Engine

“Small Business Perspectives on a Federal Data Privacy Framework”

Testimony of Evan Engstrom, Executive Director, Engine Advocacy and Research Foundation

Senate Commerce, Science & Transportation Committee
Subcommittee on Manufacturing, Trade, and Consumer Protection

March 26, 2019 | 2:30 pm

I. Introduction

Chairman Moran, Ranking Member Blumenthal, members of the subcommittee. Thank you for inviting me to testify on the role of consumer privacy protections in the U.S. startup ecosystem.

Engine is a non-profit that works with a network of startups across the nation to push for policies that advance the startup ecosystem, and right now, consumer privacy is at the top of mind for many small and new companies.

For startups, "user privacy" is more than just a regulatory concern or buzzword, it's a business imperative. With every headline-grabbing misstep by an Internet giant, consumers lose trust in the Internet economy. It's the new, small startups without name recognition, longstanding reputations, or relationships with users that consumers abandon first when that trust is lost.[1] We already see startups using privacy as a competitive advantage, recognizing that they have to do more with less in order to maintain users' trust. A strong federal privacy law that shores up consumer trust in the Internet ecosystem benefits consumers, as well as startups.

At the same time, as state and federal policymakers look to bolster privacy protections for consumers, there is a very real risk that the end result will be a complex regulatory landscape that startups on bootstrap budgets can't afford to comply with, especially compared to large companies with massive budgets and legal teams. Rules that are ostensibly pro-privacy could end up cementing the market power of those very Internet giants whose behavior sparked much of these conversations.

We've seen this with the European Union's General Data Protection Regulation, where many small companies left European markets or abandoned plans to expand to European markets rather than face the costly compliance burdens.[2] In fact, there's concrete evidence that GDPR gave the big Internet companies a boost in Europe. According to one survey, Google's ad tracker actually saw an increase, albeit small, in reach since GDPR went into effect ten months ago.[3] Facebook's ad tracker saw a small decrease, but everyone else saw significant losses. GDPR's extensive and complex obligations created new compliance burdens that large incumbents could bear but resource-constrained startups could not. Policymakers should enshrine consumer privacy protections in law, but they must work to ensure far-reaching rules promote consumer welfare without harming competition.

[1] PricewaterhouseCoopers, *Consumer Intelligence Series: Protect.me*, November 2017, available at: https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf.
[2] Hannah Kuchler, *US Small Businesses Drop EU Customers Over New Data Rule*, Financial Times, May 23, 2018, available at: https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04.
[3] Björn Greif, *Study: Google is the Biggest Beneficiary of the GDPR*, Cliqz, Oct. 10, 2018, available at: https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr.

Startups and consumer advocates are aligned in support for strong, commonsense privacy legislation. A robust, uniform set of rules that provides transparency and user choice while directly prohibiting abusive practices will increase consumer confidence and, if crafted carefully, can avoid imposing significant costs that will allow large Internet companies to grow their market share while smaller competitors struggle to cover compliance costs.

II. Congress should enshrine and build off of the goals of CCPA

We appreciate the goals of the California Consumer Protection Act as well as the ballot initiative that preceded the law. Consumers should know what types of data companies have about them and how that data is shared. These goals are important and will shore up consumers' trust in the Internet ecosystem, which will help startups grow.

While CCPA's objectives are laudable, the process leading to its passage was not. Although the ballot initiative's authors clearly spent considerable time on their proposal, the legislature spent less than a week translating the initiative's general ideas into actual bill text. As a result, California legislators were unable to fully evaluate the bill, its impact on California's startup community, or its actual value to consumers. This rushed process resulted in a well-intentioned law that is full of typos, contradictions, security loopholes, and vague obligations.

We've previously laid out our concerns about the unintended consequence of the language in CCPA.[4] The definitions in the law—specifically of "personal information" and "sale"—are so broad that they will sweep in everyday business practices small companies rely on. Its requirement that companies offer the same services to everyone regardless of consumers' privacy choices would force startups to build and maintain different business models based on different consumer privacy choices, no matter how costly to their operations. The law creates a right for a consumer to access the data a company has on her, but as currently written, it would force companies to choose between collecting more and highly sensitive information from consumers or risk complying with fraudulent access requests. The private right of action in the event of an "unauthorized disclosure" and statutory damages established by the law will create potential litigation costs that would devastate a small company. The law claims to carve out small businesses, but the exemption as written would fail to capture many California startups that are creating jobs and providing innovative products and services to consumers. While policymakers continue to refine aspects of CCPA at both the legislative and regulatory levels, several provisions that are currently set to go into effect next year will create burdens that will disproportionately impact startups.

