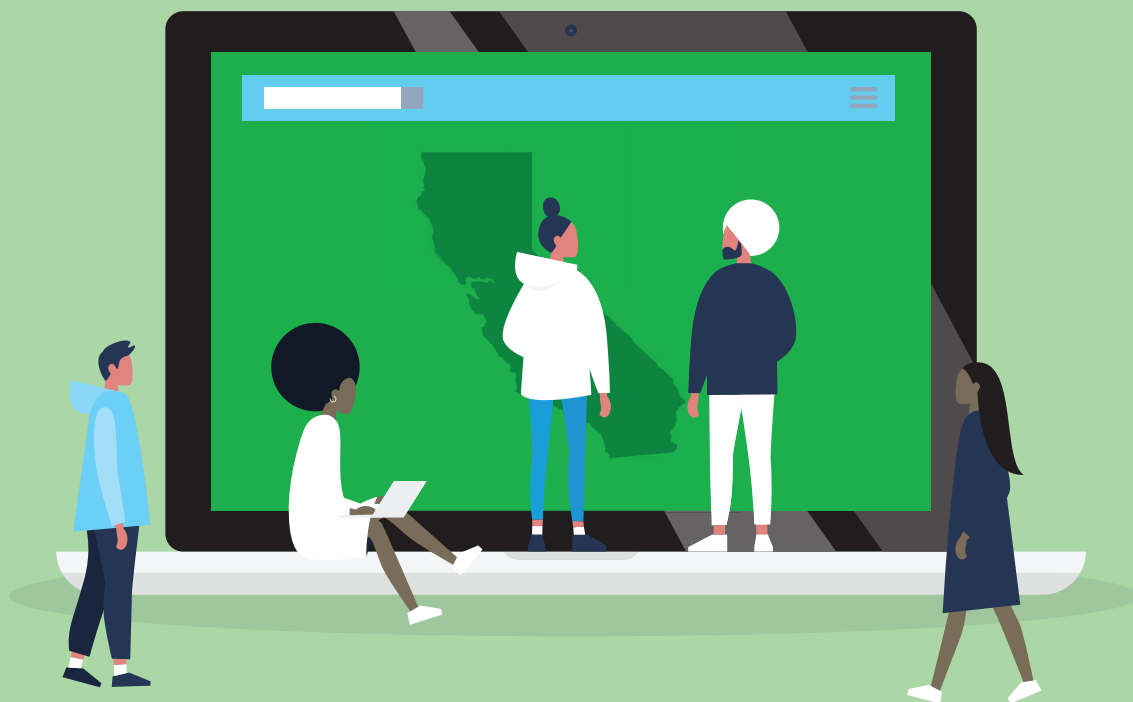




California Consumer Privacy Act: Are Consumers' Digital Rights Protected?

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.¹ As part of the study, 543 California residents made DNS requests to 234 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 primarily 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.

¹ Cal. Civ. Code § 1798.135(a)(1).

* On May 13, 2021, the Executive Summary was updated to note that requests were sent to a total of 234 data brokers, not 214.

- 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

*On May 13, 2021, the Findings were updated to clarify that the follow-up research that revealed that at least 24 data brokers did not have a DNS link was primarily focused on, but not limited to, the sites in which all three testers failed to find a DNS link.

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.² 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.³ Early surveys suggested that some companies were dragging their feet in getting ready for the CCPA.⁴ 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.⁵ 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,⁶

² 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>.

³ 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/.

⁴ *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 (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.”)

⁵ 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>

⁶ *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.⁷ 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.⁸ For example, with respect to opt outs, the regulations clarify how long the companies have to respond to opt-out requests⁹ and outline the notices that need to be provided to consumers.¹⁰ On August 14, 2020, the AG regulations went into effect.¹¹ The CCPA directs the AG to develop regulations as needed to implement the CCPA, consistent with its privacy intent,¹² and the AG has signaled that they plan to continue to consider a number of issues with respect to opt outs.¹³

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,¹⁴ the AG has had the authority to begin enforcement since July 1, 2020.¹⁵ Already, the AG's staff has notified companies of potential violations of the CCPA.¹⁶

⁷ 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/>.

⁸ Cal. Civ. Code § 1798.185(a).

⁹ Cal. Code Regs. tit. 11 § 999.315(e) (2020).

¹⁰ *Id.* at § 999.304-308.

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

¹² Cal. Civ. Code § 1798.185(b)(2).

¹³ 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/>.

¹⁴ 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>.

¹⁵ Cal. Civ. Code § 1798.185(c).

¹⁶ 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.¹⁷ 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)¹⁸—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,¹⁹ intended to capture data that is shared with third parties for behavioral advertising purposes.²⁰

¹⁷ Cal. Civ. Code § 1798.120(a).

¹⁸ *Id.* at § 1798.140(o)(1).

¹⁹ *Id.* at § 1798.140(t)(1).

²⁰ California Senate Judiciary Committee, SB 753 Bill Analysis at 10 (Apr. 22, 2019), 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.²¹ 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.²² In contrast, for opt outs, verification is not required.²³ Importantly, companies may not use the information provided by the opting out consumer for any other purpose.²⁴ The CCPA also directs the AG to design and implement a “Do Not Sell” button to make it easier for consumers to opt out.²⁵

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.²⁶ (The AG declined to finalize a design to serve as an opt-out button.)²⁷ 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.²⁸ Companies must honor consumers' requests to opt out within 15 business days²⁹ (in contrast to 45 days for deletion and access requests).³⁰

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.”

²¹ Cal. Civ. Code § 1798.135(a)(1).

²² *Id.* at § 1798.140(y).

²³ *Id.* at § 1798.135.

²⁴ *Id.* at § 1798.135(a)(6).

²⁵ *Id.* at § 1798.185(a)(4)(C).

