Comments to the
California Office of the Attorney General

Notice of Second Set of Modifications
to Proposed Regulations under
The California Consumer Privacy Act

Submitted via Email to PrivacyRegulations@doj.ca.gov

March 27, 2020

On Behalf of the Following Organizations:

Table of Contents

Introduction

The undersigned group of privacy and consumer-advocacy organizations thank the Office of the Attorney General for its continued work on the proposed California Consumer Privacy Act regulations. As the regulations approach their final form, we urge the Attorney General to make the following revisions.

Preserve the CCPA enforcement date. Some industry interests have requested that the enforcement date of the CCPA be extended as a result of the public-health crisis associated with COVID-19. At this time, when so much of daily life is happening through the use of technology, the Attorney General should decline to postpone full enforcement of the CCPA. Now is not the time to weaken protections for consumers, many of whom are more vulnerable than ever.

Don't allow service providers to build comprehensive consumer profiles. Service providers enjoy a special status under the CCPA as a result of the narrow permission they have under the law to collect and use consumers' personal information. Allowing the construction of detailed consumer profiles using information collected as a service provider is flatly contrary to the purpose of the CCPA. The Attorney General should strictly limit service providers to making use of people's information for providing the specified service, and nothing more.

Require transparency from data brokers. The CCPA requires that businesses collecting personal information provide notice to consumers at the time of collection. That rule should apply with equal force to data brokers, whose collection and use of people's information pose grave privacy risks.

Enforce do not sell through do not track. Thousands of Californians have already enabled "do not track" settings in their web browsers. A business that cannot collect a person's information cannot sell that information, and the regulations should recognize that simple fact. The Attorney General should promulgate regulations that require businesses to treat "do not track" headers as requests to opt-out of sale.

Signing Organizations

The American Civil Liberties Union is a national, non-profit, non-partisan civil liberties organization dedicated to the principles of liberty and equality embodied in both the United States and California constitutions. The ACLU of California is composed of three state affiliates, the ACLU of Northern California, Southern California, and San Diego and Imperial Counties. The ACLU California operates a statewide Technology and Civil Liberties Project, founded in 2004, which works specifically on legal and policy issues at the intersection of new technology and privacy, free speech, and other civil liberties and civil rights.

Campaign for a Commercial-Free Childhood is a nonprofit organization committed to helping children thrive in an increasingly commercialized, screen-obsessed culture, and the only organization dedicated to ending marketing to children. Its advocacy is grounded in the overwhelming evidence that child-targeted marketing—and the excessive screen time it encourages—undermines kids' healthy development.

The Center for Digital Democracy's mission is to advance the public interest in the digital age. It is recognized as one of the leading consumer protection and privacy organizations in the United States. Since its founding in 2001 (and prior to that through its predecessor organization, the Center for Media Education), Center for Digital Democracy has been at the forefront of research, public education, and advocacy holding commercial data companies, digital marketers, and media companies accountable.

Common Sense Media, and its policy arm Common Sense Kids Action, is dedicated to helping kids and families thrive in a rapidly changing digital world. Since launching in 2003, Common Sense has helped millions of families and kids think critically and make smart choices about the media they create and consume, offering age-appropriate family media ratings and reviews that reach over 110 million users across the country, a digital citizenship curriculum for schools, and research reports that fuel discussions of how media and tech impact kids today. Common Sense also educates legislators across the country about children's unique vulnerabilities online.

Consumer Action uses multilingual consumer education materials, community outreach, and issue-focused advocacy to empower low- and moderate-income, limited-English-speaking, and other underrepresented consumers nationwide to financially prosper through education and advocacy.

The Consumer Federation of America is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education.

The Electronic Frontier Foundation works to ensure that technology supports freedom, justice, and innovation for all the people of the world. Founded in 1990, EFF is a non-profit organization supported by more than 30,000 members.

Media Alliance is a Bay Area democratic communications advocate. Media Alliance members include professional and citizen journalists and community-based communications professionals who work with the media. Its work is focused on an accessible, affordable and reliable flow of information to enable civic engagement, meaningful debate and a safe and aware populace. Many of Media Alliance's

members work on hot-button issues and with sensitive materials, and those members' online privacy is a matter of great professional and personal concern.

Oakland Privacy is a citizen's coalition that works regionally to defend the right to privacy, enhance public transparency, and increase oversight of law enforcement, particularly regarding the use of surveillance techniques and equipment. As experts on municipal privacy reform, Oakland Privacy has written use policies and impact reports for a variety of surveillance technologies, conducted research and investigations, and developed frameworks for the implementation of equipment with respect for civil rights, privacy protections and community control.

Privacy Rights Clearinghouse is dedicated to improving privacy for all by empowering individuals and advocating for positive change. Founded in 1992, Privacy Rights Clearinghouse has focused exclusively on consumer privacy issues and rights. Privacy Rights Clearinghouse strives to provide clarity on complex topics by publishing extensive educational materials and directly answering people's questions. It also amplifies the public's voice in work championing strong privacy protections.

