Before the Senate Committee on Commerce, Science, and Transportation

Hearing on Enhancing Data Security

Testimony of Kate Tummarello
Executive Director, Engine

October 6, 2021

Chair Cantwell, Ranking Member Wicker, members of the committee, thank you for the opportunity to testify before you today. My name is Kate Tummarello, and I am the executive director of Engine. Engine is a non-profit organization based in Washington, D.C. that works with a nationwide network of thousands of startups to advocate for pro-startup, pro-innovation, pro-entrepreneurship policies.

I'm especially appreciative to be here today, because most of the current technology policy debates focus on concerns about how the largest industry players handle, or mishandle, consumer data. But startups are critical contributors to innovation and economic and job growth in the U.S. and have a unique perspective and need: a data security framework that accounts for the breadth and diversity of startup companies; sets clear, consistent expectations; and protects responsible actors from unwarranted legal and compliance costs in worst case scenarios.

For many startups, data security is a business imperative. Startups often don't have the name recognition or long-standing relationship with consumers that larger companies do. While high profile data breaches of large corporations and major retailers may take up headlines and congressional attention, those companies live to see another day. For a startup, one data breach can drive away users and investors and ruin a company. Startups have to constantly balance competing goals while building out a successful product or service and cultivating a satisfied user base—one of the many things they have to consider is securing user data. In fact, many startups see privacy and security as a competitive advantage and use strong security measures as a way to differentiate themselves from others in the industry.

But making user trust and data security a priority doesn't mean a startup, or any organization, can't become the victim of a cyberattack. In fact, every startup has to grapple with the fact that it could be the victim of a data breach. According to the Identity Theft Resource Center, there have been more than 1,000 data breaches every year since 2016,[1] and data breaches in the first half of 2021 are on pace to exceed last year's numbers.[2] We sometimes hear about obvious, irresponsible behavior—like losing an unencrypted hard drive—but unintentional errors can still happen at responsible companies. If one employee responds to a phishing email or uses the same password across multiple services, a data breach can occur.

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

---

[1] *2020 in Review: Data Breach Report*, Identity Theft Research Center 10 (Jan. 28, 2021), https://notified.idtheftcenter.org/s/2020-data-breach-report.

[2] *First Half of 2021 Data Breach Analysis*Identity Theft Research Center 1, 2, https://notified.idtheftcenter.org/s/2021-first-half-data-breach-analysis (last visited Oct. 4, 2021).

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. Federal data security policy needs to recognize that. As Aaron Vick, a startup advisor and former startup CEO from Jackson, Mississippi put it, "smart data security practices will and should look different for every startup. Smart and helpful data security policy should promote flexible data security practices, not make life harder for startups who are victims of data breaches."

And if a startup is a victim of a data breach, it has to spend its very limited time and resources detecting, mitigating, and investigating the breach. According to a recent survey, small firms suffer the largest losses from cyber threats relative to company size. Companies with fewer than ten employees reported spending a median of $8,000 in response to cyber attacks, but for some those costs climbed higher than $300,000 per year.[3] By contrast, the average seed-stage startup only has about $55,000 to spend per month[4]—a sum that needs to cover salaries, equipment, research, development, marketing, and more. And since the vast majority of startups do not, or do not yet, have outside funding, most startups have significantly less than $55,000 per month to spend.

A complicated regulatory and legal regime makes a disastrous situation worse for a startup in the wake of a data breach. Congress should create a federal framework that gives startups clarity on the measures they need to implement to protect consumer data and the steps they need to take if they suffer a data breach. A federal framework should also create certainty that startups won't face legal and regulatory burdens if they suffer a data breach despite their precautions.

The current patchwork of state laws provide unclear data security standards on the front end, and varying or even conflicting requirements in the wake of a breach, which creates ambiguity and uncertainty for startups that want to protect their users. For example, in notifying users of a breach, Michigan law requires companies to describe the incident that led to a data breach, while Massachusetts prohibits notices containing that sort of information.[5] And because startups almost always have users in multiple states, the first step of notifying users of a data breach can often involve hunting down additional user data the company might not otherwise have or need to determine where users are located and which state laws are implicated. These state-by-state differences drive up startups' compliance costs without making consumers any safer.

