November 21, 2022

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex B)
Washington, DC 20580

VIA ONLINE SUBMISSION

Re: Comments of Engine Advocacy in response to *Commercial Surveillance ANPR, R111004*

To whom it may concern:

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. Data-driven innovation plays a central role in technology development and entrepreneurship, and Engine accordingly appreciates the opportunity to submit these comments as the Commission considers privacy rules impacting startups' use of data.

Startups are major drivers of innovation and emerging technology, and they make outsized contributions to economic and job growth and U.S competitiveness.[1] They operate in every state, and innovate in every sector of the economy—from advanced manufacturing to agriculture to healthcare to commerce and beyond.[2] And they do this with few resources—startups are small entities by definition.[3] The most-advantaged, investor-backed seed-stage startups are working with only around $55,000 a month (companies who have not yet raised a formal funding round, and those outside of top ecosystems possess even fewer resources).[4] These funds are used for critical business needs like research and development, customer acquisition, payroll and equipment to support their growth. Every dollar spent understanding and implementing regulatory compliance—which too often varies from state to state and jurisdiction to jurisdiction—is a dollar they cannot spend toward those growth-supporting functions. By and large, startups are honest

[1] *See, e.g.*, *The Economic Impact of High-Growth Startups*, Kauffman Foundation (June 7, 2016) https://www.kauffman.org/wp-content/uploads/2019/12/PD_HighGrowth060716.pdf.
[2] *See, e.g.*, *the State of the Startup Ecosystem*, Engine 19-20 (April 2021). https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/60819983b7f8be1a2a99972d/1619106194054/The+State+of+the+Startup+Ecosystem.pdf; *see generally* #*StartupsEverywhere*, Engine, https://www.engine.is/startupseverywhere.
[3] *See, e.g.,* 15 U.S.C. § 632.
[4] *See Startup Ecosystem*, *supra* note 2, at 5, 17-18.

businesses that want to comply, but often can't afford the legal and compliance costs—leading them to close, change business models, or avoid markets with too-high regulatory burdens.[5]

To compete and succeed in the marketplace, startups need a clear, universal set of rules that enables them to efficiently serve and reach new and existing users, and avoids burdening them with excessive compliance costs and obligations. Such a framework would benefit consumers by creating strong protections and benefit startups by promoting trust in the Internet ecosystem.

The Commission should be pursuing a pro-competition and pro-consumer protection agenda in a way that supports, rather than hurts, startups. That requires a nuanced approach that recognizes the interconnected, interdependent nature of the startup and broader technology ecosystems. Startups rely on free and low-cost services provided by other, often larger companies as the building blocks of their own companies. Often, the price points of these services are subsidized by advertising revenues. And startups use advertising tools as well, both to create revenue and reach potential customers. As a result, rules aimed at, e.g., a group of large companies will necessarily impact startups who are end users and business clients of those firms.

The need for nuance and balance in privacy rules appears to be in contrast with the Commission's current approach. Indeed, the very title of the ANPR, "commercial surveillance" is pejorative and implies dubious malfeasance on the behalf of commercial actors like startups. The opening questions likewise ask about the practices "companies use to surveil consumers" and how those practices "harm consumers." The Commission cannot arrive at nuanced results upon which to build a productive, balanced set of rules if it starts with a skewed foundation.

To create a balanced picture of the actors and actions in the consumer data space and Internet ecosystem, the Commission must integrate the perspective of startups. But startups are inherently at a disadvantage when it comes to these kinds of government processes. They and their teams are busy building companies, while large entities have ample resources and dedicated teams to impact the process. The Commission should be proactive in seeking input from startups and understanding the actual consequences for them.

I. Startups need clarity and consistency from a federal privacy framework, as well as the ability to reach new and potential users in low-cost, efficient ways. (This section addresses questions 24, 26, and 29)

[5] Note, for instance, that under 15 U.S.C. § 648, the Small Business Administration (SBA)-funded small business development centers (SBDCs) shall have access to both "business analysts to counsel, assist, and inform small business clients" as well as "part-time professional specialists to conduct research or to provide counseling assistance whenever the need arises." Congress clearly recognized that professional counsel for small businesses was prohibitively expensive and thus sought to fill the compliance gap through the SBDCs. Yet many startups have expressed that the SBDCs do not provide adequate support, including by providing counsel or professional services.