²⁶ Cal. Code Regs. tit. 11 § 999.315(a) (2020).

²⁷ 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].

²⁸ *Id.* at § 999.315(g).

²⁹ *Id.* at § 999.315(e).

³⁰ 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,³¹ which lists companies that sell California consumers' personal information to third parties, but do not have a direct relationship with the consumer.³² 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.³³

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.³⁴ 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.³⁵ 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

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

³² Cal. Civ. Code § 1798.99.80(d).

³³ 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>.

³⁴ DATA BROKER REGISTRY, *supra* note 31.

³⁵ *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.³⁶ The information collected can even provide insight whether a consumer is subject to certain diseases, such as diabetes, or other insights into health status.³⁷ 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.³⁸

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

³⁶ *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>.

³⁷ *Id.* at 25.

³⁸ *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.

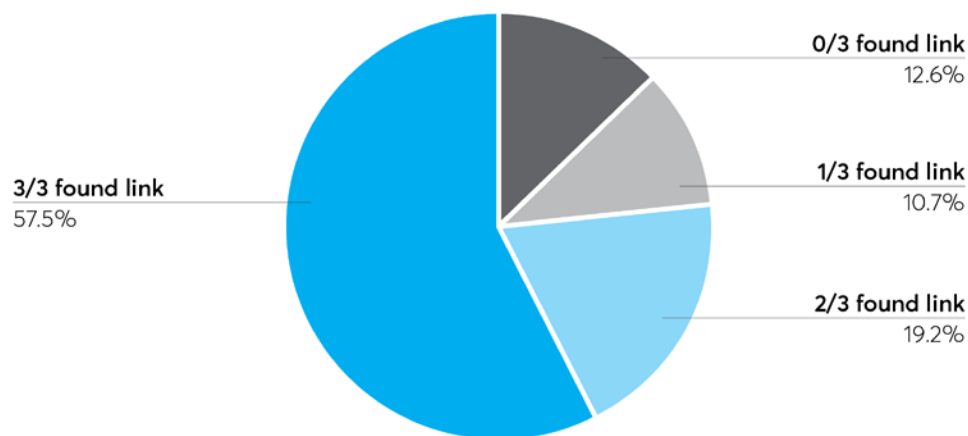
Findings

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.³⁹ 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.”⁴⁰ [emphasis added] The definitions of “sell,” “third parties,”

³⁹ Cal. Civ. Code §1798.99.82.

⁴⁰ *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.⁴¹

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.”⁴²

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.”⁴³ The CCPA clarifies that “homepage” indeed means “the introductory page of an internet website and any internet web page where personal information is collected.”⁴⁴ 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.”⁴⁵

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

⁴¹ *Id.* at § 1798.99.80(e)-(g).

⁴² 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”].

⁴³ Cal. Civ. Code § 1798.135(a)(1).

⁴⁴ *Id.* at § 1798.140(l).

⁴⁵ FSOR Appendix, *supra* note 42, Response #105.

California consumers and not the homepage made available to the public generally.”⁴⁶ 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.⁴⁷

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

⁴⁶ Cal. Civ. Code § 1798.135(b).

⁴⁷ 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."⁴⁸ 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 primarily focused 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).^{49*} 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,⁵⁰ this means that unless a consumer is familiar with the CCPA or

⁴⁸ Cal. Civ. Code § 1798.135(a)(3).

⁴⁹ 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.

* On May 13, 2021, the report was updated to clarify that this follow-up research was primarily focused on, but not limited to, the sites in which all three testers failed to find a DNS link.

⁵⁰ 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.**

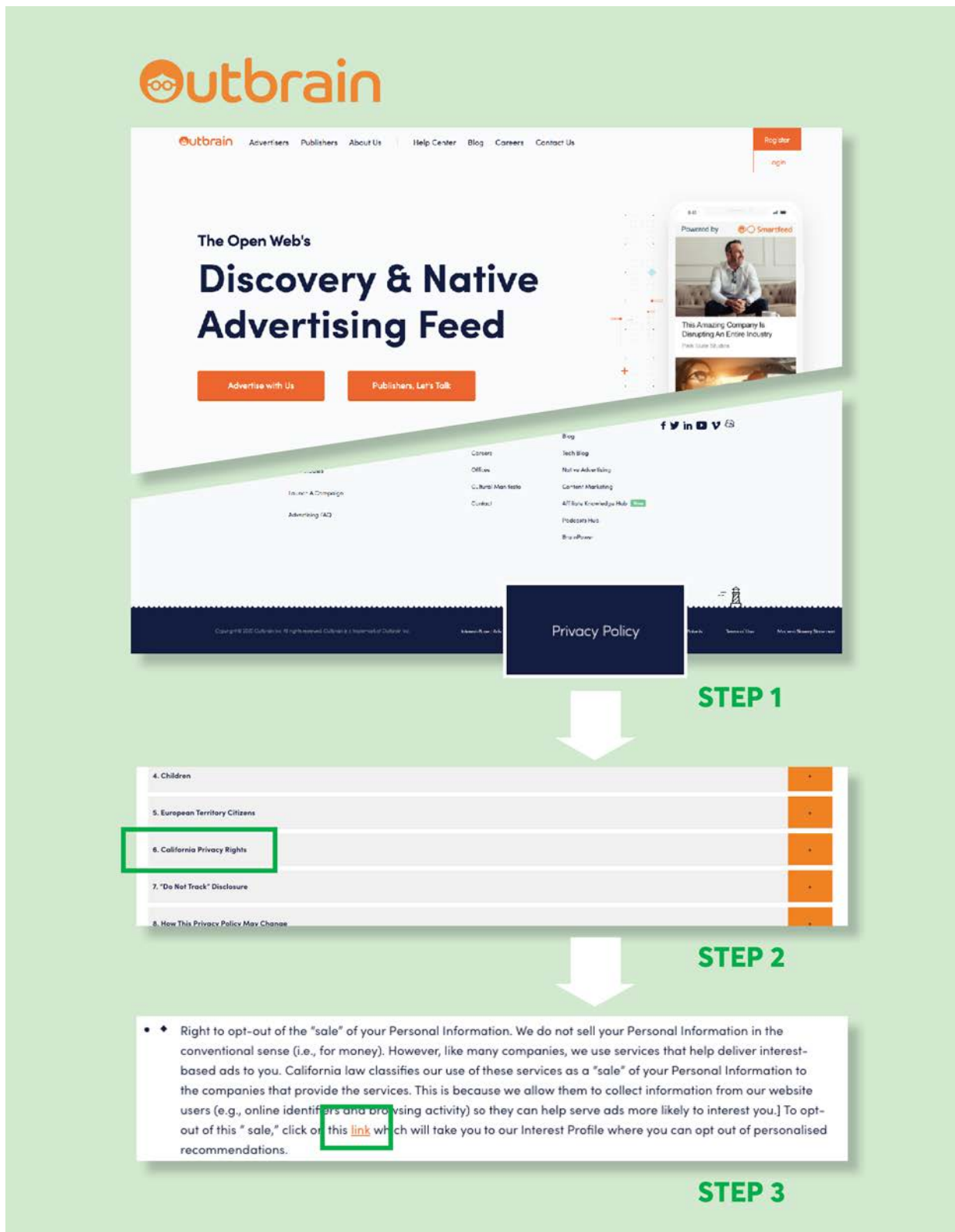
Clicking on "California Privacy Rights" opens up a text box **STEP 3**, that includes a bullet on the "Right to opt-out of the 'sale' of your Personal Information." That section includes a very small hyperlink to "opt out of personalised recommendations."

