Comments to the

Office of the Attorney General of California

Notice of Modifications to Proposed Rulemaking

The California Consumer Privacy Act

Submitted via Email to PrivacyRegulations@doj.ca.gov

February 25, 2020

On Behalf of the Following Organizations:

ACLU California

Electronic Frontier Foundation

common sense

Privacy Rights Clearinghouse

Media Alliance

CFA

ccfc Campaign for a Commercial-Free Childhood

Oakland Privacy

Table of Contents

Introduction

The undersigned privacy and civil-liberties organizations thank the Office of the Attorney General for its continued work on consumer privacy. We are disappointed that the Modified Regulations (Mod. Reg.) are largely a step backwards for protecting consumers' privacy, particularly in terms of consumers' attempting to stop the sale of their information. Most problematically, the proposed Modified Regulations limit the protections offered by the law by improperly reducing the information covered by CCPA and making it harder for consumers to exercise a key affirmative right—opting out of the sale of personal information. The proposed opt-out icon is rather confusing. And the proposed Modified Regulations also make a number of changes to the original draft that are business-friendly at consumers' expense.

The proposed Modified Regulations make it more difficult for consumers to effectively opt-out of sale of their personal information, by failing to recognize widely known signals as a request to opt-out and by placing even more burdens on consumers

The proposed Modified Regulations improperly limit the law's protective reach, by narrowing the definition of personal information and trying to carve out certain identifiers (including IP addresses) from that definition under certain circumstances.

The proposed icon for "Do Not Sell" may inadvertently lead to consumer confusion. The choice of color and the implication of a toggle function may lead to consumers believing their information is not being sold when in fact it is. We understand any confusion to be the opposite of the Attorney General's goals.

The proposed change to not require businesses to treat an unverified deletion request as an opt-out request creates an additional hurdle to jump through for consumers who are at bottom seeking to have their information out of a company and an online ecosystem.

Proposed reporting requirements are applicable to an even smaller subset of companies, instead of acknowledging that small companies who build a model on data collection and sharing can cause real privacy harms to individuals as well.

The enumeration of new rights of service providers to use personal information for their own purposes, including any contractual purposes they may have chosen to insert, blurs the line between business and service provider. Given that service provider sharing falls outside the CCPA definition of "sale" and consumers have no say over such transfers, any receiving service provider's use of such information must be limited.

Signing Organizations

The American Civil Liberties Union is a national, non-profit, non-partisan civil liberties organization with more than 1.6 million members 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.

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.

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.

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.

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.

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

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.

Section 315(c). Do Not Track & Do Not Sell.

The modified regulations would hinder the exercise of consumer rights.

The modified draft regulations would make it harder for consumers to use browser headers to opt-out from the sale of their personal information. The coalition objects to this step backwards from the original draft regulations.

The original draft regulations required businesses that collect consumer data online to treat the following as an opt-out: "user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information." *See* Original Draft Regulations § 315(c). The coalition supported this rule, because it would make it easier for consumers to exercise their right to opt-out.

Unfortunately, the modified draft regulations would add the following: "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. 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." *See* Mod. Reg. Sec. 315(d)(1).

As the coalition explained in our initial comments, thousands of Californians have already installed tools that send "do not track" browsing headers to the sites they visit. 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. 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.

Yet "do not track" headers might not fit into the new draft rule. First, some of these systems come with the pre-selected privacy settings that the consumer does not manually select. A consumer's choice to use tools that are privacy protective by default should not mean they have fewer protections, and any pro-consumer privacy regulation should not incentivize companies to not protect privacy by default—that is an absurd consequence. Second, businesses may argue that "do not track" headers do not "clearly communicate or signal that a consumer intends to opt-out of the sale of personal information." As detailed in previous comments, a desire to not have one's information tracked encompasses a desire not to have one's information sold.

Please withdraw this new Mod. Reg. Sec. 315(d)(1). And per our earlier set 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.

Section 302(a). Interpretation of "Personal Information."

The modified regulations are inconsistent with both the language and the fundamental purpose of the CCPA.

Section 999.302 of the draft regulations states that information including but not limited to IP addresses is not personal information if "the business does not link the [information] to any particular consumer or household, and could not reasonably link the [information] with a particular consumer or household." As drafted, Mod. Reg. Sec. 302 is inconsistent with the statute's language and in irreconcilable conflict with one fundamental purpose of the CCPA: to give consumers control over how they are tracked online. This problem is amplified by its explicit application to IP addresses.