A. Definition of sale. One of CCPA's central principles is the right of consumers to opt out of the sale of their personal data. Stated in the abstract, this may seem like an unobjectionable idea, but CCPA's implementation of this concept reveals some serious problems. For one,

[4] Engine, *Comments re: Implementing Implementing Regulations for the California Consumer Privacy Act*, March 8, 2019, available at: https://www.engine.is/news/category/engine-files-comments-to-california-ag-on-state-privacy-law.

CCPA defines “sale”[5] expansively, covering many commonplace practices that businesses rely on to provide goods and services to consumers. Specifically, the bill says that “releasing, disclosing, disseminating, making available, transferring, or otherwise communicating…a consumer’s personal information…to another business or a third party for…valuable consideration” constitutes a “sale” of data. It’s not clear what is included by “valuable consideration,” and we’ve heard from companies that routine data sharing that presents no meaningful privacy harms could be included in the definition of sale due to the vague “valuable consideration” language. For example, we’ve heard from a local delivery platform that sharing order trends with local merchants to help those retailers stock their shelves in accordance with consumer demand could constitute a “sale” of consumer data under the law, even if none of the shared data is connected with any individual consumer.

The definition of sale does exclude some consumer data transfers to service providers, but the exemption[6] provides limited protections because it relies on the narrow definitions of “service providers”[7] and “business purposes”[8] and prohibits service providers from retaining or using the data. This will severely limit the ability of startups to rely on third party vendors to run their business processes. Unlike large companies, which typically have the resources to build these capacities in-house, startups rely on outside vendors for everything from data processing, to analytics, to payment processing. We’ve already heard from companies who have trouble finding third-party vendors that provide necessary analytics services and can comply with the requirements laid out in CCPA.

B. Definition of personal information. Any sensible consumer privacy bill should recognize that different pieces of information raise different privacy concerns. Collecting information about a user’s favorite color does not pose the same risk as collecting her social security number. In attempting to protect consumers’ data from unreasonable exploitation, CCPA relies on an overly broad definition of “personal information”[9] that would cover virtually all information related in any way to an individual user, no matter how sensitive or innocuous. Under CCPA, any “information that…relates to, describes, is capable of being associated with…a particular consumer or household” is deemed “personal information” and subject to the full protections of the law. It also includes a long list of specific pieces of information that are included in the law’s definition—such as commercial information, “information regarding a consumer’s interaction with an…application,” and “inferences drawn” from other personal information—and gives the state Attorney General the authority to add more. It’s difficult to imagine any piece of user information that does not “relate to” or is not “capable of being associated with a particular user.”

[5] Cal. Civ. Code § 1798.140(t)(1).
[6] Cal. Civ. Code § 1798.140(t)(1)(C).
[7] Cal. Civ. Code § 1798.140(v).
[8] Cal. Civ. Code § 1798.140(d) et seq.
[9] Cal. Civ. Code § 1798.140(o) et seq.

Additionally, the definition does not explicitly carve out deidentified and aggregate consumer information, despite rigorous requirements around what constitutes deidentified data.[10] Taken together, the vast definition of personal information will increase the scope of the law, require companies to allow consumers to opt-out of harmless data collection and sharing, and dramatically increase the burden companies face when consumers exercise their rights to access and delete data about them without any clear consumer benefit.

C. Prohibition on differing service based on consumer privacy choices. CCPA prohibits companies from offering different prices or levels of quality of products and services to consumers who exercise their rights under the law, including the right to opt-out of data sharing.[11] In practice, this language would greatly limit the ability of companies to monetize free services, which would have a disproportionate impact on startups. Unlike large Internet companies that have been offering ad-supported free services for years, a startup entering the market will have a harder time getting new users who are unfamiliar with the company to pay for its products and services. Even if a startup can get some users to pay, the law would effectively require every ad-supported company to take on the burdens associated with establishing a payment processing system in case some users decide to opt-out. At the same time, a small company will have significantly fewer opportunities to offset the costs of offering a product or service for free using revenue streams from other parts of its business, while bigger companies are better positioned to take a loss on offering a free product or service.

