November 9, 2018

Comments of Engine regarding the Department of Commerce's Request for Comments on Developing the Administration's Approach to Consumer Privacy

(Docket Number: 180821780-8780-01)

I. Introduction

Engine is a non-profit technology policy, research, and advocacy organization that bridges the gap between policymakers and startups. Engine works with government and a community of thousands of high-technology, growth-oriented startups across the nation to support the development of technology entrepreneurship. Engine promotes an environment where technological innovation and entrepreneurship can thrive by providing knowledge about the startup economy and helping to construct smarter public policy. To that end, Engine conducts research, organizes events, and spearheads campaigns to educate elected officials, the entrepreneur community, and the general public on issues vital to fostering technological innovation.

As a non-profit, 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. Engine appreciates the opportunity to submit comments on the Administration's proposed approach to advancing consumer privacy while protecting prosperity and innovation. 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.[1] Creating regulatory or legislative burdens in the name of protecting users' privacy without fully understanding the actual privacy benefits and the very real threats to startups would risk unnecessarily crippling one of the most important sectors in our economy.

II. General comments

The surge in interest around privacy protections for U.S. consumers understandably comes after several high profile missteps by some of the world's largest Internet companies. Engine appreciates

[1]Kane, T. (2010). The Importance of Startups in Job Creation and Job Destruction. Retrieved from: https://www.kauffman.org/-/media/kauffman_org/research-reports-and-covers/2010/07/firm_formation_importance_of_startups.pdf

the Administration's efforts to foster a nuanced and balanced conversation around privacy that extends beyond those missteps and includes recognition of the potential impact on startups and other small businesses.

Privacy and security are top priorities for startups, which typically can't afford the reputational hit from a bombshell news report about irresponsible privacy practices as well as established Internet companies. In fact, some startups use privacy as a competitive advantage, marketing themselves to users based on the privacy protections they offer that well-known providers of similar services don't. 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 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.

It's imperative that as the federal government looks to heighten privacy protections for U.S. consumers—especially in response to concerns prompted by the behavior of the biggest Internet companies—it not create new obligations and burdens that would be impossible for startups with bootstrap budgets and few legal resources to comply with. Creating those costly burdens would make it prohibitively difficult for new and small startups to secure enough funding and get off the ground, effectively enshrining the market power of the very companies policymakers are ostensibly concerned about.

III. Privacy outcomes

A. Transparency and accountability

Engine agrees with the Administration that consumers should be informed about how companies collect, use, store, and share their information and appreciates the Administration's acknowledgment that companies need flexibility to best provide consumers with that information depending on how a company interacts with consumers to offer a product or service. Additionally, Engine agrees that companies should conduct routine internal assessments on how they collect, use, store, and share consumer data as well as be subject to external accountability mechanisms, including regulatory bodies and privacy community watchdogs.

When discussing the obligations transferred to third-party vendors, it's worth noting how a changing regulatory landscape can uniquely impact startups and other small businesses. As the Administration states, a company that deals directly with consumers should be responsible for ensuring a certain level of accountability for privacy is carried over to the

third-party vendors who process that company's user data. Startups with small or even nonexistent legal teams lack the resources to constantly update and rewrite contracts with third-party vendors to ensure compliance with an ever-changing set of regulatory requirements.

B. Control, access, and correction

At its core, the current debate over consumer privacy online is about how much control consumers have over the data they share with companies. Engine agrees with the Administration that consumers should have reasonable control over how their data is collected, used, stored, and shared and the level of control consumers have should depend on the context in which they are sharing it, including the sensitivity of the data being shared and consumers' expectations of how it will be used. The U.S. startup ecosystem is made up of companies of all sizes across all sectors that interact with consumers in a variety of ways. Requiring intuitive controls for consumers to mandate who has access to their data and when also requires flexibility so each company can find a common-sense way to provide those controls.