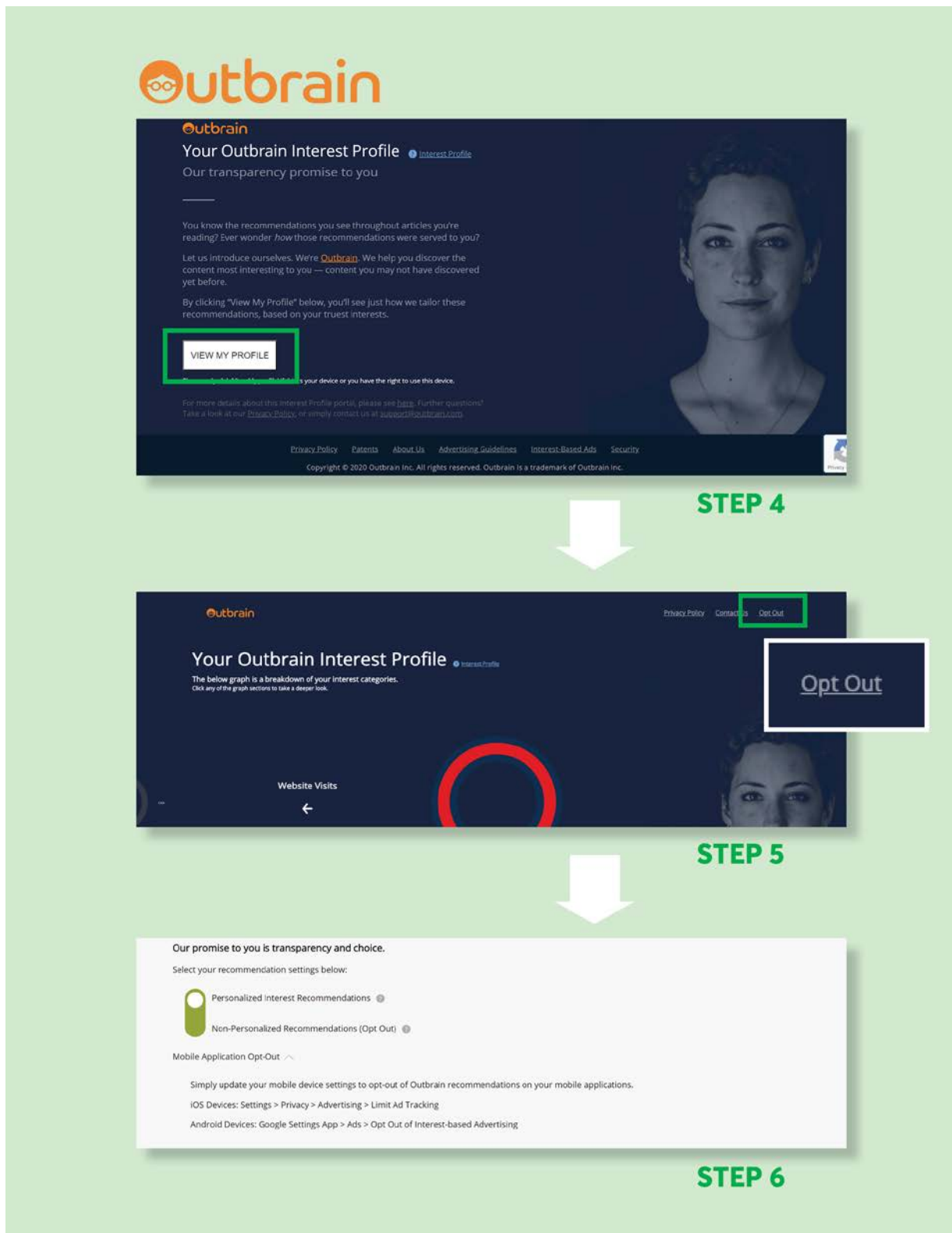
Clicking on that link takes the consumer to another to a page titled "Your Outbrain Interest Profile," **STEP 4.** (The consumer can also reach this page by clicking on "Interest-Based Ads" on the homepage.)