First, the proposed regulation is contrary to the CCPA's core definition of "personal information." Under the CCPA, information qualifies as "personal information" if it "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." That definition does not refer to the possessor's specific actions or capabilities because whether information is PI or not is a property of *the information itself*, and does not depend on its possessor. This is directly contrary to the proposed regulation, under which certain information may be PI if possessed by one business but not by another business.

This interpretation is shared by other provisions of the CCPA which are explicitly designed to address related sets of personal information which would be undermined by the proposed regulation. In particular, the proposed regulation would supplant the CCPA definition of "deidentified" information, an exception to personal information that applies exclusively to information that "cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer," with a far broader exception to personal information, excluded from the procedural safeguards applicable to deidentified information, that apples any time the *current possessor* lacks the capability to link or associate the information.

As a result, under the proposed regulation, a business would be free to sell information that its recipient could easily reidentify as long as the business itself was unable to do so. This would broadly undermine the purpose of the CCPA and the practical exercise of the rights it grants to consumers..

Instead, privacy laws must—and the CCPA does—take into account the modern reality that information is not "anonymous" and thus not personal merely because its current possessor lacks the capacity to associate it with a specific person.[1] For example,

[1] Nate Anderson, *Anonymized" data really isn't—and here's why not*, Ars Technica, September 8, 2009 (available at https://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/); *see also* Ohm, Paul, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*,

"anonymized" search queries released by AOL were nonetheless associated with particular individuals,[2] and Twitter users were unmasked by leveraging the structure of social relationships.[3] Machine learning techniques can significantly reduce the difficulty of re-identifying personal information over time.[4] Signaling the maturity of these re-identification techniques, data brokers are even offering what is effectively re-identification as a service, promising the ability to "reach customers, not cookies."[5] By excluding information from the CCPA solely because the current possessor lacks the capacity to connect it to a specific consumer, the draft regulations threaten to eliminate protections for information that has immense potential to violate people's privacy.

In addition, the regulation is particularly problematic in its application to IP addresses, which deserve and enjoy particular protection under the CCPA.

Under the CCPA, IP addresses belong to the same category of "identifiers" as a real name, an email or postal address, an account name, or a social security number.[6] The fact that multiple consumers may have the same or similar names, share email addresses or online accounts, or live at the same postal address with others does not change the fact that labelling information with a name, email address or postal address serves to "identify" the data subject, thus rendering it personal information under the CCPA. The same is true of IP addresses, which in and of themselves identify a particular consumer or device, even if they do not do so with perfect accuracy.[7]

Moreover, protecting information like IP addresses that can be used to track consumers' online activity is the goal of modern privacy laws including the CCPA. A 2019 poll of

---

August 13, 2009. UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12 (available at SSRN: https://ssrn.com/abstract=1450006).

[2] Eric Bangeman, *AOL subscribers sue over data leak*, Ars Technica, September 26, 2006 (available at https://arstechnica.com/information-technology/2006/09/7835/).

[3] Nate Anderson, *Pulling back the curtain on "anonymous" Twitterers*, Ars Technica, March 31, 2009 (available at https://arstechnica.com/tech-policy/2009/03/pulling-back-the-curtain-on-anonymous-twitterers/).

[4] Gina Kolata, *Your Data Were 'Anonymized'? These Scientists Can Still Identify You*, The New York Times, July 23, 2019 (available at https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html).

[5] *Reach Customers, Not Just Cookies*, LiveRamp Blog, September 10, 2015 (available at https://liveramp.com/blog/reach-customers-not-just-cookies/) ("Cookies are like an anonymous ID that cannot identify you as a person.").

[6] Civ. Code § 1798.140(o)(1)(A) specifies that personal information includes "identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers."

[7] For the same reason, IP addresses also explicitly appear in the definition of "unique identifier," which is "a persistent identifier that can be used to recognize a consumer, a family, or a device … including, but not limited to… an Internet Protocol address." Civ. Code 1798.140(x).

likely California voters showed that Californians overwhelmingly support a definition of personal information that encompasses all information about them, their households and their electronic devices.[8] Over 90% of voters, spanning across age, gender, party, and region of California, said it was important to be able to control their personal information in each of the following areas:

- Information collected about your computer, phone or other device that could be identified by an IP address.
- Information related to or collected about a household, including from a device in the home such as Alexa, a baby monitor, or a "smart" TV or refrigerator, that could be compiled with the use of a household IP address.
- Location information, including the history of where you've been, that could be connected to or even derived from an IP address.

