Engine

Engine
44 Tehama St.
San Francisco, CA 94105

March 8, 2019

The Honorable Xavier Becerra
Attorney General
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

Re: Implementing Regulations for the California Consumer Privacy Act

Dear Mr. Becerra:

Engine submits the following comments in response to the Justice Department's request for comments regarding the Department's rulemaking process in the wake of the 2018 passage of the California Consumer Privacy Act (CCPA). We appreciate the opportunity to comment.

## I. Introduction

Engine is a non-profit technology policy, research, and advocacy organization that bridges the gap between policymakers and startups. Based in San Francisco, California, and Washington, D.C., Engine works with a nationwide network of startups to understand how ongoing policy debates affect new and small high-growth technology companies and how to best advocate on behalf of the ever-changing and growing startup ecosystem in the U.S. The thriving U.S. startup ecosystem is responsible for some of the most innovative products and services as well as the vast majority of net job growth in the U.S. The center of that activity is undeniably in California. Creating regulatory burdens in the name of protecting users' privacy without fully understanding the actual privacy benefits and the very real threats to startups risks unnecessarily crippling one of the most important economic sectors of our state and country.

## II. Regulations have a disproportionate effect on startups, which are the companies best-positioned to innovate and challenge incumbents.

Engine supports providing consumers with increased transparency and control over their data. In fact, startups in this state, as well as the rest of the U.S., depend on maintaining consumers' trust in the Internet.

Most of the conversations surrounding consumer privacy in recent years have focused on the headline-grabbing missteps of some of the world's largest Internet companies. The ballot initiative that led to the passage of CCPA was undoubtedly inspired by[1]—and gained momentum after[2]—some understandably controversial data collection, use, and sharing practices by Silicon Valley giants came to light. While we're long overdue for a serious policy conversation about protections for consumer data, regulating with only the largest players in mind will enshrine their market power by hurting smaller companies.

Startups have the most to lose in today's policy debate about consumer privacy and in the forthcoming implementation of the CCPA. If consumers lose trust in the Internet ecosystem, it's the products and services created by startups—which typically don't have long-standing reputations or relationships with consumers—that will be abandoned first. But if policymakers create complex and burdensome regulations, startups won't be able to afford to comply since they don't have large budgets for legal resources. Ironically, writing policies based on fears about the world's largest Internet companies' data practices could ensure that only those large Internet companies continue to exist.

It remains to be seen how CCPA compliance costs will impact startups. In discussions with our statewide network of companies, it's clear that many have struggled to think about how to comply with the law since the law itself remains unsettled.

There is an illustrative example of how costly and burdensome privacy rules that can shut small businesses out of the market: the newly-implemented General Data Protection Regulation (GDPR) in the European Union. Less than a year since the implementation of GDPR last May, companies have started speaking publicly about the compliance costs they faced[3] in terms of dollars and person-hours and the choice to avoid these rules by leaving the European Union market.[4] Smaller companies are at a disadvantage in post-GDPR Europe. One study of the online advertising market found that post-GDPR, small ad tracking firms were most severely and negatively impacted, while Facebook suffered a small loss and Google actually realized a small increase in market share.[5] As California implements CCPA, policymakers should keep in mind the kind of disproportionate impact that regulations can have on startups.

## III. Startups need a balanced approach to the definition of personal information, which should explicitly exclude de-identified and aggregated data.

[1] https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html

[2] https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law

[3] https://www.mediapost.com/publications/article/309342/the-price-of-compliance-study-uncovers-gdpr-costs.html

[4] https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html

[5] https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr

Startups rely on data that carries little or no risk of privacy harms—especially de-identified and aggregated data—every day to innovate and improve their offerings to consumers. Engine is concerned that the current definition of personal information in CCPA is overly broad and does not explicitly exclude de-identified and aggregated data, which will consequently make it difficult for startups to comply with the obligations in the law that relate to the definition of personal information. CCPA rulemaking should clarify the law by explicitly excluding aggregated and de-identified data, as it's defined by the law (1798.140(h)), from the definition of personal information. More broadly, as the Department continues to consider future CCPA-related rulemakings such as updating the definition of personal information "to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns," Engine hopes the Department will take a balanced approach. It should avoid adding new categories of information that startups rely on but which do not pose the threat of substantial privacy harms for consumers.

## IV. Startups need clarity on methods for submitting verifiable requests for data that don't create opportunities for fraud or requirements for additional data collection.

