December 23, 2020

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

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

Dear Ms. Kim,

Consumer Reports[1] appreciates the opportunity to comment on the Fourth Set of Modifications to the CCPA Regulations.[2] We thank the California Attorney General's office (AG) for proposing new regulations to help to make the CCPA work better for consumers. Though the California Consumer Privacy Act (CCPA) is designed to protect consumer privacy, Consumer Reports has found that some consumers ran into difficulties when attempting to opt out of the sale of their information under the CCPA.[3] The new proposed rules will help address some—though not all—of these problems. To better ensure that consumers are able to exercise their privacy rights, we reiterate our comments submitted in response to the Third Set of Modifications (attached),[4] and additionally, recommend that the AG:

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

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

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

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

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

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

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

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

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

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

[5] Cal. Civ. Code §1798.135(a)(1).

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

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

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

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

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

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

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

---

[7] Lorrie Faith Cranor et al., *CCPA Opt-Out Icon Testing - Phase 2* at 2, 23 (May 28, 2020), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/dns-icon-study-report-052822020.pdf.
[8] Text of Modified Regulations, *supra* note 2, at §999.306(f)(1)-(3).
[9] See, eg, @JulesPolonetsky, Twitter (Dec. 10, 2020), https://twitter.com/JulesPolonetsky/status/1337116699548667907.
[10] Cal. Civ. Code § 1798.185(a)(4)(C).

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

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

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

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

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

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

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

---

[11] Cal. Civ. Code § 1798.135(a)(1); § 1798.185(a)(7).
[12] Ginny Fahs, *Putting the CCPA into Practice: Piloting a CR Authorized Agent*, Digital Lab at Consumer Reports (Oct. 19, 2020), https://medium.com/cr-digital-lab/putting-the-ccpa-into-practice-piloting-a-cr-authorized-agent-7301a72ca9f8.
[13] Cal. Code Regs. tit. 11 § 999.308(c)(5) (2020).
[14] *Id.* at 999.312(e).

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

Conclusion

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

Respectfully submitted,

Maureen Mahoney
Policy Analyst

Attachment

[15] Consumer Reports Comments on the Third Set of Modification to Proposed Regulations Implementing the California Consumer Privacy Act, *supra* note 4, at 7.
[16] *Id.* at 8-9.
[17] See, California Privacy Rights Act, § 1798.120(a); § 1798.140(e)(6), https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.
[18] *Id.* at § 1798.185(d).

October 28, 2020

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

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

Dear Ms. Kim,

Consumer Reports[1] appreciates the opportunity to submit comments in response to the Notice of the Third Set of Modifications to Proposed Regulations Implementing the California Consumer Privacy Act.[2] We welcome these proposed changes, especially those prohibiting the use of dark patterns—methods that substantially interfere with consumers' efforts to opt out of the sale of their information.[3] Consumer Reports has recently documented that some consumers are finding it very difficult to opt out of the sale of their information.[4] In our recent study, over 500 consumers submitted opt-out requests to companies listed on the California data broker registry. Many of them encountered challenges: opt-out links too often were missing from the home page or difficult to find; opt-out processes were unnecessarily complicated, and companies asked consumers to submit sensitive information to verify their identities. In response, consumers sent over 5,000 messages to the AG, urging him to step up enforcement efforts and close up

[1] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.
[2] California Attorney General, California Consumer Privacy Act Regulations, Text of Modified Regulations (Oct. 12, 2020), https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-third-set-mod-101220.pdf.
[3] *Id.* at §999.315(h)(1)-(5).
[4] Maureen Mahoney, *California Consumer Privacy Act: Are Consumers' Rights Protected?*, CONSUMER REPORTS (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf.

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

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

Below, we explain these points in more detail.

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

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

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

[5] § 999.315(h).
[6] *Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy*, NORWEGIAN CONSUMER COUNCIL (Jun. 27, 2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.
[7] Mathur, Arunesh and Acar, Gunes and Friedman, Michael and Lucherini, Elena and Mayer, Jonathan and Chetty, Marshini and Narayanan, Arvind, *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, Proc. ACM Hum.-Comput. Interact. (2019), https://webtransparency.cs.princeton.edu/dark-patterns/.

