others’ websites and mobile apps. Please see the Your Choices section of this Statement for more information about opting out of targeted advertising and controlling the use of cookies, web beacons and other similar technologies.”</p>
------------------	--

The companies in the chart below noted that they sell information, and typically gave consumers the opportunity to opt out of the sale of some information, but directed consumers to an external site to exercise their preferences with respect to interest-based advertising, online behavioral advertising, or other third-party advertising. Even if this method were effective in limiting data sharing, it adds to the complexity of the opt out for consumers, and reveals the limits of the opt-out based law. However, instead of sending consumers to a secondary opt-out portal, companies could have registered the consumer’s preference in their own database in response to the opt out and subsequently not sent the consumer’s personal information to third parties for targeted ads.

Company	Responses/Privacy Policy Language
Comcast	<p>From Comcast, “Interest-Based Advertising”: “Our sites enable cookies and other technologies that comply with the DAA's AdChoices program (see our Cookie Notice). For more information or to opt out of receiving targeted advertising from participating third-party advertisers, click on the Ad Choices icon below. After you opt out, you will still see advertisements, but they may not be as relevant to you.” (See also Appendix 4J for agent correspondence with Comcast).</p>
Clear Channel	<p>From the response to authorized agent opt-out request:</p> <p>“While we do not believe that we sell your personal information in the traditional sense, we and certain business partners may place cookies and other tracking tools on our digital properties, such as websites and mobile applications, which allow us and those companies to gather information about your online activity and serve you interest-based advertising on our websites or elsewhere. This could be considered a “sale” of personal information under the California Consumer Privacy Act (CCPA).” Clear Channel then directed the consumer to the voluntary Digital Advertising Alliance (DAA) and the Network Advertising Initiative (NAI) opt outs. (See Appendix 4K)</p>
Spokeo	<p>From Spokeo’s “Third Party Partners” policy:</p>

	<p>“Further, Spokeo.com may share some of Your Personal Information with third parties who send traffic to Spokeo.com or provide retargeting consumer marketing programs. Such third parties utilize cookies to gather data about Your visit to Spokeo.com and in the delivery of advertisements to You on the various third parties’ partners’ websites....You may opt out of this Display Advertising or customize Your preferences using the Ads Preference Manager or the AdChoices badge in the ads.”</p>
Equifax	<p>From “Equifax Online Behavioral Advertising Notice (US Only)”: “We have partnered with companies that deliver ads for our products on sites that you visit on the web....We comply with the requirements of the Digital Advertising Alliance’s (DAA) Self-Regulatory Program, whose goal is to provide you with enhanced notice about online advertising practices and choices about the ads you see. You can opt out of receiving ads based on your online behavior either by visiting the DAA opt-out page at http://www.aboutads.info/choices/ or by clicking on the Ad-Choices icon in or near the ad.”</p>
AT&T	<p>From “AT&T Privacy Policy”: “Online behavioral advertising: Online behavioral advertising is automated, customized advertising that you see when using online services, like ads in mobile apps or on websites. Those ads are served to you based on inferences about your interests. Those interests are determined from data collected about you, whether by AT&T or other parties.</p> <ul style="list-style-type: none"> • We work with ad companies that may serve ads for us, and for others, across your use of online services. These companies may use cookies, mobile advertising identifiers, and other technologies to collect information about your use of our websites and other websites. This information may be used to, among other things, analyze and track online activities and deliver ads and content tailored to your interests as part of our advertising programs, such as Relevant Advertising. • You can opt-out of online behavioral advertising from companies who participate in the Digital Advertising Alliance by going to their Consumer Choice Page or selecting this icon  when you see it on an online ad.”
Infotracer	<p>Infotracer provides an opt-out process (see Appendix 4L), but its privacy policy also claims that its parent company, Accucom, “does not sell your personal information[,]” and elsewhere in the privacy policy directs users to the Network Advertising Initiative which “offers information about some of the Internet advertising companies we may use, including how to opt-out of interest based advertising they deliver.” (When we notified Infotracer of this, they pointed out that they “currently utiliz[e] only one third-party targeted advertising provider which consumers may opt-out of through NAI,” but they will be ending all third-party targeted advertising in 2021).</p>

The fact that several companies examined in this study directed consumers to voluntary industry opt outs, such as the Digital Advertising Alliance’s, raises concerns. It’s typically not clear to consumers that these are voluntary protocols, not CCPA rights. Further, these separate

and onerous processes are clunky and often broken, don't stop companies' collection or sharing of data, and allow most other uses of data. Since they only apply to companies that choose to participate, the opt out is not comprehensive. And since they are typically based on browser cookies, they can be deleted—the consumer has to take action again if they delete their cookies. Moreover, the process would need to be repeated on each browser or device.³¹