With a good idea and a decent connection to the open Internet, a startup founder can launch and grow a company with users around the country and around the world. While a startup that grows across state lines and country borders necessitates complying with multiple policy frameworks—on everything from taxes, to labor laws, and more—policymakers should seek to harmonize those frameworks where possible. That's especially true for issues like privacy, where varying and potentially even conflicting frameworks could force companies to undergo time-consuming and resource-intensive tasks, like rewriting contracts with vendors, re-architecting data management systems, or rethinking entire business models.

As the Commission considers crafting a new privacy framework, it should be wary of creating new requirements and burdens for companies that are already attempting to navigate the growing patchwork of state privacy laws. Avoiding such burdens is particularly critical when additional compliance costs have no clear benefit to the consumer and where, if anything, those costs lead to fewer market offerings or higher prices.

Engine has long advocated for a federal privacy framework crafted by Congress and enforced by the Commission that creates strong protections for consumers while setting consistent obligations and prohibitions for startups. The rise in state activity around privacy in recent years only heightens the need for a legislative solution. As Andrew Prystai, the founder of Omaha, Nebraska-based EventVesta, told Engine, the cost of complying with differing privacy frameworks can keep startups from expanding into new markets. "Part of the reason that we have not expanded into certain states like California is because of the resources required to handle California Consumer Privacy Act (CCPA) compliance, which is something that we have to think about every time we look at entering a state that has its own, unique privacy compliance requirements," he explained, calling for "a nationwide standard when it comes to data privacy policy."[6]

We're incredibly concerned that rulemaking from the Commission would not only add onto the emerging mosaic of state privacy laws, but also that they would be subject to change in the future depending on which party controls the majority of the agency and who leads the agency as Chair. Startups are not only the least equipped to navigate multiple, competing privacy frameworks, they are also not well-equipped to navigate agency rulemaking processes. Engine appreciates the attempts from both the Commission and individual commissioners to make this process accessible to individuals and companies that don't typically participate in policymaking conversations—and we would like to be a resource if the agency is interested in connecting with individual startups or startup ecosystem support organizations—but ultimately these processes play to strengths of large incumbents that can engage through in-house and outside policy experts as well as trade associations.

[6] *#StartupsEverywhere Profile: Andrew Prystai, CEO & Co-Founder, Event Vesta*, Engine (Oct. 29, 2021), https://www.engine.is/news/startupseverywhere-omaha-ne-eventvesta.

In addition to consistency, startups need clear, bright-line rules that don't require costly engagements with counsel or expensive compliance mechanisms. Crafting a framework that creates large compliance costs will make it difficult to compete with larger companies that can easily withstand increased costs.[7] In addition to literal compliance costs, startups with limited resources are hyper aware of the opportunity costs of spending time and money on regulatory compliance. For example (though taken from a global privacy context), Mikel Carmenes Cavia, Co-Founder of San Francisco-based Onfleet, told Engine that the company saw large opportunity costs when it had to build an European cloud environment following the European Court of Justice's *Schrems II* decision.[8] "The unexpected difficulty of having to prioritize such a major change to our systems has been very costly to Onfleet and we have regrettably lost prospects and customers as a result," Cavia said. Policymakers should be aware of those types of opportunity costs, though they are incredibly difficult to explore and quantify across the entire ecosystem.

Startups—which, by definition, start out with few, if any, users—also need to be able to find their users. Finding and attracting potential users is arguably the most important step to growing as a company. Startups also often offer niche products and services to specific audiences, and casting a too-wide net to obtain new customers is a waste of their limited time and resources. The ability of new, innovative companies to target their niche products and services to specific communities helps fill crucial gaps in the market that larger incumbent companies either under-invest in or don't invest in at all.

Take, for instance, Noula Health, a New York City-based company that offers basic at-home hormone testing and one-on-one coaching with health professionals at a relatively low cost. As the company explains on its website:

> "Noula was born out of a shared frustration with a healthcare system that has failed us repeatedly and in different ways. The more we talked to friends and family the more obvious it became that every woman and person with a uterus has experienced feeling dismissed, ignored, or disbelieved by our doctors. Instead of receiving care, we stopped trusting our providers, and worse, we started doubting ourselves."[9]

And as founder Noelle Acosta told Engine,[10] one of the company's goals is to reach users who belong to groups that are traditionally underserved by the medical industry, especially Spanish-speaking patients, which is why the company is planning to launch its service in Spanish. According to studies, Latina women suffer disproportionately in key reproductive health measures, including higher rates of maternal mortality and higher mortality rates from breast and cervical