No Delay of Enforcement is Warranted

We understand some businesses have requested a delay in enforcement of the CCPA as a result of the public-health crisis associated with the response to COVID-19. We do not believe any such delay is justified in this instance. This is precisely the time we need to ensure strong protections for consumers. Technology is being increasingly relied upon for learning, socializing, working-from-home, ordering supplies, and many other activities. Californians are at a greater risk of being exploited under the guise of health, the prospect of employment, or safety. Profiting off of personal information may become more appealing to companies who are facing changes in revenue. The CCPA went into effect on January 1, and companies are already required by law to comply. Now is not the time to weaken protections for consumers, many of whom are more vulnerable than ever.

Section 314(c). Keep the Service Provider Exception Narrow

Service providers have a special status under the CCPA. The information shared with them is excluded from the definition of sale, and as a result, consumers have no ability to opt out of the sale of information to service providers. CCPA Section 1798.140(t)(2)(C). Consumers are not entitled to know the categories of service providers who receive their information. CCPA Section 1798.110(a)(4) (limiting disclosure of categories to third parties). And finally, businesses enjoy special limited liability with respect to violations by their service providers. CCPA Section 1798.145(j). Therefore, the permissible use of people's information by service providers should be narrowly circumscribed. The second modified draft regulations

would create a large and inappropriate carve-out for service providers to use personal information they obtain from businesses to profile consumers and households. If service providers wish to use consumers' personal information for such a wide range of purposes, they should comply fully with the CCPA.

The first modified draft regulations created an enumerated list of allowed activities that we feared would license service providers to use data in unexpected ways. *See* Privacy and Consumer Advocacy Organization Comments on Draft Regulations, p. 21 (submitted December 6, 2019) ("First Privacy Coalition Comments"). The second set of modifications does address one of our earlier concerns: we appreciate that the new draft narrows the carve-out in section (c)(1) to specify that processing must be "on behalf of the business that provided the personal information." But on the whole, we continue to believe that the regulations give service providers too much leeway to process personal data for their own purposes. Furthermore, the other change to the section is a step back for consumer protection.

Section (c)(3) previously granted service providers the right to use such data for internal purposes, but explicitly forbade use for purposes of "building or modifying household or consumer profiles, or cleaning or augmenting data acquired from another source." However, the second set of modifications adds the following italicized clause to section 314(c)(3):

> "A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except:
>
> > (3) For internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles *to use in providing services to another business,* or correcting or augmenting data acquired from another source;"

This is a step backwards. In previous drafts, the regulations clearly stated that a company acting as a service provider may not use data collected in that role in order to build household or consumer profiles. Under the latest revisions, however, service providers may use any data they collect to profile people however the service providers want, as long as the profiles are not used "in providing services to another business." In other words, they can build profiles for themselves.

Some of the world's largest and most prolific tracking companies have already identified themselves as "service providers" for purposes of CCPA. For example, Google has added "service provider terms" as an addendum to its standard contract with publishers who use its ad technology.[1] Similarly, Amazon claims that it does

[1] *See Helping publishers comply with the California Consumer Privacy Act*, Google Adsense Help Center, https://support.google.com/adsense/answer/9560818?hl=en.

not "sell" information under CCPA, despite sharing data through an extensive behavioral advertising network.[2] Under the latest draft regulations, such companies will be able to use personal information they collect as service providers—from which consumers have no CCPA right to opt out—in order to build and augment consumer profiles for any internal use. This new exception would allow significant new intrusions on consumer privacy. It will incentivize large companies to enter into more "service provider" relationships in order to gather data for the purpose of building consumer profiles.

This is especially concerning given the draft regulations unjustified expansion of service providers to include companies that work with government entities. The latest draft regulations seem to imply that service providers may use personal information to build profiles for providing services to a non-business entity. This means, for example, that a "service provider" may collect personal information from relationships with private companies, use it to build profiles of consumers, and offer those profiles as a service to government entities like ICE.

We request that 2nd Mod. Reg. Sec. 314(c)(1)–(5) be replaced with the text originally proposed:

> A service provider shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for the purpose of providing services to another person or entity. ~~A service provider may, however, combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity.~~

We stress the importance of removing section 314(c)(3) in particular. This section gives service providers broad license to use personal information for their own purposes, including by building consumer profiles using information collected from different businesses. That expansive permission contradicts the intent of the legislature and should be removed.

The second modified draft regulations further remove important protections for consumers whose information is collected by and held by data brokers. The changes in the second modified regulations should be removed so that consumers have a reasonable opportunity to know when data brokers collect and sell information about them.

---

[2] *See California Consumer Privacy Act Disclosures,* Amazon Help and Customer Service, https://www.amazon.com/gp/help/customer/display.html?nodeId=GC5HB5DVMU5Y8CJ2.

Section 305(d). Mandate Transparency for Data Brokers

Both the modified and second modified draft regulations represent steps backward in providing transparency to consumers who wish to understand and control how their information is being collected, used, and sold. The first draft regulations provided that, before a business that did not collect information directly from consumers could sell their information, efforts needed to be made to notify the consumer of their rights to opt-out, or confirm that the collection of information had, in the first instance, complied with the law. Draft Regs Sec. 305(d). A coalition of privacy and consumer-advocacy groups proposed concrete amendments to improve consumers' ability to exercise their rights. First Privacy Coalition Comments, p. 13–14. The Attorney General should adopt the coalition's proposal from those initial comments.