The legislature's intention that an IP address qualify as personal information is further reflected in its rejection of AB 873 (2019). According to both its author[9] and proponents[10], AB 873 was intended to expand the definition of "deidentified" information with the explicit purpose of exempting IP addresses from the CCPA in the same manner as the draft regulation.[11] The legislature properly rejected that proposal. The Attorney General should not undo that decision by incorporating it into regulations that undermine the purpose of the CCPA.

We support the Attorney General's desire to add clarity to the CCPA. But the proposed regulation would undermine rather than clarify the definition of personal information. Information that can be connected to a specific consumer should be within the scope of

---

[8] *Will California lawmakers vote to protect Californians' privacy or tech industry profits?* ACLU of Northern California, March 27, 2019 (available at https://www.aclunc.org/blog/will-california-lawmakers-vote-protect-californians-privacy-or-tech-industry-profits).

[9] Asm. Irwin, the author of AB 873, asserted that "if a store keeps IP address for web analytics, but it doesn't link that data back with a person," the IP address would still be subject to the CCPA, and that changing that was a key goal of AB 873. *See* Assembly Committee on Privacy and Consumer Protection, California Consumer Privacy Act of 2018, Mar. 25, 2019, http://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201920200AB873.

[10] Jim Halpert, who testified on behalf of the sponsors of the bill, wrote that AB 873 "would very likely have the effect of exempting IP addresses and device IDs that are maintained separately from personal data and cannot be queried or accessed by employees or third parties who could link the data." Jim Halpert, California Lawmakers Smooth Over Some of the CCPA's Rough Edges, IAPP Privacy Tracker, https://iapp.org/news/a/california-lawmakers-smooth-over-some-of-the-ccpas-rough-edges/.

[11] AB 873, much like the proposed regulation, would have excepted information from personal information (by way of categorizing it as deidentified) if the information "does not identify and is not reasonably linkable, directly or indirectly, to a particular consumer." "Reasonably linkable" appears verbatim in the proposed regulation as a necessary rather than sufficient attribute of personal information.

the CCPA even if its possessor currently lacks that capacity. And IP addresses in particular are online identifiers, both in practice and in the language of the CCPA, that inherently identify and are capable of being associated with or linked to a specific consumer, satisfying the definition of "personal information." Any contrary guidance or regulation is inconsistent with the goals and express language of the CCPA.

We therefore respectfully request that Mod. Reg. Sec. 999.302 be deleted in its entirety.

Section 306(f). "Do Not Sell My Personal Information" Button.

The recommended toggle icon would lead to consumer confusion.

Mod. Regs. Sec. 999.306(f) recommends a CCPA opt-out button and accompanying tagline that will lead to consumer confusion. The recommended icon does not clearly convey the presence of a choice and may discourage consumers from exercising their opt-out right. The coalition urges the Attorney General to modify its recommended icon to reduce the possibility of confusion.

The Attorney General should follow the recommendations outlined by Lorrie Cranor and her team of researchers and designers that developed and tested combinations of icons and taglines to signal opt-out request. Cranor et al. found that a "toggle" icon most clearly conveys to consumers the presence of privacy choices, however the icon that the Attorney General recommends in the modified draft regulations is significantly different from the icon recommended in the Cranor study, and does not clearly convey the same information.[12]

The toggle icon tested in Cranor's research is a rounded, pill shaped button divided vertically, with the left portion of the button displaying a blue checkmark on a white background, and the right portion of the icon showing a white "x" mark on a blue background (*see* Fig. 1). Every "toggle" icon tested in the Cranor study included some combination of two elements that help convey a binary decision (e.g. a +/-, a ✓/x, ✓/-, etc.)[13]. When asked to interpret this icon, consumers commonly interpreted it as "Accept/decline something", "activate/deactivate something", "okay/exit" options, or as indicative of the ability to mark something as "true" or "false."

[12] 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", p. 3 (2020) (available at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-cranor.pdf).

[13] *See id.* at 42.

Fig. 1: Toggle Icon Recommended by Cranor et al.[14]

Fig. 2: Toggle Icon Recommended in Mod. Reg. Sec. 906(f).

Conversely, the icon proposed in the modified draft regulations more resembles an interactive toggle switch, with the left half of the button displaying a white circle on a red background, and the right half of the button displaying a white x on that same red background (*see* Fig. 2).The icon appears to be an interactive toggle switch set to the "left", the white "x" seeming to indicate that whatever option was just selected is a negative option. The fact that the icon is red further reinforces this interpretation.