The law does allow companies to charge a different rate or offer a different level of products or services so long as "that difference is reasonably related to the value provided to the consumer by the consumer's data."[12] While this phrasing is likely a drafting error and obviously unworkable—how could a company know how much an individual consumer values his own data?—even a generous reading of the law's presumed goal would present existential problems for small startups. Even if companies are forced to provide service to consumers who opt-out of data sharing practices that are fundamental to the company's business model, but are allowed to recoup the lost value directly from consumers by charging a different price or offering a different level of service so long as that difference is reasonably related to the value provided to the *company* by the consumer's data, startups would have a very difficult time estimating or defending in court what would constitute a price or quality difference that's "reasonably" related to the value of a consumer's data. As startups launch and grow their businesses, there's typically not an immediate, obvious value that can be clearly assigned to individual pieces of data supplied by consumers. Even if a data set has an explicit value in the eyes of investors, data associated with any particular consumer typically does not hold much value on its own.

[10] Cal. Civ. Code § 1798.140(h) et seq.
[11] Cal. Civ. Code § 1798.125 et seq.
[12] Cal. Civ. Code § 1798.125 (a)(2).

Even worse, this non-discrimination provision would require every company that shares user data to build the infrastructure to process customer payments in the off chance that a particular consumer opts-out of the company's data practices but wishes to pay a "reasonably related" fee instead. Larger companies might be able to bear the increased overhead of payment processing, but smaller startups will not.

D. Privacy and security problems with CCPA's right to access and delete. CCPA mirrors GDPR in that it attempts to provide consumers with a right to access and delete the personal information companies have about them. These rights, in and of themselves, are a crucial part of consumer privacy protections, but they need to be reasonably cabined to prevent unintended burdens for companies. The law provides reasonably broad exceptions for when a company does not have to complete a consumer's request to delete data, but the law should be more inclusive of practices that build in privacy protections by design, such as data minimization, aggregation, and using synthetic data. If a company has deidentified a data set or used an existing data set of personal information to create artificial data that mimics the characteristics of the real data set, it could lose the ability to "delete" a consumer's data once it has been baked into an aggregate or synthetic data set. Requiring companies to do so could actually force them to collect additional consumer personal information and reidentify the data. For some immutable data structures like blockchains, deleting user data may be technically impossible.

Of greatest concern is that the law requires companies to comply with "verifiable" consumer requests for data. While the exact requirements are expected to be fleshed out in the Attorney General's rulemaking, the law prohibits companies from requiring users to create an account in order to submit a verifiable request.[13] This restriction makes sense when talking about data brokers with whom most consumers don't directly interact, but consumer-facing companies should explicitly be allowed to require users to sign in to their accounts to make such requests. Otherwise, companies will have to collect significantly more personal information to verify that a person requesting a consumer's data is, in fact, that consumer or run the risk of disclosing a consumer's personal information without their consent.

E. Private right of action in the event of a data breach. CCPA creates a private right of action that will let consumers bring lawsuits against companies that suffer from "an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures," and the law sets the damages at "not less than one hundred dollars and not greater than seven hundred and fifty per consumer per incident."[14] Putting aside the question of what constitutes an individual "incident" in the context of a data breach, the vague language included in this provision—especially "unauthorized access…or disclosure" and "reasonable security

[13] Cal. Civ. Code § 1798.100(d).
[14] Cal. Civ. Code § 1798.150 et seq.

procedures"—will create uncertainty for startups that will ultimately be decided inconsistently in the courts. No matter how thorough a company's data security practices are, determining whether they were legally "reasonable" is not amenable to early adjudication in a lawsuit. As such, data breach litigation is a lose-lose proposition for startups: settling, paying a damages award, or even litigating a case to victory will likely bankrupt most early-stage companies, as CCPA does not envision attorneys' fees awards to the winning party. The availability of significant statutory damages wholly unrelated to any actual harm suffered creates financial incentives for any individual implicated in a data breach to bring a lawsuit, since startups will almost always be better off settling a lawsuit rather than paying a statutory damages award or incurring legal costs to dismiss a meritless claim.

F. CCPA's small business exemption fails to capture startups. We appreciate the California legislature's attempt to carve out small businesses from the onerous burdens imposed by the CCPA, but the law sets the threshold for businesses so low that few companies with users in California will qualify. The law creates three requirements to be considered a small business: a company must have less than $25,000,000 in annual gross revenues, make less than 50 percent of its annual revenues from the sale of personal data, and handle data relating to fewer than 50,000 consumers, households, or devices. In practice, setting the threshold at 50,000 consumers, households, or devices will quickly sweep in small Internet-based companies whose products and services are accessed from multiple devices. For instance, if each consumer visits a website that tracks unique visitors from a smartphone, a personal computer, a work computer, and a tablet, the 50,000 figure quickly drops to under 13,000 "users or devices." At the same time, the law doesn't include an on-ramp, meaning that a startup that suddenly becomes popular could immediately find itself in violation of the law.