Unfortunately, subsequent modified draft regulations have all but eliminated notice to consumers when their information is collected and sold by data brokers and other entities, many of which consumers have no knowledge of. Each subsequent revision of the draft regulations has further limited consumers' rights with respect to data brokers under the CCPA.

The first modified draft regulations allowed businesses *that do not collect information directly from consumers* to avoid providing notice-at-collection by including a privacy-policy link in their data-broker registration. Mod. Draft Regs. Sec. 305(d). The second draft regulations remove the requirement that the business not collect information directly from consumers, allowing *all* data-broker registrants to avoid notice-at-collection, even if the data broker collects information directly from consumers. 2nd Mod. Draft Regs. Sec. 305(d).

The change in the second draft regulations is a mistake. If a business collects information directly from consumers, it should provide robust notice at collection, whether it is a data broker or not. There is no reason why data brokers—whose business model is particularly pernicious to privacy—who collect information directly from consumers should provide any less notice than other companies who collect information directly from consumers. Therefore, the coalition proposes that the Attorney General adopt the following revision to 2nd Mod. Regs. Section 305(e).

> A business that is ~~A data broker~~ registered as a data broker with the Attorney General pursuant to Civil Code section 1798.99.80 et seq. ~~the business~~ does not need to provide a notice at collection to the consumer if the information is not collected directly from the consumer and the business~~it~~ has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out.

Section 315(d). Enforce Do Not Sell Through Do Not Track

The regulations require businesses to treat certain privacy controls as opt-out from sale. The second modified draft regulations are an improvement from the previous

round of modifications, but would still hinder consumer choice when compared with the original draft regulations.

We commend the removal of this clause from section 315(d)(1): "The privacy control shall require that the consumer affirmatively select their choice to opt-out and shall not be designed with any pre-selected settings." Many consumers choose the software they use specifically to reflect their privacy choices. If a user selects a browser extension or application in order to protect their privacy, they should not also need to select a separate setting in order to enjoy one of the most important privacy protections granted by CCPA, the right to opt out of sale. This change removes perverse incentives that would have encouraged non-privacy protective defaults by companies.

However, we continue to oppose the remainder of the text added by the first modifications at Section 315(d)(1): "Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to opt-out of the sale of personal information." As the coalition has explained before, many major web browsers already include settings by which users can easily choose to send "do not track" headers with all of their web traffic. Thousands of Californians have already enabled this "do not track" browsing header. A business that cannot collect a person's information cannot sell that information. The greater (do not collect) includes the lesser (do not sell). So businesses should treat "do not track" headers as requests to opt-out of sale.

We remain concerned that some businesses may not interpret "do not track" headers as a "clear" signal that the consumer intends to opt out of sale. As detailed in previous comments, a desire to not have one's information tracked encompasses a desire not to have one's information sold. However, the latest regulations do not clearly require businesses to treat the former (a request to opt out of tracking) as indicative of the latter (a request to opt out of sale). They leave open the possibility that a business may ignore a Do Not Track request.

In short, please withdraw 2nd Mod. Reg. Sec. 315(d)(1). And per our earlier sets of comments, please add this clause to the end of Mod. Reg. Sec. 315(c):

> A business shall treat a "Do Not Track" browsing header as such a choice.

308(c)(1)(g)(3). Clarify Treatment of Minors and Opt-In

This section of the proposed regulations details privacy-policy requirements and would require companies to state "whether the business has actual knowledge that it sells the personal information of minors under 16 years of age." As a number of us explained in our comments on February 25 (Comments re Modified Reg. Sec. 308(c)(1)(e)(3)), this provision is unnecessary and should be struck.

This language is unnecessary because the 2nd Modified Regulations already require that privacy policies provide the critical information parents or minors need to know in these circumstances. Specifically, privacy policies must provide a description of the process for opting-in to sale of information if companies allow this. That is detailed in Second Modified Regulation Sec. 308(c)(9).

It should be struck for a few reasons. First, the statement is confusing. It is unclear what effect, if any, it may have for a company to state whether it "has actual knowledge that it sells the personal information of minors." Whether a company has actual knowledge that it is selling minors' personal information, which includes willfully disregarding a consumers' age per the statute, is not something a company can disclaim in a privacy policy. Allowing a company to pretend to disclaim it is confusing.

Second, requiring additional duplicative disclosures goes against the Second Modified Regulations' aim to require easy to read and understandable privacy policies. Privacy policies are already long.[3] Repeating largely duplicative information, separate from and without critical "how to" information about what consumers can do in response, should be avoided. Removing this requirement may aid in consumer comprehension and understanding and does not take away from the meaningful transparency requirements imposed by the CCPA.

We therefore request that the Attorney General strike 2nd Mod. Reg. 308(c)(1)(g)(3).

Conclusion

The coalition appreciates the Attorney General's work on these proposed rules and urges the Attorney General to take the steps recommended in these comments to ensure that consumers' privacy rights are protected.

[3] Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. Times Privacy Project (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.