Engine would like to see a federal privacy framework improve opportunities for informed user consent across the Internet ecosystem. Several policy proposals have called for either opt-in or aggressive opt-out mechanisms. Engine is concerned that either an opt-in or an aggressive opt-out regime may produce unintended negative consequences for the startup ecosystem and user privacy. Depending on how consent mechanisms are crafted, users may face "notice and consent fatigue," where the inconvenience of an ever-increasing set of privacy notifications leads consumers to blindly provide consent to avoid the hassle of processing every privacy choice. Or, if rules are crafted to make opting-out or refusing to opt-in the default choice, users may simply decline to provide consent to every data collection practice, even those that they would approve if they took the time to think about the decision. If this occurs, startups would be unable to compete in any sectors that depend on access to large datasets, because large incumbents that have been collecting user data for more than a decade would have an insurmountable advantage.

Engine also agrees that consumers should have qualified access to their own personal data held by a company and the ability, within reason, to correct or delete their own personal data that's held by a company. However, it's critical that there be clear bounds on what a user can request be corrected and deleted and that companies not be required to change or delete

data they rely on to provide their products and services, prevent fraud, or comply with legal and regulatory obligations.

IV. Goals for federal action

A. Harmonize the regulatory landscape, Interoperability, and FTC enforcement

Engine appreciates the Administration's comments on the importance of harmonizing the regulatory landscape. Since the Internet is inherently interstate and global, creating a state-by-state patchwork of laws will ensure that only companies with large legal teams are able to compete for users across state lines. A federal privacy framework should preempt individual states' privacy laws to ensure regulatory consistency and predictability, necessities for startups that are constantly launching, pivoting, and expanding.

Privacy protections should be uniform throughout the U.S., and enforcement of those protections should be predictable. Engine agrees with the Administration that the Federal Trade Commission is the federal agency most appropriate for enforcing a federal privacy framework, and Engine would support giving the FTC rulemaking authority to better enforce that framework and bring penalties for violations. Allowing other officials, including states attorneys general, to enforce a federal framework without tailored restrictions could effectively create a patchwork of 50 interpretations of a federal framework, where enforcement could dramatically vary state to state, essentially adding another layer of regulatory complexity for startups to navigate.

Engine also strongly opposes creating a private right of action, which would leave startups vulnerable to costly abusive litigation and subject them to uncertainty regarding how courts across the country will interpret obligations and penalties under a federal privacy framework. For instance, the California Consumer Privacy Act creates a private right of action for consumers whose data has been made vulnerable by a company that suffered a data breach in the absence of "reasonable" data security practices. The law also establishes statutory damages between $100 and $750 per user per incident and gives the courts wide discretion to determine penalties based on factors including the severity of the data breach and the company's worth. A federal framework that included that kind of private right of action—or even a broader private right of action that included any violation of a privacy law, which some have called for in California—could quickly have startups defending consumer lawsuits in several courts across the country and facing hundreds of thousands of dollars in potential

penalties. Even if such lawsuits were fundamentally meritless, the cost of litigating in multiple jurisdictions under different interpretations of the law would be ruinous for most startups.

Engine also appreciates the Administration's comments on interoperability. It's true that the Internet allows startups to grow their businesses across global borders. As other governments pursue privacy and security protections, the U.S. government should continue to champion policies that allow for the cross-border flow of data and push back on protectionist policies that would shut out competition from American startups.

B. Scalability

Engine appreciates the Administration's framing of the privacy debate as it relates to scalability, or determining the appropriateness of a regulatory burden based on "the scale and scope of the information an organization is handling" as well as distinguishing between organizations that have direct relationships with and collect data from consumers as opposed to third-party vendors that process consumer data on behalf of others. Engine agrees with the Administration that, "in general, small businesses that collect little personal information and do not maintain sensitive information about their customers should not be the primary targets of privacy-enforcement activity, so long as they make good-faith efforts to utilize privacy protections."

C. Comprehensive application

Consumers' privacy should be protected comparably across not just the Internet, but across all commercial interactions where user data is collected and stored. Since "comparable protections" does not necessarily require identical protections, the context of how a company interacts with consumers should be a major factor in how significant a burden it faces under a federal privacy framework. Engine appreciates the Administration's acknowledgment that varying business models and technologies can present different impacts on consumer privacy. Nowhere is that truer than in the startup ecosystem: an agriculture technology startup collecting temperature data should be treated differently under a federal privacy framework than an app that collects biometric information.