Ideally, a privacy law would be clear, straightforward, and consistent enough that companies of all sizes can afford to comply, especially recognizing that even a small company can create privacy harms depending on the sensitivity and scope of the consumer data it handles. However, the many burdens created by CCPA outlined above that have little to do with actually protecting consumer privacy highlight the need for small business protections when privacy laws start with good intentions but end up with drafting errors and unintended consequences.

We hope to see these issues and more addressed as California lawmakers and the state Attorney General continue refining and clarifying the law. But the mere fact that the law is still so ambiguous in so many ways with the 2020 implementation date closing in makes it even more burdensome for startups that will struggle to become CCPA compliant on such a short timeline. Many of the companies that we work with are forced to put off planning for CCPA compliance until the law and regulations are more settled, and even the biggest startups will have to budget for outside consultants to help shape their compliance strategies. Unlike GDPR—which, despite its costs and consequences, gave companies two years to come into compliance—the CCPA enforcement date looms while the law's requirements are still in flux. If the thoroughly debated rules under GDPR still cost companies significant time and resources to comply with, the compliance costs will be even higher in light of the short timeline and rushed process for CCPA.

III. A single, federal standard is better for startups and better for users

Beyond our specific concerns with CCPA's provisions, the risk of every state adopting its own privacy laws will make it even more difficult for startups to compete with large incumbents. As each new state law goes into effect, startups will be faced with an increasingly complex—and potentially conflicting—set of requirements and obligations when it comes to how they can collect, use, store, and share user data. Even if state laws don't differ dramatically, small variations multiplied over 50 iterations will create insurmountable administrative hurdles for all but the most well-funded companies. For example, putting aside differences in specific data collection practices that each state will regulate, each jurisdiction is likely to have slightly different requirements for transparency policies, user data correction or deletion requests, and reporting obligations.[15]

Additionally, even if two state privacy laws are virtually identical, startups will almost certainly have to renegotiate all of their vendor contracts to cover compliance with each new law. Unlike massive Internet companies that can build most of their services in-house, startups rely on several—sometimes dozens—of vendors to run the day-to-day processes that keep the business running, including cloud storage, payment processors, and backend website hosting. With every regulatory and legislative update requiring downstream compliance, startups have to redo contracts with each vendor to ensure they're not inadvertently and unknowingly running afoul of the law. We've heard from startups that the contract revisions required for GDPR compliance alone created significant costs for companies, and we expect CCPA compliance to be no different. Startups can't afford to spend the time and money do this again for every state, and it's hard to see how the value to consumers of 50 slightly different state laws would outweigh the resulting costs to competition and innovation.

A single, strong federal standard written into law by Congress can ensure equal protections for users across state lines while saving startups the cost of having to comply with differences in state laws that, at best, all get at the same consumer protections in different ways.

IV. Components of a strong federal law

A single, strong federal law that preempts state laws is necessary to avoid the specific problems with CCPA and the broader anti-competitive impacts of state-by-state privacy regulation. There have been several federal legislative proposals introduced in recent months that contain provisions

[15] CCPA requires companies to provide detailed reports to any user who sends a "verifiable consumer request," but the law leaves it up to the California Attorney General to determine how a company must verify the identity of a user making a request. §§ 1798.100(d), 1798.140(y) In the absence of federal preemption, companies will have to create separate systems to comply with every state's unique process for verifying and responding to user requests.

that would address these concerns and bolster consumer privacy without harming innovation or competition. We appreciate lawmakers' thoughtful and deliberate approach on those proposals, including the several bills introduced by members of the committee. As Congress continues to consider privacy legislation, the following proposals can be incorporated in a way that protects consumers without placing undue burdens on small companies.

A. Right to access, correct, and delete. Engine supports lawmakers' efforts to provide consumers with a way to access, correct, and delete their data when it's held by companies. Consumers have a right to know what kinds of data companies collect and share, and they should be able to correct inaccurate data and disengage with a company by deleting their data. But it's important that these rights be balanced to reflect the ways that companies store and use data. If a company aggregates and deidentifies consumer data, uses real consumer data to create synthetic data sets, or uses customer data to train machine learning applications, there will be technological limits on how much the resulting data can be accurately connected back to individual consumers. Requiring companies to re-identify individual consumer data so they can comply with consumer requests to access, correct, or delete their data would end up forcing companies to collect even more user data, undermining the central purpose of privacy legislation.