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

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

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

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

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

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

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

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

[13] § 999.315(h)(1).

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

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

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

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

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

[14] § 999.315(h)(4).

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

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

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

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

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

[15] § 999.315(h)(5).
[16] ACBJ (last visited Oct. 28, 2020), https://acbj.com/privacy#X.
[17] Cal. Civ. Code § 1798.185(a)(4)(C).

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

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

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

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

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

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

[18] Ginny Fahs, *Putting the CCPA Into Practice: Piloting a CR Authorized Agent*, DIGITAL LAB AT CONSUMER REPORTS (Oct. 19, 2020), https://medium.com/cr-digital-lab/putting-the-ccpa-into-practice-piloting-a-cr-authorized-agent-7301a72ca9f8.
[19] § 999.326(b)

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

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

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

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

> "Sale" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's

[20] § 999.315(g)
[21] Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously—The Attorney General Needs to Act*, DIGITAL LAB AT CONSUMER REPORTS (Jan. 9, 2020), https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb.
[22] Spotify, "Additional California Privacy Disclosures," (July 1, 2020), https://www.spotify.com/us/legal/california-privacy-disclosure/?language=en&country=us; Amazon.com Privacy Notice," (January 1, 2020), https://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496&ref_=footer_privacy#GUID-8966E75F-9B92-4A2B-BFD5-967D57513A40__SECTION_FE2374D302994717AB1A8CE585E7E8BE.
[23] Tim Peterson, *'We're Not Going to Play Around': Ad Industry Grapples with California's Ambiguous Privacy Law*, DIGIDAY (Dec. 9, 2019), https://digiday.com/marketing/not-going-play-around-ad-industry-grapples-californias-ambiguous-privacy-law/.
[24] Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley—And Won*, N.Y. TIMES (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html; Cal. Civ. Code § 1798.140(o); Cal. Civ. Code § 1798.140(t).
[25] Cal. Civ. Code § 1798.185(a).

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

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

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

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

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

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

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

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

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

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

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

---

[27] Chris Hoofnagle, *Facebook and Google Are the New Data Brokers* (Dec. 2018), https://hoofnagle.berkeley.edu/wp-content/uploads/2018/12/hoofnagle_facebook_google_data_brokers.pdf.
[28] Cal. Civ. Code §§ 1798.125(a)(2) and .125(b).
[29] *Id.* at § 1798.125(b)(4).
[30] *Id.* at § 1798.185(a)(6).
[31] Jon Brodkin, *AT&T To End Targeted Ads Program, Give All Users Lowest Available Price*, ARS TECHNICA (Sept. 30, 2016), https://arstechnica.com/information-technology/2016/09/att-to-end-targeted-ads-program-give-all-users-lowest-available-price/.
[32] *Too Much of a Good Thing*, THE ECONOMIST (March 26, 2016), https://www.economist.com/briefing/2016/03/26/too-much-of-a-good-thing.
[33] *FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets*, Fed. Trade Comm'n (Feb. 26, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology.

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

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

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

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

Additionally, it would be helpful to provide guidance outside of the rule that signals such as the Global Privacy Control—a new, CR-supported effort to create a "Do Not Sell" browser signal[36]—are likely to be considered binding in the future.

Conclusion

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

[34] § 999.315(c).
[35] Lara O'Reilly, *Apple's Latest iPhone Software Update Will Make It A Lot Harder for Advertisers to Track You,* BUS. INSIDER (Sept. 10, 2016), http://www.businessinsider.com/apple-ios10-limit-ad-tracking-setting-2016-9.
[36] Press release, *Announcing Global Privacy Control: Making it Easy for Consumers to Exercise Their Privacy Rights,* Global Privacy Control (Oct. 7, 2020), https://globalprivacycontrol.org/press-release/20201007.html.

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

Respectfully submitted,

Maureen Mahoney
Policy Analyst
Consumer Reports