---

[7] *See generally infra* §II.
[8] *#StartupsEverywhere profile: Mikel Carmenes Cavia, Co-Founder & VP of Engineering, Onfleet*, Engine (May 7, 2021), https://www.engine.is/news/startupseverywhere-sanfrancisco-ca-onfleet.
[9] *See About,* Noula, https://noula.com/about.
[10] *#StartupsEverywhere Profile: Noelle Acosta, Founder & CEO, Noula Health*, Engine (Oct. 28, 2022), https://www.engine.is/news/startupseverywhere-newyork-ny-noulahealth.

cancer, and they are less likely to receive regular mammograms and pap tests.[11] With the overlapping audiences of women and birthing people and Spanish-speakers, Noula has plans to reach their target users with online ads. "All of our growth is user-generated word of mouth from people looking for information about how to better take care of their bodies. And as we grow, we will be investing in online ads to reach users who may be looking online for that information," Acosta told Engine.[12]

II. An overly burdensome privacy framework will make it more difficult for startups to compete against large and incumbent companies. (This section addresses questions 27, 39, and 50.)

Any new privacy obligations the Commission creates will necessarily impact competition and will particularly impact startups. Burdensome, costly rules will advantage large incumbent firms and burden innovative entrants, as they have with previous privacy rules and other regulations.[13] The Commission should be especially concerned with these consequences of the current proposed rules that contemplate changes to the online ad ecosystem because those personalized ads are both effective, low-cost means of reaching customers and potential sources of revenue.[14] In this light, the Commission must recognize that while competition and protecting consumers is not a zero-sum game, if not done thoughtfully, privacy rules can be onerous for startups and inhibit competitive entry.

Onerous, expensive rules can create regulatory moats that advantage large incumbent firms while burdening entry from small innovative companies like startups. For example, many companies found the European Union's General Data Protection Regulation too burdensome and in response left the EU market.[15] Several small companies use geoblocking technologies to avoid serving EU users since it does not yet make financial sense for them to serve EU users.[16] Large companies, meanwhile, have continued to serve the EU market without such fundamental business interruptions. Likewise in the U.S., startups have avoided expanding into or serving users in certain states with privacy laws that carry compliance costs that they cannot yet afford, as highlighted above.[17] Initial compliance with

---

[11] *See, e.g.*, Blanca Ramos et. al, *Latina Women: Health and Healthcare Disparities*, 258-271 Social Work in Public Health 25:3-4 (2010), https://www.tandfonline.com/doi/full/10.1080/19371910903240605.
[12] *Supra* note 10.
[13] *See, e.g.*, Rosyln Layton & Julian McLendon, *The GDPR: What It Really Does and How the U.S. Can Chart a Better Course*, III(A), III(E) Federalist Society Review (Oct. 29, 2018), https://fedsoc.org/commentary/publications/the-gdpr-what-it-really-does-and-how-the-u-s-can-chart-a-better-course; David Roland-Holst, et. al, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations*, Berkeley Economic Advising and Research 10-11 (Aug. 2019), https://engine.is/s/BEAR-CCPA-Impact-Assessment.pdf.
[14] *See, e.g.*, John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, IAB (Oct. 2021), https://www.iab.com/wp-content/uploads/2021/10/IAB_Economic_Impact_of_the_Market-Making_Internet_Study_2021-10.pdf; *The importance of targeted advertisingfor startup ecosystems in Europe*, Allied for Startups (Nov. 18, 2021), https://alliedforstartups.org/2021/11/18/the-importance-of-targeted-advertising-for-startup-ecosystems-in-europe/.
[15] *See, e.g.*, Layton & McLendon, *supra* note 13.
[16] *See, e.g.*, *id* at III(A).
[17] *See, e.g.*, *supra* §I; *Prystai*, *supra* note 6.

the California Consumer Privacy Act, for example, costs an estimated $50,000[18]—consuming a month of a startup's runway.[19] Startups' responses to consumer privacy laws are not because they do not want to comply but rather represent the best choice as they work to compete with the limited resources at their disposal.

