



April 30, 2024

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Washington, DC 20580

VIA ONLINE SUBMISSION Re: Impersonation SNPRM, R207000

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. We appreciate the opportunity to comment on the agency's work to combat impersonation fraud. Startups certainly benefit from the increased consumer trust in the marketplace that can be achieved by mitigating impersonation fraud, but enforcement changes that consider online and technology service providers liable for the violative conduct of their users will make it risky and costly to offer any product or service that could, theoretically, be used in a fraudulent impersonation scheme. These comments address questions four and seven of the SNPRM.

I. Startups benefit from clear legal standards, such as an actual knowledge requirement.

The U.S. startup ecosystem has thrived under existing liability frameworks that correctly recognize that service providers have limited, if any, visibility into and control over how users use their products and services when they're widely available on the market. And startups on bootstrap budgets contend best with bright-line rules that are clearly articulated and applied consistently. The proposed § 461.5 "Provision of Goods or Services for Unlawful Impersonation Prohibited" includes a standard of "knowledge or reason to know," which creates less certainty than an actual knowledge standard and opens the door to startups facing the unrealistic expectation that they investigate or even predict whether any one user will use their product or service in a way that violates the Commission's rule.

As noted in the SNPRM, a wide range of companies could fall into the broad category of "individuals or entities that provide the means and instrumentalities for impersonators," including Internet companies like dating websites and social media platforms. The startups innovating in these two realms, just as an example, already invest significant energy in content moderation to keep their corners of the Internet safe, healthy, and relevant for their users.¹ Despite those efforts, they cannot ensure that their platforms will

¹ See, e.g., #StartupsEverywhere profiles: Heather Hopkins, Founder & CEO, Hulah (Oct. 20, 2023) <https://www.engine.is/news/startupseverywhere-losangeles-calif-hulah>, and Andrew Prystai, CEO and Co-Founder, Event Vesta (Oct. 29, 2021) <https://www.engine.is/news/startupseverywhere-omaha-ne-eventvesta>



never be used by one person impersonating another. Given how broadly this rule will touch on the Internet and startup ecosystems, a requirement that providers have actual knowledge that their products or services are being used for unlawful impersonation would create more certainty and avoid stifling legitimate business activity.

II. The ecosystem of artificial intelligence companies is large, diverse, and rapidly evolving.

While the text of the SNPRM doesn't specify a focus on artificial intelligence technologies, the Commission's public statements² on the proposed expansion of the rule have been largely focused on the use of artificial intelligence to generate "deepfake" images, videos, or text that could be used to impersonate a government entity, business, or individual. While the problem of impersonation fraud using artificial intelligence is well documented, the proposed expansion of the rule is not sufficiently tailored, and it will impact a broad sweep of legitimate and socially beneficial uses of artificial intelligence. Artificial intelligence—including generative artificial intelligence—is still an emerging technology for which innovators are still discovering new and beneficial use cases. Imprecise regulation that places burdens on them—and not specifically on malevolent actors exploiting technology for illegal purposes—is the wrong approach and should be avoided. Coupled with the knowledge standard discussed above, promulgating rules that will affect such a large, diverse, and rapidly evolving ecosystem runs the risk of chilling innovative artificial intelligence startup activity.

* * *

Thank you for considering our feedback as the Commission proposes rules on impersonation. We hope to be a resource as the Commission considers the perspective of startups, and we look forward to engaging with the Commission as the process continues.

Sincerely,
Engine

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

² Press Release, Federal Trade Commission, FTC Proposes New Protections to Combat AI Impersonation of Individuals (Feb. 15, 2024), <https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-proposes-new-protections-combat-ai-impersonation-individuals>.