Outside of the type of data a company collects, the relationship between a company and consumers should be a factor when considering what kind of regulatory burdens to put on a company. In instances where consumers truly have no choice, companies should face

additional obligations and burdens. For instance, cable and telephone companies have exclusive relationships with their customers: if a customer wants to watch a television show or make a phone call, the customer's data about those actions will necessarily flow through the cable or phone company. That exclusivity is often heightened by the lack of competition in the telephone and cable markets in much of the company, often leaving customers with few choices. The Federal Communications Commission (FCC) has specific privacy rules in place recognizing the unique relationship between telephone companies and their customers. Until Congress passed a resolution under the Congressional Review Act in early 2017, there were similar privacy rules in place recognizing the unique relationship between Internet Service Providers and their customers.[2]

Unlike the ISP market, the Internet ecosystem is a hotbed of competition. With an open Internet, a startup with a small staff located anywhere in the country can compete with the biggest companies and reach countless users across the country and the world. While prominent companies have undoubtedly risen to the fore in certain verticals of the Internet ecosystem—such as search and social media—the Internet doesn't have several of the natural barriers to entry that the cable, telephone, and Internet service markets do. With more options to choose from online, consumers aren't forced to give their data over to any particular company and can even choose to engage with a company based on its privacy practices.

Regulators can encourage even more competition in the Internet ecosystem by boosting the industry's efforts around data portability—the policy of companies providing consumers with the means to transfer their data between competing services. Several Internet companies are already working cooperatively on the technical tools to give "all individuals across the web [the ability to] move their data between online service providers whenever

[2] The FCC has promulgated rules under Section 222 of the Communications Act, as added by the Telecommunications Act of 1996, to protect customer proprietary network information (CPNI), which is "personally identifiable information derived from a customer's relationship with a telephone company" and includes information such as a customer's call records. Under the law, "the general principle of confidentiality for customer information is that a carrier may only use, disclose, or permit access to customers' individually identifiable CPNI in limited circumstances: (1) as required by law; (2) with the customer's approval; or (3) in its provision of the telecommunications service from which such information is derived, or services necessary to or used in the provision of such telecommunications service."
Bazan, Stevens, Yeh (2007). *Government Access to Phone Calling Activity and Related Records: Legal Authorities* (CRS Report No. RL33424). Retrieved from Federation of American Scientists website: https://fas.org/sgp/crs/intel/RL33424.pdf

they want,"[3] and the European Union's newly implemented General Data Protection Regulation includes data portability requirements. The concept of data portability should be viewed as another way for consumers to exercise control over their data and increase competition in the Internet ecosystem, which will give startups more opportunities to challenge incumbents. While the issue will undoubtedly raise questions about which data belongs to which consumer and whether transferring one consumer's data could pose privacy risks to another consumer, encouraging data portability will become even more critical as the debate over a federal privacy framework advances.

V. Other considerations

A. Small business exemption

The framework as laid out by the Administration doesn't adequately consider the critical discussion around whether federal action should include an exemption for startups and other small businesses.

And while privacy advocates rightly note that even a small company can do serious privacy harms to consumers, companies covered by a small business exemption would still be subject to FTC enforcement against unfair and deceptive practices under Section 5 of the FTC Act as well as sector-specific privacy laws.

Several legislative proposals have been put forward with varying small business exceptions. Most notably, the California Consumer Privacy Act creates three criteria for determining if a company qualifies for the small business exemption. If a company has $25 million in annual revenue, derives half or more of its annual revenue from selling personal information, or has data of 50,000 or more users, devices, or households in California, it must comply with the obligations in the law. According to the drafters, the 50,000 users, devices, or households threshold was meant to exempt the true small businesses and startups. Setting the threshold so low was misguided. A new startup that provides a service across multiple devices or collects data in the course of commonplace and frequent interactions can easily hit the threshold. For example, an app that keeps passwords for consumers is likely to be used across several devices. If that app has 13,000 users (slightly more than one quarter of the "users" a company would have before hitting the small business threshold in the California

[3]Data Transfer Project: https://datatransferproject.dev/

law) but each user has the device installed across four devices (such as two laptops, a smartphone, and a tablet), the company would serve 52,000 devices and fall outside of the law's small business exemption.