Beyond compliance costs, the privacy rules contemplated by the Commission can impact the amount of revenue a company can generate, too. Startups rely on personalized, targeted advertising in two ways. First, startups use targeted ads to reach and find new customers. Because many startups necessarily offer niche products and services—targeted advertisements are the most effective way to spend their limited marketing resources.[20]

Second, many startups offer their services for free and generate revenue by selling ad space. This advertising subsidizes free content and services, which is to the benefit of startups and other new entrants to the market who don't yet have large and loyal audiences. If startups could no longer subsidize their services with advertising—as a result of purpose limitation rules or otherwise—and had to charge users for access, it would be harder for them to grow, diminishing both competition and options for consumers.

More generally, startups do not have the infrastructure to do many fundamental business functions on their own. Instead, they rely on dozens of companies—including those who also provide "specific enumerated services"[21]—who offer those functions, often at relatively low costs that are possible because the enumerated service providers serve advertisements to create revenue. The Commission should not adopt rules that unnecessarily complicates the ability of startups to use third-party services for everything from data analytics, to web hosting, and more. Doing so would ultimately negatively impact end users—including startups—through higher prices for those products and services and increased compliance costs. Should the Commission limit the ability of service providers to participate in the advertising ecosystem, costs for those services would inevitably increase for end users—redirecting how startups allocate their limited resources and diminishing their overall competitiveness.

III. Unnecessarily restrictive data collection and use limitations will hinder startups and their ability to grow and expand their business offerings. (This section addresses questions 10, 43, 44, 45, and 46.)

Some types of data and some uses of data present such clear potential harms to consumers that a federal privacy framework should prohibit those kinds of collections and uses, but the Commission

[18] *See, e.g.*, Roland-Holst et. al, *supra* note 13.
[19] *See Startup Ecosystem*, *supra* note 2, at 5, 17-18.
[20] *See, e.g.*, *importance of targeted advertising forstartup ecosystems*, *supra* note 14.
[21] *Id.*; *see generally Display Advertising Ecosystem,* https://www.researchgate.net/figure/Display-advertising-ecosystem_fig3_321805749 (illustrating the volume of services involved in the advertising ecosystem).

should be incredibly precise in identifying those kinds of prohibitions to avoid limiting startups' ability to use data in innovative, innocuous, and beneficial ways. Especially when considering limiting or prohibiting types of data that can be collected, the Commission should weigh the context and potential consumer benefits of that data. Take, for instance, biometric data that fuels facial recognition technology. While biometric data, and facial data specifically, can have incredibly privacy-invasive uses, a startup that uses data to recognize when a human face is present—to, for example, accurately blur the background when a face is present on a screen—shouldn't face the same kind of burdens as a company offering a more privacy-invasive product or service. Rather than eliminating uses of entire categories of data, the Commission will have to do careful, detailed, and forward-looking analysis to sort out what uses of each specific kind of data should be limited.

Additionally, limiting the collection and retention of data to only "the extent necessary to deliver the specific service that a given individual consumer explicitly seeks or those that are compatible with that service" will limit a startup's ability to develop new products and services or even pivot to new business offerings. Startups often start with one product or service in mind and then shift or expand as they identify other or additional opportunities.[22]

IV. Startups need a data security framework that accounts for the breadth and diversity of the ecosystem, incentivizes responsible actors, and creates clear and consistent expectations. (This section addresses questions 32 and 35.)

Data security is not a one-size fits all solution. As Engine told lawmakers during a Senate Commerce Committee hearing last year:[23]

> "The startup ecosystem isn't a monolith, and each company's risk assessment and security measures are going to look different. A two-person startup collecting non-sensitive data from a handful of users will have a very different risk profile than a larger startup collecting sensitive data from thousands of users. At the same time, a new and small startup won't have the resources to spend on the security and compliance measures that a larger company will. Being responsible stewards of user data will look different for every company, depending on its resources as well as the sensitivity and amount of data it has."

Instead of rules that treat all data-holders equally, a federal data security framework should establish standards based on how much and what kind of data a company collects. And a startup should be able to easily figure out whether and how to comply with those standards using readily available tools and techniques.

---

[22] *See generally infra* §VI.

[23] *Hearing on Enhancing Data Security: Hearing Before the Comm. on Commerce, Sci., and Transportation*, 117th Congress (2021) (testimony of Kate Tummarello) https://www.commerce.senate.gov/services/files/3B1B0CB5-B41E-4542-B981-9581B2387FE5.