As written, CCPA could put companies in the complicated position of either having to collect more personal information or run the risk of unauthorized disclosure of consumer data in an effort to comply with the law. CCPA requires companies to "promptly take steps to determine whether the request is a verifiable request," and the time to complete those steps cannot add to the 45 days a company has to respond to a verifiable request. While the law (1798.180(a)(7)) includes "a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account" as a verifiable request under the law, it also prohibits a company from "requir[ing] the consumer to create an account with the business in order to make a verifiable request" (1798.130(a)(2)).

If a consumer has a relationship with a company, submitting a verifiable request through the consumer's password-protected account with the company is arguably the most pro-privacy way to process consumer requests for their own data. If companies are kept from using established relationships with consumers to receive and evaluate requests, they will have to either collect additional, likely sensitive, information—such as photo or government-issued identification—or run the risk of disclosing information to a bad actor posing as a particular consumer, which triggers other risks and legal penalties. The Department should craft rules regarding verifiable requests to minimize the administrative burden on companies, the need to collect additional information, and the risk of fraudulent access to consumer data.

## V. The design and procedure of the opt-out function should include flexibility reflect the various ways startups interact with consumers.

Startups interact with users in a variety of ways. The design of everything from a website to an app to a connected device varies wildly across the technology industry and startup ecosystem. The rules regarding "a recognizable and uniform opt-out logo or button" should take those variances into account. Ideally, the Department would seek input from a diverse set of technology industry and startup ecosystem members who can provide expertise on user interfaces so that the uniform opt-out logo or button can be developed in way that clearly communicates its purpose and consequences across various interfaces and contexts.

Engine supports the Department using its rulemaking process to add some flexibility to a company's obligations once a consumer opts-out of the sale of his or her information and new burdens and obligations are triggered. Given the realities that startups face—and the realities of the data architectures they rely on—it is not practical to expect complete and immediate compliance with an opt-out request once it has been submitted by a consumer. Engine also supports the Department adding flexibility to choices consumers are granted when they want to opt-out of the sale of their personal information. The current definition of "sale" in the law (1798.140(t)(1))—specifically the inclusion of "making available...or otherwise communicating…[to] a third party for monetary or other valuable consideration"—is so broad that it will likely sweep in data sharing that could benefit consumers. The opt-out process could be constructed so consumers can opt-out of types of sales to entities they find troubling, such as data brokers, without opting out of all data sharing covered under the new law.

## VI. CCPA should retain a 30-day cure period to ensure startups can improve the security of users without immediate fear of costly statutory damages.

Currently CCPA (1798.150(b)(1)) gives businesses a 30-day window to address consumer complaints about alleged unauthorized access and exfiltrations, thefts or disclosures in violation of the law before consumers can bring a case for statutory damages. This provision allows good actors to receive notice so they can respond to security concerns before facing statutory damages. Those statutory damages can be cripplingly damaging under the law, which sets them at between $100 and $750 per consumer per incident. Policymakers have suggested removing this 30-day cure period, but we urge that the provision stay in the law. Allowing companies and consumers to communicate about security concerns without immediate fear of legal actions resulting in costly statutory damages will encourage developments that improve security for users.

## VII. CCPA rulemaking should seek to minimize compliance burdens for the diverse business models represented in California's startup ecosystem.

The startup ecosystem in California contains companies of all sizes offering products and services that depend on wildly different business models. Each company faces different regulatory and legal obligations at the state and federal level, and there is no one-size-fits-all compliance strategy. The compliance issues faced by an app that collects biometric health-related data from its users are very different than the compliance issues faced by an Internet platform that allows individuals to sell physical goods online or the compliance issues faced by a website producing children's programming. Engine appreciates the concerted efforts the Department is making in this rulemaking process to harmonize CCPA's obligations with existing obligations under state and federal law and add exceptions to CCPA when necessary to resolve any conflicts.

## VIII. Conclusion

While the trope of a young startup CEO coding an ingenious app out of a garage or dorm room with little regard for its users' privacy has pervaded popular culture, California's thriving startup ecosystem is full of companies working in good faith to protect the privacy and security of their users. Startups support giving users better and more informed control over their data. We support the overall goals of CCPA, but we hope policymakers continue to refine and clarify the law—including through the Department's rulemaking process—to ensure California's startups can innovate and compete.