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."⁵¹ (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).⁵² For example, all three testers failed to find the Do Not Sell link for the data broker Freckle I.O.T. Ltd./PlaceIQ. 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).

⁵¹ Cal. Code Regs. tit. 11 § 999.315(a) (2020).

⁵² These companies are: AcademixDirect, Inc., Fifty Technology Ltd, Freckle I.O.T. Ltd./PlaceIQ, 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.

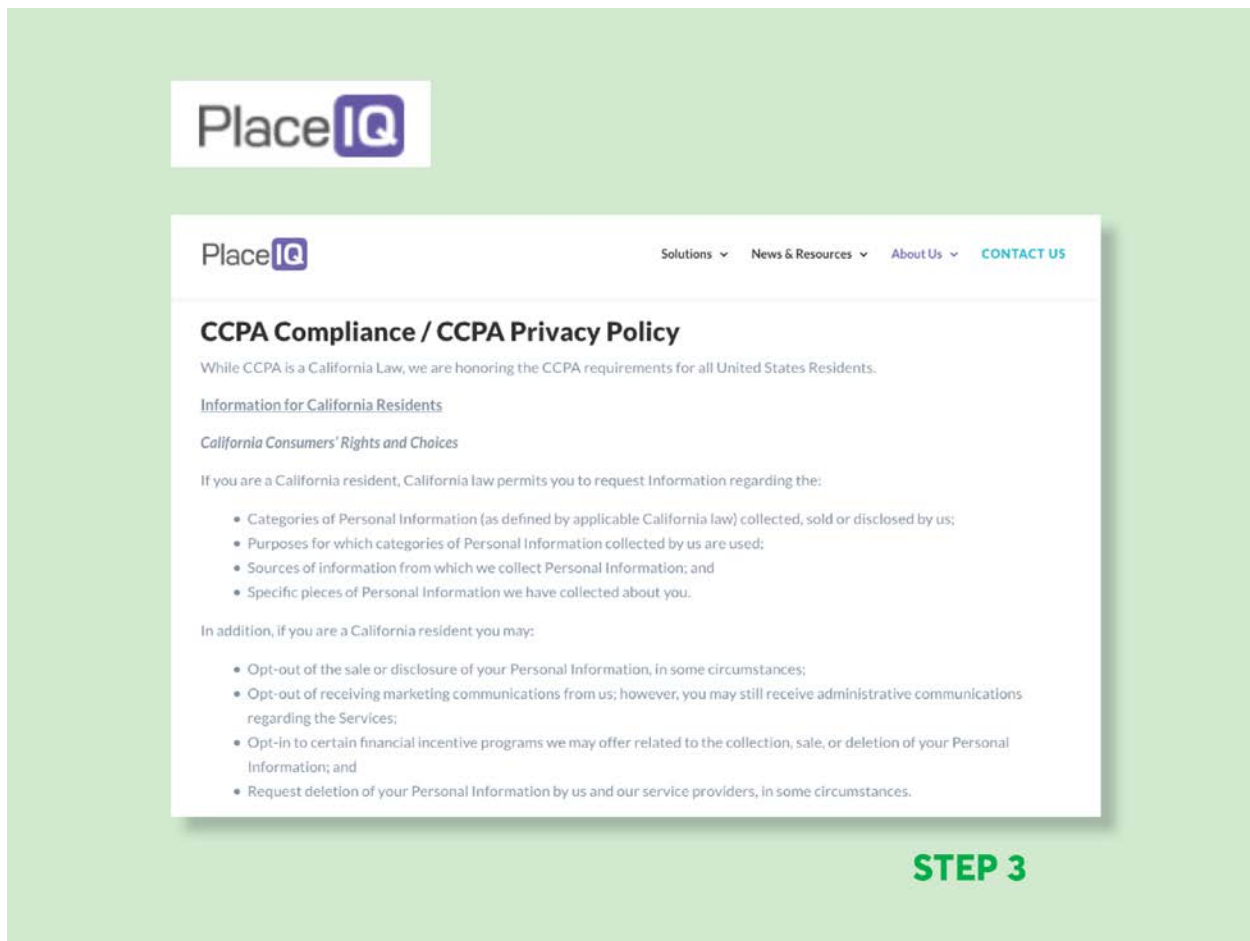
California Consumer Privacy Act: Are Consumers' Digital Rights Protected?

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

STEP 1: A callout box labeled "Allow cookies" points to the "Allow cookies" button on the website's cookie banner.

STEP 2: A callout box labeled "Consumer Options: Privacy Policy, CCPA & Do Not Sell" points to the "CCPA & Do Not Sell" link in the "Consumer Options" section of the website's footer.

The background image shows the PlaceIQ website interface, including the header with navigation links (Solutions, News & Resources, About Us, CONTACT US), a hero section with a COVID-19 research announcement, a section about location intelligence, a partner section (Data Cloud, Experian, comscore, MARKETING EVOLUTION), a cookie banner, and a footer with various links and contact information.



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 email⁵³—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./PlaceIQ 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./PlaceIQ 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?”

⁵³ 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

Advertisers

Publishers

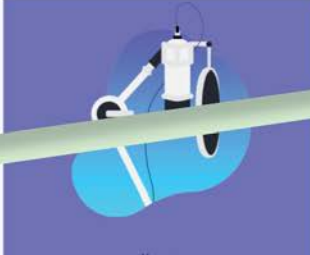
About

Press

Log in

Contact us

Modern podcast technology for publishers and advertisers.