In addition, service provider relationships can be an avenue to share personal information for advertising outside of the CCPA opt out. For example, in [Acxiom's privacy policy](#), they claimed that they disclose personal information to their service providers for a business purpose, including to “programmatic advertising marketplaces/platforms[,]” which would be outside of the CCPA opt out.³²

Cookie-based opt outs

Several companies provided cookie-based solutions for consumers to opt out of the sale of their data for online advertising under the CCPA. While it's preferable to provide a cookie-based opt out than claiming that the CCPA opt out doesn't apply, requiring authentication to opt out, or not providing any in-house option to stop it, it was sometimes onerous and confusing for consumers. This points to problems with the opt-out based law, where often it is difficult to strike the right balance between ease of opt out and efficacy.

Home Depot, for example, confirmed that they stopped the sale of some information pursuant to the authorized agent request, and additionally directed the consumer to visit their website, submit an opt-out request there, and receive a cookie on their browser to stop online advertising, or “Digital Sales.” ([Appendix 4M](#)). Neustar offered a cookie-based opt out for online data. They also provided the opportunity to submit online identifiers—such as IP address and cookie IDs—to process the opt out, though obtaining those identifiers would be challenging for many consumers. ([Appendix 4N](#)). Merkle provides a cookie-based opt out for “certain uses of information in a digital environment,” including interest-based advertising.³³ And LiveRamp includes a cookie-based opt out for targeted advertising (in addition to separate Mobile Opt-outs and a Permanent Opt-Out for information associated with name and email address).³⁴

³¹ *Statement of Justin Brookman Director, Privacy and Technology Policy Consumers Union Before the House Subcommittee on Digital Commerce and Consumer Protection*, Understanding the Digital Advertising Ecosystem at 11-12 (June 14, 2018), <https://advocacy.consumerreports.org/wp-content/uploads/2019/07/Brookman-Testimony-June-14-2018.pdf>; *Statement of Justin Brookman Director, Consumer Privacy Center for Democracy & Technology Before the U.S. Senate Committee on Commerce, Science, and Transportation*, A Status Update on the Development of Voluntary Do-Not-Track Standards at 3 (April 24, 2013), <https://cdt.org/wp-content/uploads/pdfs/Brookman-DNT-Testimony.pdf>.

³² Acxiom, US Products Privacy Notice (Dec. 22, 2020), <https://www.acxiom.com/about-us/privacy/highlights-for-us-products-privacy-policy/#ccpa>.

³³ Merkle, Data Product Privacy Notice, (last updated Jan. 1, 2020), <https://www.merkleinc.com/getting-know-your-privacy-rights/privacy-notice>.

³⁴ LiveRamp, Your Data, Your Rights, https://your-rights.liveramp.com/templates/optout_individual.html.

Inadequate opt-out notice and communication

Companies often did not provide adequate information in response to authorized agent submissions. For example, some companies simply didn't respond to agent requests submitted through standard opt-out channels. And some companies never directly confirmed whether the opt-out request would be honored.

Under the CCPA and implementing regulations, companies are not required to provide notice of receipt of an opt-out request, nor are they required to provide notice if and when the request has been honored, but they are required to at least provide notice if the request is declined.³⁵ Some companies may be violating the law by denying requests without providing notification, but we have no way of knowing—it's also possible that the company has honored the request but just not notified us. The AG should clarify these notice requirements so that agents and consumers know whether their privacy rights are being respected.

Companies' poor compliance with notice requirements and other communication issues posed significant challenges for authorized agents. While the CCPA requires companies to explain in their privacy policies how an authorized agent may submit a request on a consumer's behalf, several failed to include that provision in their disclosures.³⁶

Moreover, some customer service agents were unable to give the authorized agent direction in how to properly submit a request. This often had the effect of making it difficult or impossible for us to submit a request. Companies are required by the CCPA to be able to give consumers, and by extension agents, proper direction in making requests.³⁷

No response

Several companies provided no response to opt-out requests submitted through the standard opt-out channels (though some ultimately responded to support requests, acknowledging receipt of the request). We still have not received any confirmation that the requests have been honored or denied.

Spy Dialer. Though we submitted "Do Not Sell" requests through the designated online interactive form, we never heard back in regard to any support request or privacy-related form submitted through Spy Dialer's website.

Equifax. We sent opt-out requests via email to Equifax's customer care email address on October 22, and followed up on the requests with additional emails: one to the same email address, and one to a different customer service email address, on November 9. (Submitting an opt-out request through the consumer online portal is not an option for authorized agents, since

³⁵ Cal. Code Regs. tit. 11 § 999.315(g).

