PRIVACY

Why it matters to startups:

Much of the conversation around privacy and data security focuses on large Internet companies, but startups have to navigate the same legal and regulatory framework around data without the resources of their larger counterparts. Several states have privacy laws coming into effect, more states are considering their own, and Congress and agencies like the Federal Trade Commission are looking to advance privacy rules, with many proposals tailored to young users. These efforts have similar overarching goals but contain relevant differences that leave startups to grapple with varying requirements and obligations that increase costs.

The evolving and varying laws at the state level add to a longstanding patchwork of state data security and data breach notification laws, which create disparate requirements about how startups have to protect against data breaches and what a startup has to do to notify users if it is the victim of a data breach.

KEY TAKEAWAYS:

- Startups prioritize their users, and to that end spend hundreds of thousands on their privacy and compliance programs, but each new state with a unique privacy law adds another tens of thousands in duplicate costs.
- Startups need one uniform, consistently enforced set of rules around user privacy to provide predictability, streamline costs, and promote stability as they launch and grow, especially as several varying state privacy laws take effect.

What policymakers can do

Policymakers should prioritize crafting a uniform federal privacy and data security framework that creates certainty for startups while providing strong protections for consumers. Over a dozen states have enacted unique data privacy laws, and more are gearing up to pass their own in 2024. The 117th Congress came closer than ever to passing a comprehensive federal privacy framework, but familiar sticking points hindered progress, including whether and to what extent the federal framework would preempt state laws and how to enforce the law. Congress should create one federal standard so startups know their obligations and responsibilities under the law, regardless of where they're located, and that framework should be consistently enforced to ensure certainty and to minimize opportunities for bad actors to weaponize costly legal action against startups.

Policymakers should also defend the ability of technology companies to protect their users through encryption. The push for "backdoors"—or intentional vulnerabilities in hardware or software that can be exploited by law enforcement—will do more harm than good by opening up products and services and their users to malicious actors.

STARTUP SPOTLIGHT

Inspirit VR

(Palo Alto, Calif.)
Aditya Vishwanath, Co-Founder & CEO

Inspirit is a virtual reality technology platform that revolutionizes the way children learn by providing immersive experiences in the classroom.

"[I]n the U.S., many states have their own rules—or no rules—and we have to approach compliance in every state on a case-by-case basis. Most people who are creating platforms like me have no legal or policy background whatsoever. We're all engineers, designers, or creators. So trying to figure out how to build a business in an environment with differing rules about the same issue becomes hard and expensive."