March 26, 2020

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

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

Consumer Reports[1] thanks the California Attorney General's office (AG) for the opportunity to comment on its second set of modifications to the proposed rules implementing the California Consumer Privacy Act (CCPA).[2] As consumers shift to working from home and spending even more of their time online in light of the COVID-19 crisis, now more than ever, they need baseline protections to protect their privacy and security. We appreciate that the AG has improved upon the previous draft rules, particularly by eliminating the exemption for IP addresses from the definition of personal information.[3] But other steps, such as a new provision that could allow service providers to build profiles to deliver targeted advertising, undermine existing protections.[4] We reiterate the requests from our previous comments, particularly to close targeted advertising loopholes by strengthening the definitions of sale and service provider, and to further limit pay-for-privacy;[5] and additionally call on the AG to:

- Deny the request from industry to delay enforcement of the CCPA;
- Maintain a strong, inclusive definition of personal information;

[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 (Feb. 25, 2020), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-redline-020720.pdf.
[3] § 999.302(a).
[4] § 999.314(c)(3).
[5] See, Consumer Reports Comments on Modified Proposed Rules Implementing the California Consumer Privacy Act (CCPA) (Feb. 25, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/02/CR-CCPA-Comments-2.25.20-FINAL.pdf.

- Ensure that Do Not Track signals are honored as opt-out requests;
- Tighten up service provider language; and
- Set up an appeals process for responses to access requests.

Companies are seeking to evade the letter and the spirit of the CCPA, and to avoid any punishment for doing so. By sending a clear message that companies need to respect the CCPA, the AG can better protect consumers' constitutional right to privacy.

The AG should deny the request from industry to delay enforcement of the CCPA.

The AG should reject the cynical attempt by many industry groups to use the recent coronavirus crisis to evade their responsibilities under the law. Dozens of companies and industry trade groups requested that the AG delay enforcement of the CCPA to January 2021.[6] This latest effort to avoid compliance with the CCPA comes as more and more consumers work from home, increasingly relying on online communications to work, stay in communication with healthcare professionals, and obtain access to necessary supplies. It is critical for policymakers to ensure fairness, safety, and transparency for consumers in the marketplace. Industry shouldn't exploit the health crisis to ignore consumer requests to companies to stop selling their data.

This most recent letter is just the latest in a series of attempts to evade the CCPA. Last year, industry supported a raft of bills to gut the CCPA. Thanks to the efforts of several legislators, the worst bills failed to advance. Lawmakers also held the line against a last-minute wave of lobbying from industry groups such as the California Chamber of Commerce and the Internet Association, which sought to introduce amendments to exempt additional consumer information from the law.[7] Though the CCPA went into effect in January, many companies have avoided complying with the law.[8] In late January, advertising groups also called on the AG to delay the effective date of the CCPA until January 2021.[9]

[6] Association of National Advertisers et al, Request for Temporary Forbearance from CCPA Enforcement (March 17, 2020), https://www.law360.com/articles/1255181/attachments/0.
[7] Consumer Reports et al., *Joint news release: 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/.
[8] Maureen Mahoney, *Many companies are not taking the California Consumer Privacy Act seriously—the attorney general needs to act* (Jan. 9, 2020), https://medium.com/cr-digital-lab/companies-are-not-taking-the-california-consumer-privacy-act-seriously-dcb1d06128bb.
[9] 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.

Companies making a good faith effort to comply with the CCPA have nothing to fear. Compliance should be fairly straightforward—access, deletion, and opt-out of sale. Companies that don't collect and retain unnecessary data, and those that don't sell consumers' data, should have very little difficulty in complying. Unfortunately, even those not making a good faith effort may find themselves off the hook, due to weak enforcement provisions in the CCPA. The AG enforcement section includes a "right to cure" provision that ties the AG's hands from taking action if the company "cures" the violation in 30 days,[10] meaning that the AG can spend months building a case against a company that is flagrantly violating the law, only to find that it goes nowhere. Further, once a consumer's privacy has been violated by unauthorized disclosure of information, there's no way to cure the damage. On top of that, the California Attorney General has limited resources to protect the privacy of 40 million Californians; earlier, the AG's office noted that they only have the enforcement capabilities to bring a few cases per year.[11]