While there's no perfect answer for where to draw the line around a small business exemption, Engine supports creating a nuanced exemption based on the number of employees a company has and the company's revenue rather than on a single metric like the number of users. With the promise of the Internet, even a small company can have a user base that grows quickly and disproportionately to the actual size of the company and the ability of the company to navigate complex regulatory burdens. A legislative proposal from Reps. Suzan Delbene and Hakeem Jeffries creates a "small business exemption" that relieves companies with 500 or fewer employees from certain aspects of the proposal. Crafting a broad exemption for companies with 500 or fewer companies and a reasonable annual revenue threshold could avoid some of the anti-competitive impacts of a federal privacy regime.[4] It's also critical that any small business exemption include an on-ramp or reasonable grace period so that companies don't suddenly find themselves in violation of privacy law. Creating a system of escalating obligations or deferred enforcement as a company meets and then surpasses the small business exemption's threshold would allow quickly growing companies to appropriately scale up their legal and compliance resources without forcing them to take on burdensome costs or risk violating the law—either of which can destroy a small, new startup—all at once.

B. Defining personal or sensitive information

Any federal action on privacy must stem from the understanding that user data fuels much of the economic growth and innovation happening online and in the U.S. startup ecosystem. But not all data is created equal, and not all data should require the same privacy protections. Startups often rely on anonymized, aggregated, or non-sensitive user data to provide, improve, and monetize their services. There is a clear consensus forming that certain types of "sensitive" or "personal" or "personally identifiable" data deserve additional protections under a federal privacy framework, including health data, financial data, precise geolocation information, and data about child users.

But several legislative proposals put forward definitions for "sensitive" or "personal" data that go far beyond the consensus around what data would actually expose consumers to

[4] Information Transparency & Personal Data Control Act, H.R. 6864, 115th Congress (2018).

privacy harms when collected or shared. Companies regularly rely on data about how consumers use an app or navigate a website, and making it difficult or impossible to collect and share that data will only keep companies from being able to offer innovative and convenient products and services.

Equally concerning are proposals that include vague terms such as "political preferences" or "religious beliefs," since it's not clear if those are characteristics can be inferred from a user's activity online. For instance, if a consumer navigates to a certain politically-leaning news website or downloads a religious text on a reading app, it's unclear whether that would be considered data about the consumer's political preferences or religious beliefs.

A federal privacy framework, especially one that grants the FTC rulemaking power, should include a tailored definition of "sensitive" information that triggers additional privacy protections when being collected or shared. While the FTC should have the flexibility to update its rules to keep up with changing technologies, the framework should also limit the ability the agency to dramatically alter and broaden that tailored definition of "sensitive" information.

As a part of definition sensitive or personal information, some policy proposals have put forward "non-discrimination" provisions, or language that prevents companies from offering different services or prices based on the level of data a consumer shares with the company. The California Consumer Privacy Act allows companies to offer a different service or price if a consumer exercises his rights under the law if the difference in price or service "is reasonably related to the value provided to the consumer by the consumer's data." Calculating the value of an individual's data in the context of a novel startup is likely to be an impossibly ambiguous inquiry, opening the door to costly litigation over a company's pricing decisions.[5] For a startup that might pivot or add to existing offerings and revenue streams, it would be impossible to know the value of a consumer's data and whether the difference in price or service could be deemed to be "reasonably related" to the difference in value to the startup between consumers who share their data and those that don't.

[5] In most jurisdictions, startups engaged in litigation will be unable to recover damages for lost profits because the value and likelihood of success for a new business is too speculative to properly calculate lost profits. In light of this established precedent, it seems unlikely that startups will be able to meaningfully calculate the potential lost value attributable to a single user's data, particularly considering the value of user data is generally a function of the breadth of the data set as a whole rather than any individual data point.

VI. Conclusion

Engine appreciates the opportunity to provide feedback on the broad framework articulated in the Administration's request for comment. The outline of the discussion in the request for comment sets the table for a thoughtful and nuanced conversation around the critical issue of consumer privacy. Engine looks forward to working with the Administration and other policymakers to develop a privacy framework that protects users' privacy while encouraging innovation and promoting the thriving U.S. startup ecosystem.