In addition to setting a floor for practices to protect consumers' data, a data security framework should incentivize pro-security practices. Many startups see pro-privacy and pro-security measures as their competitive advantage and already take additional steps beyond standard best practices to keep their users' data safe. These kinds of companies should be rewarded for their proactive efforts. One way to do that is found in existing state law, as we described in our testimony to Senate Commerce:[24]

> "One bright spot in the current policy landscape is where state laws incentivize security measures by, for instance, easing compliance burdens if a data breach impacts only encrypted data. Encryption is one of the most effective ways startups can secure their users' data, and startups can benefit from policies that encourage and incentivize strong security measures, including encryption and data minimization. As Ben Golub, CEO of Atlanta-based encrypted, decentralized cloud storage company Storj, explained, 'we design our decentralized systems so there are no single points of failure, and so that they are highly resistant to both traditional and ransomware attacks. The widespread use of encryption is key to protecting sensitive consumer, financial, healthcare, and research data from compromise—by us or by bad actors—and those are the kinds of measures we should be encouraging.'"

Ultimately, a data security framework must also recognize that even the most responsible actors can fall victim to a data breach, and that depending on the scope and the type of data involved, not all data breaches should be treated equally. Startups already have to navigate varying and sometimes conflicting state laws around data breach notification. A federal framework should harmonize, not further complicate, the regulatory burdens a startup has to comply with if—despite its reasonable and responsible efforts to protect against data breaches—it is the victim of a data breach. As noted above, a patchwork of requirements and prohibitions—including around data security—will create disproportionate burdens for startups looking to grow across state lines, and policymakers should prioritize a single, consistent set of rules with a federal framework crafted by Congress and enforced by the Commission.

V. Startups need bright line rules that don't require general audience websites and services to collect additional data to determine users' ages. (This section addresses questions 15, 18, 21, and 23.)

Many startups that have products and services aimed at general audiences unknowingly and unintentionally have users that are children. The current framework under the Children's Online Privacy Protection Act allows startups aimed at general audiences to operate without having to determine the age of every user while ensuring that those that want to create products and services aimed at children—the definition of which is established under the law with a bright line cutoff—have heightened protections for their young users' privacy. If startups with general audience

[24] *Id.*

users have to determine the age of their users to, for instance, apply different privacy settings by default, startups will have to collect and maintain more data than necessary.

Take, for instance, Overland, Kansas-based Bryght Labs, which makes ChessUp, a smart chess board that lets players of varying skill and experience levels learn and play chess with a global community of players. As founder Jeff Wigh told Engine, "ChessUp came from the idea of making the learning experience of chess much more accessible and immediate, allowing kids to play a game right out of the gate…with their family and not have to worry about the skill differences."[25] ChessUp maintains user profiles to track games, record stats, and match players up against one another, but the company doesn't keep data about the age of its users, as its product is meant for all ages. "Our experience is built around making chess easier and more approachable to learn. We want the experience to connect to our product to be brief and convenient as well," Wigh told Engine. "As a company, we don't want to be in the position of having to collect and retain information about our users' ages or implement age restrictions. That would create a burden for us and be privacy-invasive for our users."

While the Commission is examining online protections for children, it's critical that it recognize the role encryption plays in protecting all Internet users, including children's data and devices.[26] Recent policy proposals risk undermining encryption in the name of children's safety, but as the Commission looks to advance both privacy and data security protections, it must recognize that encryption is one of the most readily available methods that companies, including startups, have to protect their users. Policies that force companies to introduce intentional vulnerabilities into their products and services weakens privacy and security for all users, including children.

VI. Many startups use "algorithmic decision-making" in innovative ways to compete and provide tailored solutions to consumers. (This section addresses questions 48, 56, 57, and 59.)

Any federal privacy framework must recognize that the use of algorithmic decision-making is widespread across the technology ecosystem and is a key tool that many companies, including startups, use to differentiate their products and services and create personalized, tailored solutions to their users. One set of rules—such as restricting the use of algorithmic decision making systems or requiring companies using those systems to comply with evaluation and certification requirements—will create disproportionate burdens on the vast range of startups employing algorithmic decision-making in a wide variety of ways and contexts. Even rules that attempt to identify high-risk uses of algorithmic decision-making could include innocuous and beneficial uses.

---

[25] *#StartupsEverywhere Profile: Jeff Wigh, Founder &CEO, Bryght Labs*, Engine (Feb. 4, 2022), https://www.engine.is/news/startupseverywhere-overlandpark-ks-bryghtlabs.
[26] Natalie Campbell, *A Safer Internet Starts with More Encryption*, Internet Society (Feb. 8, 2022), https://www.internetsociety.org/blog/2022/02/a-safer-internet-starts-with-more-encryption/.