³⁶ *Id.* at § 999.308(c)(5)(a).

³⁷ Cal. Civ. Code § 1798.135(3).

it requires identity verification via text message). While we ultimately received an email indicating that Equifax received the request for support we sent on November 9, we have received no further communications to date. Equifax may well have honored the request, but we have not received confirmation.

Comcast. Comcast sent us seven notices in response to seven opt-out requests. (For example, see [Appendix 4J](#)). However, neither we nor the consumers received responses to additional opt-out requests submitted on behalf of three other consumers. Without a confirmation note, the agent has no idea whether the opt out was effective or whether further action is required to process the request. (Follow-up correspondence indicated that, though the requests were sent, Comcast does not have a record of the three opt outs referenced here and were therefore likely not processed).

Refusal to correspond

Intuit. We sent our authorized agent opt-out request to PrivacyOfficer_@intuit.com as it was the only North America privacy contact email we could find listed. Intuit responded that this was the incorrect channel for the request, did not provide a different email contact for the request, and expressly warned, “We will not respond to any further emails coming directly from datarightsstudy@cr.org.” A follow-up call to the phone number provided in the email also failed to elicit any information about submitting CCPA requests. See [Appendix 4C](#) for the full correspondence.

Disclosures fail to outline authorized agent process

Companies are required to explain in their privacy policies how an authorized agent may submit a request on the consumer’s behalf. However, only 16 out of the 21 companies examined in this project included any mention of the authorized agent in their disclosures.³⁸ Without knowing whether a request was submitted through the appropriate channels, it is difficult for the agent to tell whether it would be honored, especially since companies aren’t required to (and sometimes did not) provide confirmation that it had been.

Opt-out request processed as deletion request

One Airbnb customer service agent handled one of our authorized agent opt-out requests as a deletion request. In response to this opt-out request, the company responded: “I’ve forwarded your inquiry to a member of my team who can better assist you. Please feel free to add any additional information to this email, and we’ll be in touch with you soon.” ([Appendix 4O](#)). The outlier opt out was then incorrectly handled as a delete request, which kicked off an additional

³⁸ The companies that mentioned authorized agent processes in their disclosures were: Acxiom, Airbnb, AT&T, Brandwatch, ClearChannel, LiveRamp, Equifax, Gap, Home Depot, Intuit, Merkle, Neustar, Sovrn, Spokeo, Spydialer, and Starbucks. The companies that did not mention authorized agent processes in their disclosures were Amazon, Comcast, Infotracer, Oracle, and Trader Joe’s. Screenshots of disclosures are on file with the authors.

verification flow requiring the consumer to submit a proof of her identity, and thankfully was caught by the consumer soon thereafter. ([Appendix 4P](#))

V. Recommendations

Ineffective opt outs posed challenges to consumers and the authorized agents seeking to opt out on their behalf. The AG should aggressively enforce the CCPA to hold accountable the companies that avoid the CCPA and its implementing rules, and to incentivize other companies to comply. In addition, the AG should issue additional rules to help make the authorized agent work as intended. Without the authorized agent as an effective option for exercising privacy rights, consumers are much less likely to be able to fully protect their privacy.

The AG should hold companies accountable when they violate the law.

The AG needs to hold companies accountable for failure to comply with the CCPA's authorized agent provisions. Without a viable authorized agent option, consumers could be left to navigate complicated processes or interfaces in order to exercise their California privacy rights themselves. Enforcement will help ensure that companies work harder to make sure that they have appropriate agent flows.

The AG should also step in when customer service isn't effective, and should consider directing enforcement resources to encourage better training in this area.

The AG should clarify that data shared for cross-context targeted advertising is a sale, and tighten the restrictions on service providers.

Many 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.³⁹ While the newly-passed California Privacy Rights Act will largely address these loopholes, these provisions will not go into effect until January 1, 2023.⁴⁰ Thus, the AG should exercise its broad authority to issue rules to clarify that the transfer of data between unrelated companies for any commercial purpose falls under the definition of sale.⁴¹

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

³⁹ Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously—The Attorney General Needs To Act* (Jan. 9, 2020), CONSUMER REPORTS DIGITAL LAB AT MEDIUM, <https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb>.

⁴⁰ The California Privacy Rights Act, Sec. 31(a).

⁴¹ Cal Civ. Code § 1798.185(a)(2).

to perform certain limited services on its behalf.⁴² 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.

The AG should prohibit dark patterns as outlined in the Third Set of Proposed Modifications.