Consumers shouldn't lose their right to privacy in a crisis. As tech companies work to create new solutions to address the scarcity of health services, consumers need baseline protections for that data more than ever. For example, a Google subsidiary, Verily, has launched a new service in two counties in California to help consumers determine whether or not coronavirus testing is appropriate.[12] While they're offering a good service, there should be some reasonable limits on what they do with the data, as consumers are very vulnerable at this time.[13]

Consumers working from home need protections too. Well before this most recent crisis, about 43% of Americans spent at least some time working from home.[14] Now, many more have joined them, and are relying on their internet service providers, Google platforms, and teleconferencing services to work, communicate with co-workers, and order office, medical, and sanitizing supplies. In fact, due to these societal shifts, tech companies are expected to profit financially from this crisis.[15] In light of the recent health crisis, Consumer Reports recently examined teleconferencing service Zoom's privacy policies, and found that, while Zoom isn't necessarily doing anything objectionable with consumer data, its privacy policy gives the company a lot of leeway to share details about the calls, including instant messages and the names of participants,

---

[10] Cal. Civ. Code §1798.155(b).
[11] Yuri Nagano, *California Attorney General Plans Few Privacy Law Enforcement Actions, Telling Consumers to Take Violators to Court*, SAN FRANCISCO PUBLIC PRESS (May 15, 2019), https://sfpublicpress.org/news/2019-05/california-attorney-general-plans-few-privacy-law-enforcements-telling-consumers-to-tak.
[12] Julia Carrie Wong, *Google's Coronavirus Testing Website Arrives – With Serious Privacy Concerns*, THE GUARDIAN (Mar. 16, 2020), https://www.theguardian.com/us-news/2020/mar/16/coronavirus-testing-website-trump-promised-verily.
[13] Katie McInnis, *Privacy Concerns Raised by Verily's Baseline COVID-19 Pilot Program*, CONSUMER REPORTS, (Mar. 23, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/03/Consumer-Reports-letter-to-Verily-Alphabet-3.23.20.pdf.
[14] Niraj Chokshi, *Out of the Office: More People Are Working Remotely, Survey Finds*, N.Y. TIMES (Feb. 15, 2017), https://www.nytimes.com/2017/02/15/us/remote-workers-work-from-home.html.
[15] Daisuke Wakabayashi et al., *Big Tech Could Emerge From Coronavirus Crisis Stronger Than Ever*, N.Y. TIMES (Mar. 23, 2020), https://www.nytimes.com/2020/03/23/technology/coronavirus-facebook-amazon-youtube.html.

with third parties, even for advertising.[16] Consumers are transmitting sensitive information through these channels, and without the CCPA, they have next to no protection over the sale of that data. The AG should reject industry's request to throw out basic consumer protections in response to the crisis.

The AG should maintain a strong, inclusive definition of personal information.

We thank the AG for deleting the provision in the first revised proposed rules, § 999.302(a), that would have removed IP addresses from the definition of personal information. While information that can't be tied to a single, identifiable person should not necessarily be subject to access or deletion requests, particularly without controls to ensure that one's search terms are being shared with another person, if companies are using that data to target ads, it's identifiable and eliminating it from the definition of personal information is contrary to the clear language of the statute.[17] Consumers should retain opt-out rights in this case. IP addresses are explicitly included in the CCPA's definition of personal information,[18] and to remove them would clearly subvert legislative intent. Deleting this provision properly closed up a potential new loophole for targeted advertising. We urge you to not reinsert the provision or weaken the definition of personal information in any way.

IP addresses, even though they appear to be "anonymous," allow companies to access a significant amount of data about consumers and their families. While IP addresses assigned to consumers are often *dynamic* (in that they are periodically rotated), these numbers may in practice not be changed for months at a time; and as companies migrate to IPv6 addresses, there may be no need to rotate IP addresses at all as IPv6 effectively eliminates the problem of address scarcity. It can easily be used to track user behavior over time, even without access to cookies or other identifiers.[19] Moreover, correlation of IP addresses allows companies to engage in cross-device tracking, as devices that share local networks are considerably more likely to be operated by the same persons—meaning that they're used to develop detailed profiles about consumers, across devices, and about those with whom they live and spend time, for ad targeting purposes.[20] Currently, the CCPA gives consumers the right to opt out of its sale to third parties, but removing IP address from the definition of personal information would rescind this right.