B. Consumer controls over sharing data with companies. Engine supports giving consumers control over their data through a notice and consent regime with robust transparency and accountability requirements. At a high level, a federal privacy law should be careful to craft notice and consent requirements so that they don't create large obstacles to data collection—either with an opt-in mechanism or an onerous opt-out mechanism—that would harm startups' ability to collect the data they need to provide the products and services they offer. If new legislation unreasonably limits the collection of non-sensitive data, startups will be structurally prevented from competing with large Internet companies in areas that require access to data sets, like machine learning, as more established platforms have already generated these data sets over years of operation.

While meaningful user control over how companies collect and share data should be central to any federal privacy law, startups should not be forced to create new subscription-based services if some users choose to opt-out of their data practices. Startups should be permitted to compete on their chosen features and privacy practices and not forced to create an alternative service alongside their core product to reflect idiosyncratic consumer data choices. The costs associated with the non-discrimination provisions in CCPA and several federal proposals would make it significantly harder for startups to compete with large incumbents that have the resources to offer both ad-supported and subscription-based products or the brand equity to switch to a completely fee-based service. As long as a company's data practices are made clear to consumers in a truly understandable and transparent manner, startups should be able to require that consumers provide certain information in order to access the service if that information is necessary for the company to provide the service it wants to offer. For instance, if a startup publishing platform wishes to distinguish itself from larger rivals by offering a more curated product that recommends articles to users based upon an internal recommendation engine, it will need to track consumer reading habits within the website to provide reading recommendations. Allowing users to opt-out of this data collection practice while still receiving access to the core product will make it impossible for the startup to offer the service it believes will help it compete with larger incumbents. We appreciate that some federal proposals have addressed this concern by allowing companies to require consumers provide certain data—or allowing companies to deny service in the absence of the consent to collect that data—if the data is necessary to the company's operation.

C. Heightened protections for truly sensitive data. Engine supports increased user control over personal data with robust transparency and accountability requirements, but there are certain types of data that could present heightened privacy harms, and it makes sense to treat the collection, use, and sharing of that specific data differently under the law. However, it's important that the definition of sensitive data under the law be limited to truly sensitive information, such as precise geolocation information, government-issued identification numbers, biometric information, health information, financial information, etc. In instances where companies want to collect truly sensitive information, consumers should have the ability to opt-out without being denied access to the service or forced to accept a different level of quality of service. The only exception to this should be if the company truly needs the data to perform the service the customer is requesting. For instance, a mapping application needs a user's precise geolocation information to provide navigation directions as requested by the user. However, a flashlight app has no clear functional need to access a user's precise geolocation information to deliver its service to a consumer, and even if that flashlight app wanted to serve relevant advertising based on a user's location, it could target ads using more general, less sensitive data such as region or zip code.

D. Restrictions on objectionable uses of data. Under a notice and consent regime with robust transparency and accountability requirements, Engine would support additional restrictions on specific uses and sharing of data if those restrictions are targeted at activities that present increased potential privacy harms. For instance, we would support a prohibition on using consumer data related directly or indirectly to race, age, gender, and other protected characteristics to make decisions about finance, housing, or employment opportunities, including serving advertisements about finance, housing, or employment opportunities.

E. FTC rulemaking and enforcement around a federal standard. If a federal privacy law creates a uniform nationwide standard, Engine would support Congress giving the Federal Trade Commission the authority to write rules to implement the law and bring civil penalties to enforce the law. We would like to see the FTC's resources increased to meet that kind of demand. If Congress is considering giving state attorneys general the authority to enforce the federal standard, there should be some requirement that the attorneys general coordinate with the FTC to ensure consistent enforcement of a predictable federal standard.

V. Conclusion

Congress has a chance to build up from the California law by creating a single, federal standard for privacy that protects consumers regardless of where they're located, avoids competition- and innovation-limiting pitfalls, and encourages good data hygiene for companies of all sizes. 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, the U.S. startup ecosystem is full of companies working in good faith to protect the privacy and security of their users. Congress should strive to create a federal privacy framework that protects consumers without imposing unnecessary burdens that put honest startups at a competitive disadvantage to large incumbents.