Cranor *et al* noted that there is already a risk that a toggle icon can be interpreted as an actual control (rather than a static icon), which could deter users from interacting with it.[15] The design recommended by the Attorney General encourages this misinterpretation by resembling an interactive toggle switch rather than an icon visually representing a binary choice.

Recommendations for reducing consumer confusion.

Rather than clearly conveying the presence of an opt-out right, the ambiguous button invites consumers to ask, "Is this an interactive toggle?" "If this is a toggle, is the toggle set to 'yes, sell my personal information' or 'no, do not sell my personal information'?" and "Does the red 'x' mean my information is already being sold, or does it mean I have not yet exercised my right to opt-out of those sales?"

The privacy coalition respectively recommends that the Attorney General redesign the opt-out button to reduce the possibility of confusion by using the toggle icon recommended by Cranor et al.; a blue icon that includes both a check mark and an x mark, to help convey the presence of choice. Further, it is left unclear how this icon will display across mobile devices and different user agents, and so we urge the Office to ensure that their recommendations with regard to the opt-out icon will display clearly and legibly on any device that the consumer uses to access the business's website.

[14] *See id.* at 3.

[15] *See id.* at 31.

Section 313(d)(1). Unverifiable Requests to Delete.

The modified regulations would create additional burdens on the exercise of consumer rights.

The coalition opposes the Attorney General's modified draft rule which would allow a business that cannot verify the identity of a deletion requestor to, instead of treating the request as one to opt-out of sale as initially proposed, instead allow the business to respond by asking the consumer if they would like to opt-out of the sale of their personal data and providing information about opting out. Having businesses add an additional step for consumers to take, versus automatically treating the request as one not to sell, is burdensome on consumers and time-strapped families. Further, consumers may already feel overwhelmed by various "privacy choices" including exercising their rights under the CCPA and this provision adds to the confusion. A Pew Research Center survey, polled U.S. adults on their understanding of the current laws and regulations in place to protect their data privacy and 63% said they understand very little or not at all, so it may be difficult for them to exercise their rights.[16] Thus, the coalition proposes Mod. Reg. Sec. 999.313(d)(1) be revised to the original language, by having a business treat an unverified request to delete as a request to opt-out of sale.

Section 314(c)(1). Service Providers Use of Personal Information.

The modified regulations would inappropriately expand the rights of service providers to use personal information.

We appreciate that the modified draft regulations remove the explicit allowance of service providers combining personal information from two different entities for security and fraud purposes. However, we are concerned that the new enumerated list of exceptions still enables service providers to combine information for those purposes (as a "use" of information to protect against security incidents or fraud under Mod. Reg. Sec. 314(c)(4)) as well as a host of other new activities.

For example, Mod. Reg. Sec. 314(c)(1) enables service providers to use or share information as long as it is to perform a service specified in a contract. This is not limited to services which benefit the contracting business. Service providers, especially larger ones, can and do specify all manner of activities in a contract, not all of which benefit businesses or consumers.

Mod. Reg. Sec. 314(c)(3) enables service providers to use personal information to build and improve the quality of their products and services, so long as this use "does not include building or modifying household or consumer profiles, or cleaning or augmenting

[16] Brooke Auxier & Lee Rainie, *Key takeaways on Americans' views about privacy, surveillance and data-sharing*, Pew Research Center (Nov. 15, 2019).

data acquired from another source". Presumably, reaching out to consumers directly to advertise or offer new products or seek other feedback would qualify, as long as a "profile" is not created. This stretches the notion of what a consumer expects from a service provider.

We request that 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.~~

Section 317(g). Transparency

The modified regulations would be a step backwards on transparency.

Previous draft regulations called for companies to post metrics about their CCPA compliance if they collected information on over 4 million consumers. The coalition noted that this threshold was too high, and requested that businesses be required to publish metrics on their compliance with CCPA requests to those with either $25 million in annual revenue, or 50% of revenue generated from the sale of personal information. Instead, in a step in the opposite direction, the modified draft regulations require even fewer companies to report--those with over 10 million consumers--even ones whose entire business model may be premised on selling consumers' personal information. This will increase business opacity and make it harder for consumers, as well as legislators, journalists, and public interest advocates, to understand how companies are protecting privacy and complying with the CCPA.

Transparency about compliance is critical, especially given that the Attorney General has noted he has capacity for only a few cases a year. We respectfully request that the regulations be changed per our earlier suggestion:

A business that alone or in combination ~~buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 10,000,000 or more consumers in a calendar year~~ **has annual gross revenues in excess of twenty-five million dollars or derives 50 percent or more of its annual revenues from selling consumers' personal information**, shall:

Conclusion

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