Mozilla Corporation
2 Harrison St
Suite 175
San Francisco, CA 94105

November 8th, 2021

California Privacy Protection Agency
Attn: Debra Castanon
915 Capitol Mall, Suite 350A
Sacramento, CA 95814
Via email: regulations@cppa.ca.gov

Re: Comments on proposed rulemaking under the California Privacy Rights Act of 2020 (PRO 01-21)

Dear Ms. Castanon:

Thank you for the opportunity to comment on the California Privacy Protection Agency's ("Agency") preliminary rulemaking regarding the California Privacy Rights Act of 2020 ("CPRA").[1]

Mozilla is the maker of the open-source Firefox web browser, the Pocket "read-it-later" application and other products and services that collectively are used by hundreds of millions of individuals around the world. Mozilla is also a global community of contributors and developers who work together to keep the internet open and accessible for all. As a mission-driven technology company and a not-for-profit foundation, we are dedicated to putting people in control of their online experience, and creating an internet that is open and accessible to all. To fulfill this mission, we are constantly investing in the security of our products and the privacy of our users.

General Comments

For Mozilla, privacy is not optional. It is an integral aspect of our Manifesto, where Principal 4 states that Individuals' security and privacy on the internet are fundamental and

[1] California Privacy Protection Agency, "Invitation for preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020" (Sept. 22, 2021), https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf

Mozilla Corporation
2 Harrison St
Suite 175
San Francisco, CA 94105

must not be treated as optional. We actualize this belief by putting privacy first in our own products with features like Enhanced Tracking Protection (ETP)[2], Total Cookie Protection (TCP)[3], DNS over HTTPS[4] and our end to end encrypted Firefox Sync service.[5] We also promote privacy in our public advocacy, having engaged with privacy and data protection related issues across the world. [6]

Mozilla has long been a supporter of data privacy laws that empower people, including the landmark California privacy laws, California Consumer Privacy Act (CCPA)[7] and CPRA[8]. We're engaging today in support of the progress made thus far — but there's much more to do. The internet is powered by consumer data. While that data has brought remarkable innovation and services, it has also put internet users, and trust online, at substantial risk. We believe that everyone should have control over their personal data, understand how it's obtained and used, and be able to access, modify, or delete it.

Our comments below focus specifically on Global Privacy Control (GPC), which we are experimenting with within Firefox and we think can play an integral aspect in making a right to opt-out meaningful and easy to use for consumers.

---

[2] Latest Firefox rolls out Enhanced Tracking Protection 2.0, https://blog.mozilla.org/en/products/firefox/latest-firefox-rolls-out-enhanced-tracking-protection-2-0-blocking-redirect-trackers-by-default/
[3] Firefox 86 Introduces Total Cookie Protection, https://blog.mozilla.org/security/2021/02/23/total-cookie-protection/
[4] Firefox continues push to bring DNS over HTTPS by default for US users, https://blog.mozilla.org/en/products/firefox/firefox-continues-push-to-bring-dns-over-https-by-default-for-us-users/
[5] Privacy by Design: How we build Firefox Sync, https://hacks.mozilla.org/2018/11/firefox-sync-privacy/
[6] https://blog.mozilla.org/netpolicy/category/privacy/
[7] Bringing California's privacy law to all Firefox users in 2020, https://blog.mozilla.org/netpolicy/2019/12/31/bringing-californias-privacy-law-to-all-firefox-users-in-2020/
[8] Four key takeaways to CPRA, California's latest privacy law, https://blog.mozilla.org/netpolicy/2020/11/20/here-are-four-key-takeaways-to-cpra-californias-latest-privacy-law/

Mozilla Corporation
2 Harrison St
Suite 175
San Francisco, CA 94105

Response to Agency topic #5: Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of their Sensitive Personal Information

Mozilla strongly supports the approach taken in the regulation to use settings at the platform level, particularly in web browsers such as Firefox, to allow consumers to opt-out of the sale or sharing of their personal information. Firefox today blocks third-party tracking. However, our technical protections are less suited for cases of first parties that might collect consumers' data and sell or share that data without the consumers' knowledge. As more browsers move to restrict cookies, we expect more websites to shift to this first party data collection and opaque sharing of that data behind the scenes.

Moreover, consumers cannot reasonably be expected to opt-out of the sale or sharing of their information individually from every party they interact with on the Internet. That is why a universal opt-out mechanism, set by the user, sent by the browser to all websites, and then enforced by the regulators, is so critical. Mozilla in October began experimenting with just such a setting: the Global Privacy Control (GPC), a feature available for experimental use in Firefox Nightly. Once turned on, it sends a signal to the websites users visit telling them that the user does not want to be tracked and does not want their data to be sold.

Unfortunately, the enforceability of GPC under CCPA remains ambiguous, with competing interpretations of do-not-sell requirements and with many businesses uncertain about their exact obligations when they receive a signal such as the GPC. The practical impact is that—**businesses may simply ignore the GPC signal**—especially if they have elected to use any other two mechanisms to receive opt-out requests.

History shows that without a clear legal mandate, most businesses will not comply with consumer opt-out signals sent through browsers. This vacuum is the same reason that

Mozilla Corporation
2 Harrison St
Suite 175
San Francisco, CA 94105

Do Not Track ("DNT") failed to gain adoption. It was eventually removed by all major browsers because it created a false sense of consumer protection that could not be enforced.

Mozilla encourages the California AG to expressly require business to comply with GPC. The 2023 Colorado Privacy Law has taken this step, and the addition of California would pave the path for other global privacy regulators to similarly update their laws. Further, enforcement authorities should expect businesses to interpret the GPC as governing both the direct sale of consumer's information as well as the sharing of consumers' information for programmatic advertising targeting purposes. Regulators, consistent with the intent of CCPA and CPRA, must step in to give tools like the GPC enforcement teeth and to ensure consumers' choices are honored.

Conclusion

We're grateful for the opportunity to share Mozilla's views in this preliminary submission and look forward to ongoing engagement with the Agency. We will seek to expand on topics of interest as the Agency continues stakeholder outreach and when new regulations and/or changes to existing regulations are published. If you have any questions about our submission, or if we can provide any additional information that would be helpful, please do not hesitate to contact us.

Sincerely,

Jenn Taylor Hodges
Head of US Public Policy
Mozilla