I'm an

I'm a

Do not sell my personal information

By using this site, you agree to the use of cookies by Megaphone and our partners to provide the best experience, analyze site use and deliver advertising. [Privacy Policy](#)

Close

Do not sell my personal information

Close

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

CR | Digital Lab

25

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.⁵⁴

⁵⁴ 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,

* On May 13, 2021, this chart was corrected to note that the number of requests to send or receive email were 209, not 204; and that several consumers were asked to “Provide a selfie,” not “Provide a profile.”

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 several sections:

- A section with three 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." with input fields for: First Name, Last name, Phone, Mobile Phone, Email, Address, Address2, City, State (a dropdown menu currently showing "CA"), and ZIP/Postal Code.
- A section 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". This entire section is highlighted with a green rectangular box.
- A blue "Submit" button at the bottom.

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

⁵⁵ 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 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.

the answer company
THOMSON REUTERS

THOMSON REUTERS

In order to protect your privacy, before fulfilling your request, we will need to verify your identity. Follow the instructions below to verify your identity. We will only use this data to verify your identity and will delete the data as soon as the transaction is completed. Once your identity has been verified, you will receive an email from Thomson Reuters explaining next steps.

Drivers License *
Please capture via mobile device
Status: Incomplete

Facial Similarity Snapshot *
Please capture via mobile device
Status: Incomplete

Mobile phone *
(201) 555-0123

Continue on Mobile

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.⁵⁶ 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.

⁵⁶ *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.⁵⁷ 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.

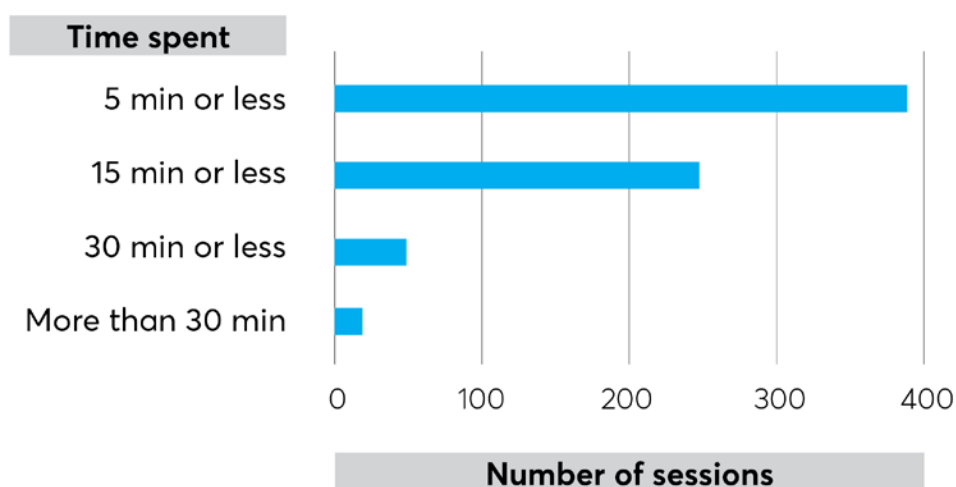
We also asked consumers about how long they spent to complete a request, and to not include the time spent filling out the survey. While the vast majority of consumers spent less than 15 minutes at a time on requests—and the most common amount of time was less than 5 minutes—some consumers reported that 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

⁵⁷ 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.⁵⁸ They reported being unable to proceed with their request in another 7% of tests.⁵⁹ These 14% of cases represent a DNS process clearly failing to support a consumer's CCPA rights.

⁵⁸ 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. . .”

⁵⁹ 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.⁶⁰

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

⁶⁰ 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.⁶¹ 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.”⁶² X-Mode also sells personal information to third party applications and websites.⁶³ 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.⁶⁴ Because it sells such sensitive information, X-Mode should be particularly careful to protect the anonymity of consumer data and respect consumers’ privacy preferences.

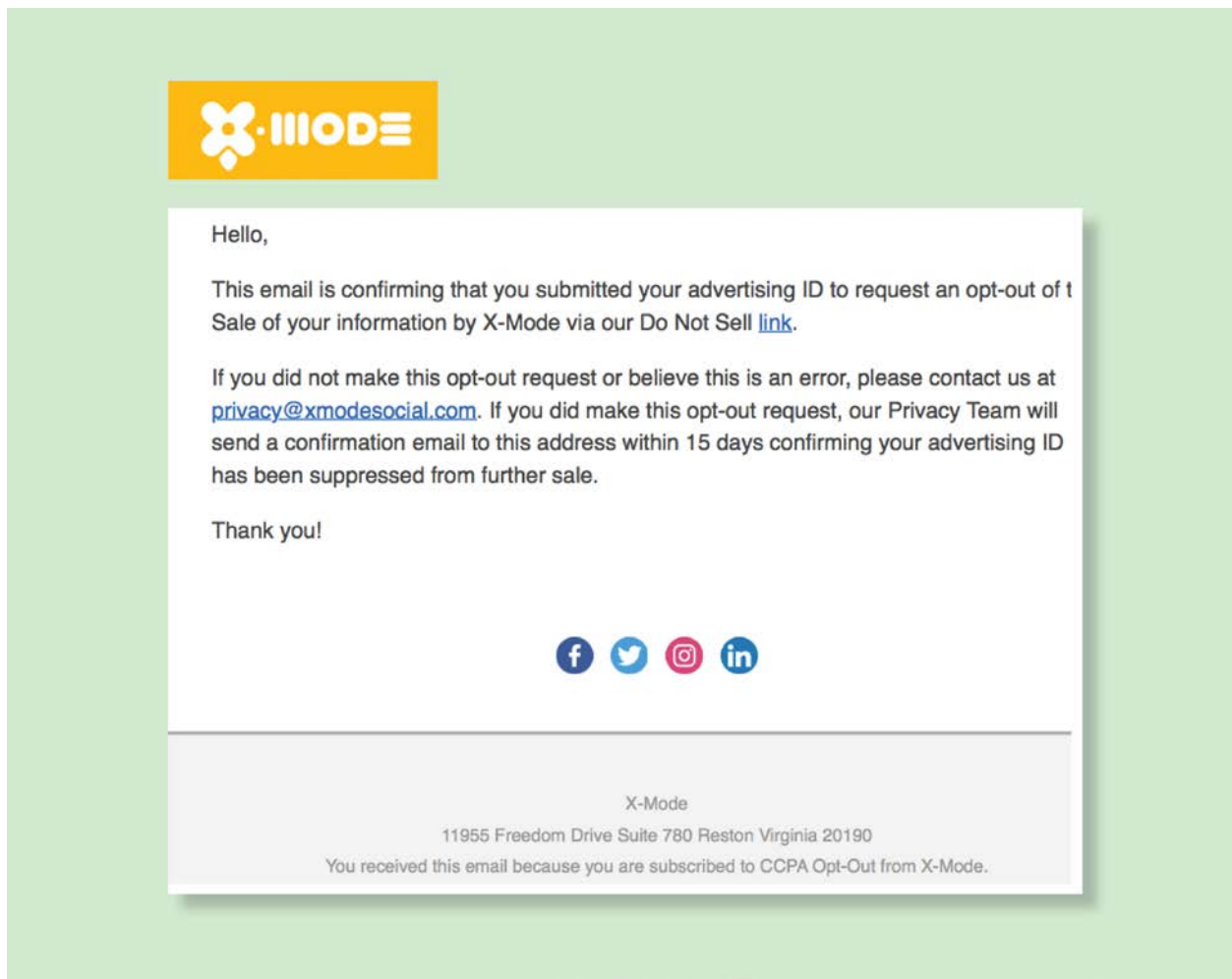
After submitting the opt-out request in April 2020, the author received the following email confirming that she had been placed on an “CCPA Opt-out” mailing list:

⁶¹ 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>.

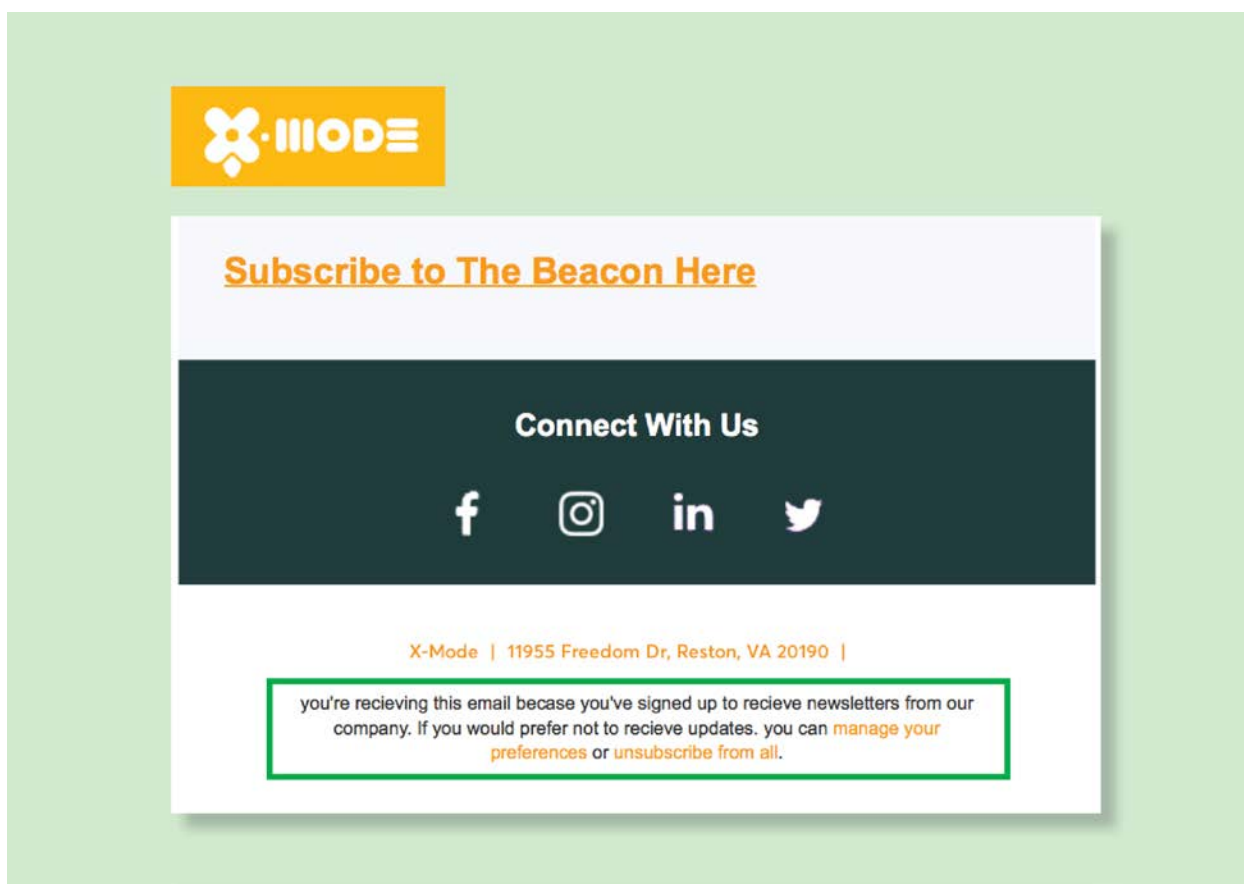
⁶² Jake Ellenburg, quoted in Karuga Koinange, *How Drunk Mode, An App for the Inebriated, Became Data Location Company X-Mode Social*, TECHNICALLY (Feb. 27, 2020), <https://technical.ly/dc/2020/02/27/how-drunk-mode-app-became-data-location-company-x-mode-social/>.