For instance, San Francisco-based Scoop provides a service that allows employers to match employees up to carpool together using the company's algorithm.[27] And Noula uses an algorithm to recommend healthcare information for users to have more informed conversations with their outside medical professionals.[28] These are two examples of companies that operate in what could be defined as sensitive spaces—employment and healthcare—but their services focus on using algorithms to add features and expand access to information, not excluding users from opportunities.

And regulatory burdens will be especially difficult for startups to shoulder, limiting the number of new companies that compete in the algorithmic decision-making space. Prystai's startup EventVesta uses an algorithm to curate events posted on the platform based on the interests and preferences of its users, and he warned against policies that would limit the ability of startups like his to compete on algorithm-based curation:[29]

> "[N]ot having the ability to build a more sophisticated algorithm would be a massive hindrance to our long term ability to grow. This would impact our ability to compete with foreign companies, and frankly would create some regulatory capture and give an unfair advantage to established companies by allowing them to grandfather in prior work while putting a large cost burden on new entrants in this space."

The Commission should also consider the impact that unnecessarily broad data minimization requirements will have on startups looking to build algorithms to help them scale and better serve their users. Startups' goal is to scale, and they are likely to collect data with the goal of building better products and algorithms in the future to support those efforts. Startups are already inherently at a disadvantage when building algorithms, as it can be expensive and time consuming for new companies to obtain data and virtually impossible to obtain the kinds of data sets large incumbent companies have spent years or decades building.[30] Data minimization requirements could frustrate this path to scalability and undermine their competitiveness.

VII. Startups should be subject to the Commission's civil penalty leniency program, consistent with the Small Business Regulatory Enforcement Fairness Act (SBREFA).

(This section addresses question 94.)

Given FTC investigations and enforcement actions can have the effect of shutting down a small business, it is essential that the FTC counterbalance any of its proposed remedial authorities against

[27] *#StartupsEverywhere profile: Charles Knuth, Senior Director, Strategic Research Initiative, and Lizzie Ryan, Communications Manager, Scoop Technologies*, Engine (Apr. 3, 2020), https://www.engine.is/news/startupseverywhere-san-francisco-calif.
[28] *Supra* note 10.
[29] *Supra* note 6.
[30] *See, e.g.*, *RFI Response: National AI Research Resource (NAIRR)*, Engine (Sept. 1, 2021), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/612fd79874a9b127a859bbd2/1630525336986/NAIRR+RFI.pdf.

the mandates in section 223 of SBREFA.[31] That mandate directs the FTC "to provide for the reduction, and under appropriate circumstances for the waiver, of civil penalties for violations of a statutory or regulatory requirement by a small entity."[32] For startups that meet the small entity definition under the Small Business Act, it is crucial that the FTC consider less-burdensome enforcement tools for ensuring compliance, including but not limited to requiring a startup to correct the violation within a reasonable correction period or requiring a startup to participate in a compliance assistance or audit program.

While startups would be most benefited by a federal privacy framework crafted by Congress, if the Commission proceeds with a new trade regulation in this space, it should look to minimize penalties for startups in accordance with its report to Congress on SBREFA.[33] Civil penalties, like compliance costs, will fall disproportionately on startups, and the Commission should show leniency to the small and new companies that are making good faith efforts to keep up with a shifting patchwork of privacy obligations. The Commission should also avoid taking a wide view of the health, safety, environmental, or economic harms that exempt a company from leniency since, as discussed above, a startup may be operating in, for instance, the health space but not in a way that could facilitate significant harm. The FTC should limit its enforcement to those startups which have engaged in willful conduct, exercised bad faith, or committed Federal Trade Commission Act violations that lead to actual and significant health, safety or environmental harms.

* * *

Thank you for the opportunity to submit feedback as the Commission considers creating privacy rules. Startups need a consistent federal privacy framework that creates clear obligations for companies while preserving their ability to reach potential users in efficient, low-cost ways. We look forward to engaging with the Commission as the process moves forward.

Sincerely,

Engine

Engine
700 Pennsylvania Ave. SE
Washington, DC 20003
policy@engine.is

[31] 5 U.S.C. § 601, *note.*
[32] *Id.*
[33] *Report to Congress: Small Business Regulatory Enforcement Fairness Act*, Federal Trade Commission (Mar. 1998), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-congress-concerning-small-business-regulatory-enforcement-fairness/sbrefa98.pdf.