December 6th, 2019

Attn: Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Via email: PrivacyRegulations@doj.ca.gov

Dear Privacy Regulations Coordinator:

Thank you for the opportunity to submit comments on your proposed regulations for the California Consumer Privacy Act of 2018 (CCPA). The CCPA will bring important privacy and data protection rights to Californians, and it is key to ensure that this implementation is well-conceived.

Mozilla is the maker of Firefox, the open-source web browser used by hundreds of millions of people. We also create new apps and tools that put people in control of their online experience, and keep the internet open and accessible to all. We're the keeper of the open web, and a trusted technology company known for the privacy and security of its products and our values-driven approach. As the makers of the Firefox browser, we recognize that we are in a unique position to enable a trusted internet. It's why we provide our users with more control within the browser and limit the data that we collect and use in accordance with our Lean Data Practices. We also work to shape policy and legislation across the globe, as we have done in California.

We're here today because we believe the internet and our industry is in crisis, and real work must be done to regain the promise of the internet. Governments - from local and state to federal and international - play a huge role in realizing that promise, and in protecting the privacy of internet users. To that end, earlier this year we released a blueprint that we believe can guide comprehensive privacy legislation at any level. We are pleased to work with you and your office to realize the promise of a trusted internet that enables people to create and share.

General comments

Core to making CCPA an implementable privacy and data protection law is the clarity the related regulations need to bring. It is important that the regulations provide that clarity so that consumers are as clear as possible about their rights and companies know with reasonable certainty what is expected of them. We intend these suggestions to help define the regulations in order to provide truly meaningful controls and compliance programs that benefit consumers.

Definition of "third parties"

Any law depends on thorough and specific definitions in order to properly apply rules and responsibilities, and doubly so for a complex law like CCPA.

> *999.301(e) — "Categories of third parties" means types of entities that do not collect personal information directly from consumers, including but not limited to advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers.*

For the rules around third party data collection and sale to have real impact, the definition of third parties - or that of third party collection - is key. Unfortunately, this definition seems to carve out several important stakeholders in any data-sharing economy. This definition should be clarified to note that some entities act as both a first and third party. Usually, third party interactions are defined by the context of the data collection - not whether or not the party has a direct relationship with the user. More and more, we see companies collecting data from a number of contexts: first parties, as a third party on a different site, or simply buying data directly.

For example, many social networks and online platforms collect data directly from a consumer through direct online transaction on their platform, but also from indirect methods - whether purchasing that data or by embedding tracking elements in other websites. Defining the data collection relationship by an entity as first or third party - as this definition seems to do - raises many questions around implementation and the strength of protections that CCPA will offer.

> *999.301(h) — "Household" means a person or group of people occupying a single dwelling.*

While we recognize that your office does not have the latitude to change the application of the "household" definition in the broader law, we continue to have great concern at the use of a household as an aggregate unit for the purposes of "right to know" and "right to access". The current household definition and implementation will be an avenue for abuse of the CCPA, and support strong regulatory guidelines on its use.

We appreciate that the verification of a household as an aggregate unit requires all members of that household. However, it is not clear whether the data received by a household with a verified request should be all data about all persons in that household, or an aggregated (and deidentified) set of information, which could somewhat protect privacy within larger households. Also, depending on the data the entity has about the household, in many circumstances even aggregated/de-identified data is still able to be identified to a person because the sample size of the household is likely to be very small. It is not clear who may be considered a member of a household; many single dwellings have transient members, or people who live there part-time. There is no way to determine whether these members are a part of the group under this definition.

Fraud and authentication

It has been broadly noted that verification of any request for information under "right to know" or "right to access" must be adequately authenticated. While these regulations significantly clarify what kind of verification is adequate, we are concerned that the authentication processes are not strong enough and may result in data being released to non-authorized persons.

For example, it will prove to be difficult to reasonably authenticate any request where a service has minimal information about a user, let alone one from a household; records may not even exist to confirm or refute any claim as to who may live in a particular household. In particular, it is unclear whether there are adequate ways to verify a consumer's request when it is submitted through a third party service. The opportunity for fraud and abuse is high particularly if the business responding to such a request does not have a meaningful opportunity to pursue their own authentication other than asking the authorized agent for proof of such authorization. There have been multiple reports from Europe about records released based on badly authenticated, or unauthenticated, requests based on the GDPR.

We strongly encourage the Attorney General's office to set a high bar on acceptable authentication for any request, and continually monitor how this provision is used, and how to improve it, on a regular basis. We hope that strong authentication methods at third parties services will facilitate a secure and trusted consumer mechanism for those who choose to use them, as well as provide a solid liability protection for companies acting on these requests in good faith.

Metrics about Personal Data Requests

999.317. Training; Record-Keeping (g)(1)

Mozilla has published a transparency report for years, and we believe in transparency as a vital tool in helping to understand requests. While our transparency report generally focuses on requests from government and law enforcement entities, we have reported the number of Personal Data Requests received under GDPR and other data protection laws since July of 2018.

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. We extend these principles to all of our users regardless of when they submit a Personal Data Request, where they are located, or whether a data protection law (such as the CCPA) grants them express privacy rights.

Mozilla takes great care to avoid collecting user location as we do not need it in order to provide our service. Companies like Mozilla that extend the same personal data rights to any person and cannot determine that individual's location, will have difficulty complying with the metrics reporting as outlined in the draft regulations. We do not want to ask users who send us data access requests for additional personal information in order to comply with a metrics standard. There is no benefit to the user in providing residency information and it makes no difference when we provide the control rights universally.

In addition the specific reporting breakdowns required (for requests to know, to delete, and to opt-out) and median response times do not significantly increase the understanding of how CCPA rights are being exercised and complied with. The metrics requirements appear to assume that requests are always clear and unambiguous and are received in systems that allow for automated response time tracking.

In reality, the ways in which consumers exercise these rights are not always clear and concise; they often combine requests in vague, non-specific language and pieces of requests may be separated or handled

as a bulk action. Users may also locate, or be directed to, self-service portals where they can exercise their rights and not need to receive any company human support at all. For example, it would be difficult to ascertain whether a self-deleted account should be measured as a CCPA data request or not.

It's important to also note that companies may not use ticketing or contact systems that includes queues or other functionalities that allow them to accurately calculate median response times. But many companies, including Mozilla, rely on email for many requests where such calculations are far from simple or automated.

We respectfully suggest the metrics reporting requirements to be simplified to include only the information most salient for consumers and the Attorney General.

In conclusion

We are pleased to offer any additional explanation of these concerns to your office, or address any other topics of interest. We look forward to continuing to discuss the path forward for protecting the privacy rights of Californians, of all Americans, and indeed of everyone worldwide.

Sincerely,

Heather West
Head of Public Policy, Americas
Mozilla