---

[16] Allen St. John, *Zoom Calls Aren't as Private as You May Think. Here's What You Should Know*, CONSUMER REPORTS (Mar. 24, 2020), https://www.consumerreports.org/telecommunications/zoom-teleconferencing-privacy-concerns/.
[17] Cal. Civ. Code §1798.140(o)(1)(A).
[18] *Id.*
[19] Dennis Hartman, *The Advantages & Disadvantages to a Static IP Address*, TECHWALLA (last visited March 7, 2019), https://www.techwalla.com/articles/the-advantages-disadvantages-to-a-static-ip-address.
[20] *Cross-Device Tracking: An FTC Staff Report*, FED. TRADE COMM'N at 3 (Jan. 2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf.

The AG should ensure that Do Not Track signals are honored as opt-out requests.

We appreciate that the AG has kept the requirement that companies must honor browser privacy signals as an opt-out of sale.[21] Forcing consumers to opt out of every company, one by one—including from data brokers, whom consumers may not even know are collecting their data—is simply not workable. However, the current draft 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.

First, the AG should make it explicit in the rules that enabling Do Not Track opts the consumer out of the sale of their information. Instead, the updated draft regulations require browser signals to clearly convey that it constitutes an opt-out of sale.[22] This language unduly restricts consumer agency, particularly because it would mean that signing up for Do Not Track—likely the most well-known privacy setting, at one time adopted by Safari, Internet Explorer, Chrome, and Firefox—would not opt consumers out of sale.[23] Consumers would reasonably expect that enabling Do Not Track would opt them out of sale to third parties. This would mean that consumers already using DNT—by one estimate, nearly a quarter of American adults—would be much less likely to benefit from the AG rule, since they would likely assume that they had already opted out of sale.[24] Currently, major web browsers do not have comparable CCPA-specific settings, and we are unaware of any concrete plans to offer them in the near future. If companies can ignore DNT and similar requests, consumers may have no scalable way to opt out of data sales across the hundreds of sites and apps with which they interact.

Do Not Track was developed in response to consumer outcry over the fact that cookies enabled companies to track consumers' behavior across the web.[25] While it makes sense that a company would be able to view a consumers' activity on its own site, consumers would not reasonably expect that a company could also see what they were doing on other sites as they searched the Internet. It is precisely this type of transfer of data between first parties and third parties over which the CCPA attempts to give consumers control. It is a reasonable assumption that a consumer signing up for DNT would be opting out of sale to third parties.

---

[21] § 999.315(d).
[22] § 999.315(d)(1).
[23] Glenn Fleishman, *How the Tragic Death of Do Not Track Ruined the Web for Everyone*, FAST COMPANY (Mar. 17, 2019), https://www.fastcompany.com/90308068/how-the-tragic-death-of-do-not-track-ruined-the-web-for-everyone. While it is true that in 2012, Microsoft enabled DNT in its Internet Explorer browser by default, that was discontinued in 2015 following sustained criticism.
[24] Kashmir Hill, *'Do Not Track,' the Privacy Tool Used by Millions of People, Doesn't Do Anything*, Gizmodo (Oct. 15, 2018), https://gizmodo.com/do-not-track-the-privacy-tool-used-by-millions-of-peop-1828868324.
[25] Electronic Frontier Foundation, Do Not Track (last visited Mar. 23, 2020), https://www.eff.org/issues/do-not-track.

But DNT isn't the only platform-level privacy setting governing third-party sharing. 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.[26] 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.

The AG should tighten up guardrails on use of data by service providers.

The AG should clarify that when the consumer has opted out of the sale of their information, data cannot be shared—even with a service provider—to target advertising on another site or service. We appreciate that the AG has kept the proposed § 999.314(d), which provides that "A service provider shall not sell data on behalf of a business when a consumer has opted-out of the sale of their personal information with the business." Nevertheless, the language should be tightened further, especially since many companies incorrectly claim that the data-sharing engaged in for targeted advertising purposes is not a sale.[27] 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

[26] 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.
[27] 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/.