We appreciate that the AG has proposed to “require minimal steps to allow the consumer to opt-out” and to prohibit dark patterns, “a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer’s choice to opt-out[.]” in the Third Set of Proposed Modifications to the CCPA Regulations.⁴³ This proposal should be finalized as quickly as possible. This is essential, given the difficulties that authorized agents and consumers have experienced in attempting to stop the sale of their information, as demonstrated in the study.

The AG should require companies to notify agents when the opt-out request has been received and when it has been honored.

Too often, the company provided no information on whether or not the opt-out request had been honored. While the CCPA rules require companies to notify consumers if an opt-out request has been rejected, there is no requirement to provide notice of receipt, or notice of confirmation—nor is there guidance on how to respond to opt-out requests when the company does not possess the consumer’s data. The authorized agent was, in some cases, unable to explain to the consumer whether or not the opt-out process had been completed.

To ensure that the authorized agent service is effective, companies must be required to provide notification upon receipt and completion of the opt-out request. Required notification is also important for compliance purposes. For example, the regulations require companies to comply with opt outs within 15 business days. Without providing adequate notification, there’s no way to judge whether or not the company has honored the law and to hold them accountable if not.

Further, if the company does sell consumers’ personal information, but does not have personal information about the consumer who is the subject of the request, the company should be required to notify the agent that the request has been received, and that the company will honor the opt out if and when they do collect the consumer’s data.

In the case of an agent opt out, the notification should go to the agent. Otherwise, the consumer could end up getting emails from hundreds, if not thousands, of different companies.

⁴² IAB CCPA Compliance Framework for Publishers & Technology Companies, *supra* note 24.

⁴³ California Attorney General, California Consumer Privacy Act Regulations, Text of Modified Regulations at §999.315(h)(1)-(5) (Oct. 12, 2020), <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-third-set-mod-101220.pdf>.

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

The regulations provide helpful guidance with respect to consumer access and deletion requests, which ensures that even if a consumer inadvertently submits a request incorrectly, there is a process in place to help them submit it properly.

If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either: (1) Treat the request as if it had been submitted in accordance with the business’s designated manner, or (2) Provide the consumer with information on how to submit the request or remedy any deficiencies with the request, if applicable.⁴⁴

The AG should clarify that this guidance applies to all authorized agent-submitted requests as well.

VI. Conclusion

The “authorized agent” provision is a crucial tool to make it more practical for consumers to exercise their privacy rights under the CCPA. It provides a great opportunity to help consumers take control of their privacy, and this study has shown that consumers are interested in leveraging its benefits. Unfortunately, too many companies have made it difficult, if not impossible, for agents and consumers to submit opt-out requests. The AG should enforce companies’ compliance with the law so that the authorized agent provisions work as intended. Moreover, the AG should promulgate additional common-sense rules to make sure that opt outs are simple and effective, even when submitted by an authorized agent.

⁴⁴ Cal. Code Regs. tit. 11 § 999.312(e).

VII. Appendix

2A: Companies selected for CR authorized agent pilot

1. Acxiom
2. Airbnb
3. Amazon
4. AT&T
5. Brandwatch ([formerly](#) Crimson Hexagon, Inc.)
6. Clear Channel
7. Comcast
8. Equifax
9. Gap
10. Home Depot
11. Infotracer
12. Intuit
13. LiveRamp
14. Merkle Inc.
15. Neustar, Inc.
16. Oracle
17. Sovrn, Inc.
18. Spokeo, Inc.
19. Spy Dialer, Inc. dba SpyDialer.com
20. Starbucks
21. Trader Joe's

2B: [Industry Outreach Email for CR Authorized Agent DNS](#)

2C: [Opt-Out Request from Consumer Reports Authorized Agent](#)

2D: [Sample Opt-Out Request](#)

4A: [Acxiom Opt-Out Correspondence](#)

4B: [Acxiom Opt Outs by Mail](#)

4C: [Intuit Opt-Out Response](#)

4D: [Intuit Privacy Question Form](#)

4E: [Oracle Opt-Out Response](#)

4F: [Oracle Opt-Out Portal Links To Download Registry](#)

4G: [Home Depot Identity Verification](#)

- 4H: [Amazon Opt-Out Response](#)
- 4I: [Starbucks Opt-Out Response](#)
- 4J: [Comcast Opt Out Response for Non-Customers](#)
- 4K: [Clear Channel Opt-Out Response](#)
- 4L: [Infotracer Opt-Out Response](#)
- 4M: [Home Depot Opt-Out Confirmation](#)
- 4N: [Neustar Opt-Out Response](#)
- 4O: [Airbnb Inconsistent Opt-Out Response](#)
- 4P: [Airbnb Mistaken Opt-Out Verification](#)