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

⁶⁴ 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.

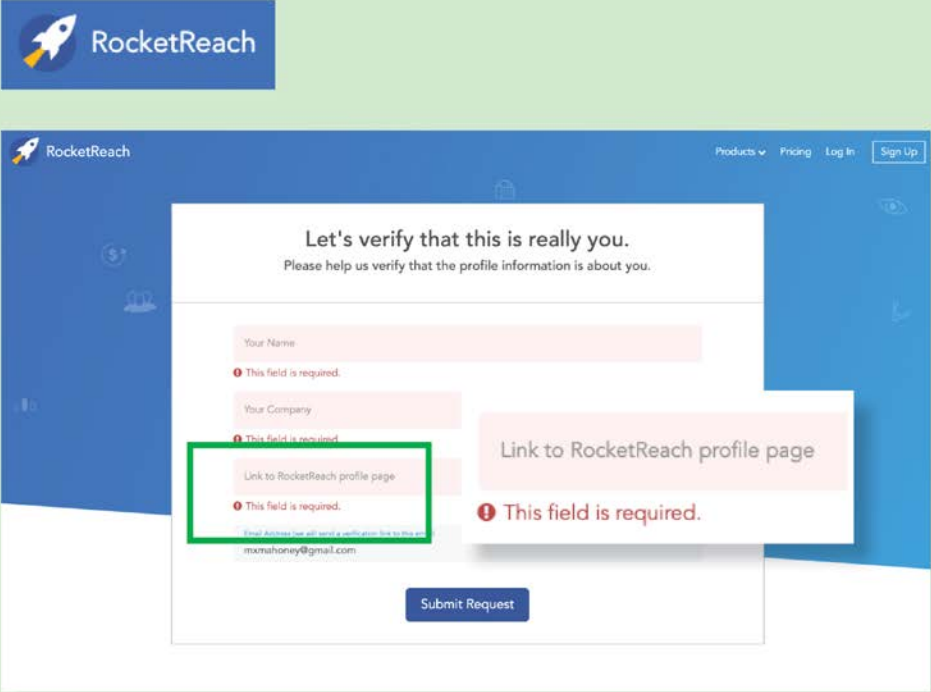


Since the only interaction that the author has had with X-Mode was to opt out—by definition, data brokers do not have relationships with consumers—the only way that she could have “signed up” was through opting out of the sale of her information. This behavior violates the CCPA’s prohibition on reuse 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.⁶⁵ 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: "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 is a light green gradient.

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

⁶⁵ 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);⁶⁶
- 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

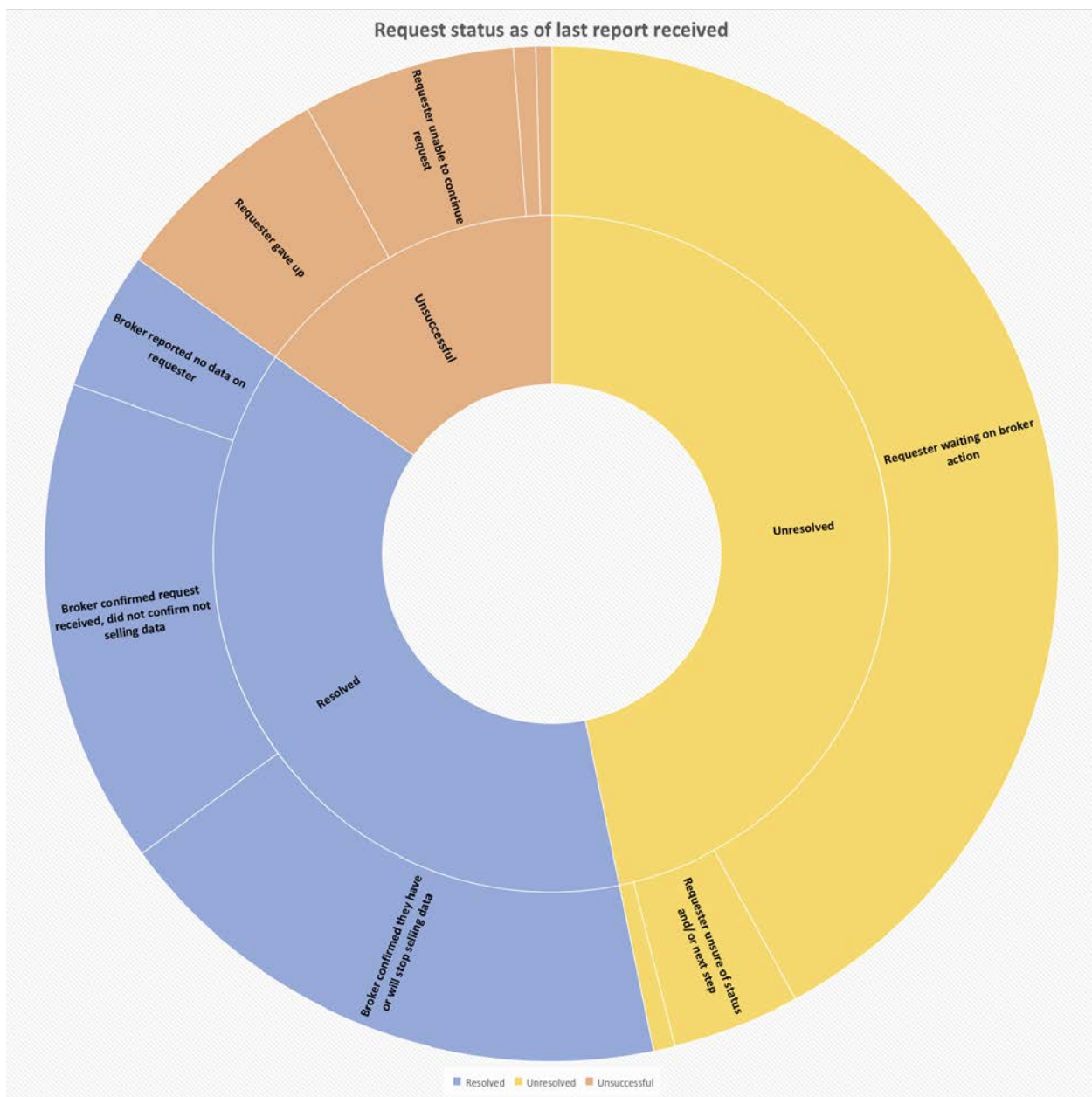
⁶⁶ Testers' references to “Do Not Contact” likely refer to consumers' right to be added to a company's internal “Do Not Call” list under the Telemarketing Sales Rule, 16 CFR § 310.4(b)(1)(iii)(A). Do Not Track refers to a request to stop tracking information about a consumer's activity across multiple 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