In addition to having to navigate state laws, startups also have to worry about being sued if they are victims of a data breach in some states. A lawsuit—especially one where an organization's data

---

[3] *Hiscox Cyber Readiness Report 2021*, Hiscox 9 (Apr. 2021), https://www.hiscoxgroup.com/sites/group/files/documents/2021-04/Hiscox%20Cyber%20Readiness%20Report%202021.pdf.

[4] *The State of the Startup Ecosystem*, Engine 17 (Apr. 22, 2021), https://engineis.squarespace.com/s/The-State-of-the-Startup-Ecosystem.pdf.

[5] Jeff Kosseff, *Hacking Cybersecurity Law*, 2020 U. Ill. L. Rev. 811, 838-39 (2020).

security measures are dissected in a lengthy discovery process—can easily cost hundreds of thousands of dollars in legal fees,[6] which would entirely deplete a startup's limited resources. This approach to enforcement also opens up the door for courts to issue inconsistent rulings about what security measures are adequate under the law,[7] which creates compliance confusion and costs that fall disproportionately on startups. It also creates opportunities for malicious or misguided lawsuits where, for instance, a startup is sued by a competitor or faces a nuisance value lawsuit and chooses to settle rather than engage in lengthy and expensive litigation.[8] Again, a federal framework should create clarity and consistency and restrict the opportunities for bad faith litigation.

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."

As Congress considers ways to increase data security for consumers across the Internet, lawmakers should keep startups in mind. Congress should create a federal framework that incentivizes strong security measures that make sense for startups and their unique risk profiles, allows room for the universe of responsible security measures to grow and adapt as the cybersecurity threat landscape evolves, and creates consistency and certainty for responsible actors, including ensuring that they won't face unnecessary burdens in the event of a data breach.

Finally, Congress should promote training and support for a top cybersecurity talent pool—and therefore a diverse cybersecurity talent pool—because these professionals will be vital to keep pace with emerging technology and new threats, and because they can (and should) be a part of ongoing policy discussions about data security. As Safi Mojidi, Founder of Hacking the Workforce, has explained: there are "legislative gaps [that] should be addressed immediately in order to achieve more

---

[6] Marcia Ernst, *Data Breaches: They're Not Just Problems for the IT Department — They Can be Legal Headaches Too*, SGRLAW (Summer 2016), https://www.sgrlaw.com/ttl-articles/data-breaches/.
[7] *Cf.* Kosseff, *supra* note 5, at 823-27 (discussing the possibility of shifting or unclear decisions in data security orders).
[8] *Cf. TCPA Litigation Sprawl: A Study of the Sources and Targets of Recent TCPA Lawsuits*, U.S. Chamber Institute for Legal Reform (Aug. 31, 2017), https://instituteforlegalreform.com/research/tcpa-litigation-sprawl-a-study-of-the-sources-and-targets-of-recent-tcpa-lawsuits/ (discussing expanding trends in Telephone Consumer Protection Act suits targeted against legitimate U.S. businesses, and not just "unscrupulous scam telemarketers").

consistent standards for how organizations use personal information, while also providing industry with clear national guidance on how to protect privacy and security. [But w]hen thinking through the consequences of policy decisions, we need to make sure we have some of the brightest, diverse minds in the room, who can think about the impact on entire communities that policies would have."[9]

We appreciate the committee's attention to this issue and the broader effort to create a federal privacy framework. We hope lawmakers will continue to take into account the unique challenges startups face in this space and find a legislative solution that works for the thousands of startups that want to be secure, responsible, and successful. To quote Tony Hyk, CEO of Minneapolis-based digital health startup TheraTec, "if lawmakers are going off an assumption that every business is trying to do bad things, then they don't understand startups. There will be a few bad actors, but legislating for the lowest common denominator is not the right approach."

[9] *#StartupsEverywhere profile: Safi Mojidi, Founder, Hacking the Workforce*, Engine (July 9, 2021), https://www.engine.is/news/startupseverywhere-alexandria-va-hacking-the-workforce.