> than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

The AG should also delete the new proposed language in § 999.314(c)(3), which explicitly allows service providers to build profiles for its own purposes. Given that many companies are already exploiting vagueness in the CCPA to claim a service provider exemption to deliver targeted advertising outside of the consumer opt-out, this new language could significantly undermine the CCPA by allowing service providers to use browsing, geolocation, dating app activity, and health data to derive detailed insights into consumers' lives and to better target ads on their own and potentially others' sites. Service providers shouldn't have the right to create profiles with its customers' data for its own unrelated purposes. Unless this language is tightened, companies could interpret this language as carte blanche to deliver targeted advertising in spite of an opt-out.

The AG should set up an appeals process for access requests.

Companies have an unfair advantage in deciding whether or not to honor access requests, because it's not always easy for consumers to tell whether or not the company has fully complied. Especially in light of the many confusing exemptions, it's difficult for a consumer to know whether a company has released all of the covered information it has collected about them—or whether their exemption claim is legitimate. For example, at least one company, Airbnb, has claimed a trade secret exemption for not releasing consumer data. To address this, the AG should set up a process for appealing access decisions.

Consumers may suspect that a company hasn't been fully forthcoming—for example, the *Washington Post* noted that Uber only released the data involved in some of their interactions with the company:

> [R]equests under the new law reveal huge variance in the data the companies disclose. Uber reveals a customer's rating, but doesn't disclose some customer service calls, users' ratings of drivers or any inferences about its users that help shape its business decisions. The company also maintains other data undisclosed in CCPA requests, according to people familiar with the matter, such as whether a credit card is corporate or personal.[28]

Employees of Consumer Reports have also run into problems in attempting to access their data. When a journalist at Consumer Reports recently sought to access their personal information from Airbnb, the company claimed an exemption based on intellectual property grounds:

[28] Greg Bensinger, *So Far, Under California's New Privacy Law, Firms are Disclosing Too Little Data — Or Far Too Much*, WASH. POST (Jan. 21, 2020), https://www.washingtonpost.com/technology/2020/01/21/ccpa-transparency/.

Airbnb takes its responsibilities for privacy and data protection very seriously. For example, so as not to adversely affect the rights and freedoms of others, we have not included some information where the inclusion would adversely affect intellectual property or other rights, or the data protection rights of third parties.

Trade secrets have the potential to be a significant exemption, since a company could potentially try to exempt any information that they've submitted to processing on intellectual property grounds. The CCPA itself does not provide a trade secret exemption but instead directs the AG to develop rules.[29]

In addition, Epsilon couldn't provide the requestor with information because it could not verify their name and address. While companies shouldn't release information if they can't verify the consumer's identity, there should be a process by which any errors or issues can be resolved, so that customers can access their data.

THERE WAS A PROBLEM

Thank you for contacting Epsilon. We can't verify the name and address submitted, so your request can't be completed. Please click the "Make another request" button below to resubmit your name and address.

Make another request

Additionally, the requestor was surprised to find that Gap could not locate any of their data, because they were a regular customer. Even though the requestor had shopped with Gap multiple times, Gap reported that:

We were unable to locate any data associated with the email address that you provided. If you would like to submit another request with an alternate email address, then please use the link below.

Similarly, Comcast shared only a small amount of information. Even for such categories as "Service Activity Information" and "Account Information," the response was: "No data found for this category."

As a result, the AG should require companies to establish an appeals process for consumers who have not received information that may be covered under the law. Companies should be required not only to perform a meaningful investigation, free of charge, and either provide the requested information or a thorough response to the consumer, similar to the process for reinvestigation under the Fair Credit Reporting Act,[30] but to also file their response with the Attorney General. Companies should also be required to forward any complaints about a company's failure to comply with the CCPA to the AG to aid in regulation and enforcement.

[29] Cal. Civ. Code § 1798.185(a)(3).
[30] 15 U.S.C § 1681(i).

Conclusion

Thank you for the opportunity to submit comments on the updated draft rules. We would be happy to address any questions you have.

Respectfully submitted,

Maureen Mahoney
Policy Analyst
San Francisco, CA

Justin Brookman
Director, Privacy and Technology Policy
Washington, DC