* Some responses did not include enough data to categorize, and were not included in the chart (Note added May 13, 2021).



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.

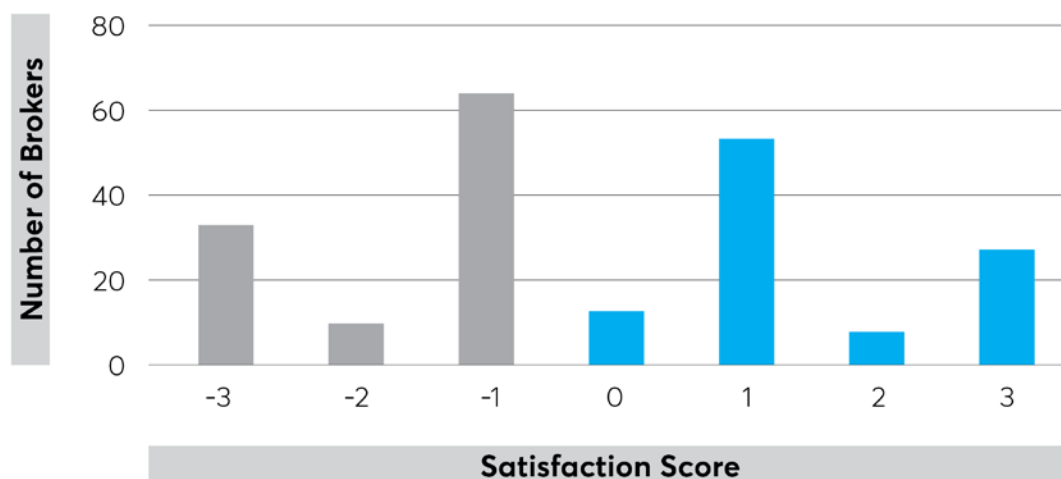
About 52% of the time, the tester was “somewhat dissatisfied” or “very dissatisfied” with opt-out processes.

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.⁶⁷

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.

⁶⁷ 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,⁶⁸ 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.⁶⁹ 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

⁶⁸ Cal. Civ. Code § 1798.155(b).

⁶⁹ 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.”⁷⁰ 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.”⁷¹ 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.

⁷⁰ Cal. Civ. Code § 1798.185(a)(4)(C).

⁷¹ 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.⁷² 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.⁷³ 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.

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

⁷³ 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; 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.⁷⁴ 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.

⁷⁴ 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

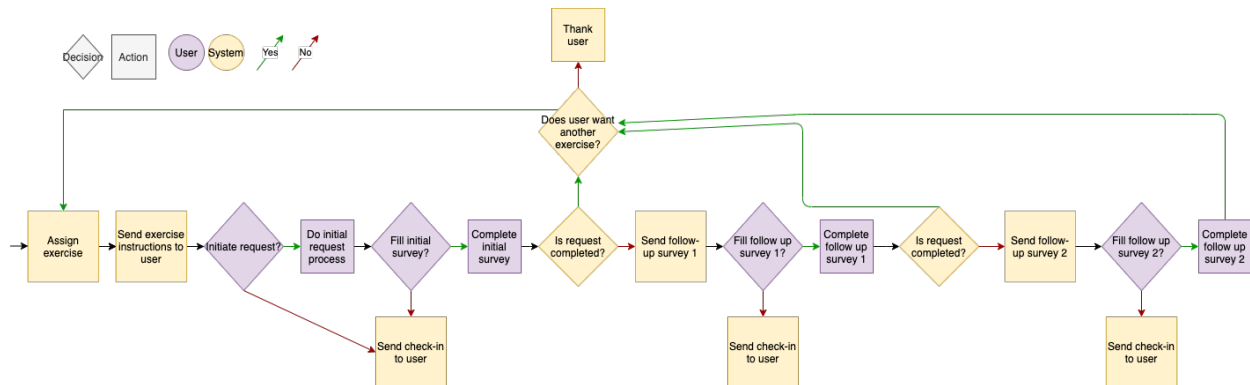
Overall, we found that consumers were too often dissatisfied with CCPA opt-out processes. This study uncovered some cases where the DNS process was short, clear, and satisfactory. It also found that some companies aren't complying with the CCPA, and that consumers were often left frustrated and without 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.⁷⁵

⁷⁵ 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 1, Social Catfish LLC 2](#)
[Spectrum Mailing Lists](#)
[SRAX, Inc.](#)
[USADATA, Inc.](#)
[zeotap GmbH](#)

* On December 3, 2020, we replaced the screenshots for LeadsMarket, Social Catfish, and SRAX to provide a clearer view of the entire homepage.

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./PlaceIQ](#)

[Marketing Information Specialists, Inc.](#)

[Media Source Solutions](#)