User 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. As several states consider and pass their own privacy laws —many of which are written with the same overarching goal but contain small differences—startups are left to grapple with varying requirements and obligations that increase compliance and legal costs. The evolving and varying laws at the state level adds 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. A federal privacy and data security framework can create consistency for startups while ensuring strong protections for consumers.

Key takeaways:

- Startups need one uniform, consistently-enforced set of rules around user privacy to provide predictability and stability as they launch and grow.
- As policymakers think through privacy and data security rules, it's crucial that they consider the impact on small and new companies.
- Startups can benefit from reasonable, commonsense privacy and data security rules that help restore consumers' faith in the Internet ecosystem and ensure access to markets around the world.
- A federal framework should incentivize pro-privacy and strong security measures that make sense for a wide range of startups and their unique risk profiles without creating unncessary compliance costs or legal risks.

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. Virginia, Colorado, and California have passed their own laws in recent years, and more states are set to act in 2022. While Congress has spent much of the last few years discussing a federal privacy framework, several sticking points remain, including whether a 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.

Additionally, policymakers should 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

Storj
(Atlanta, GA)
Ben Golub, CEO

Storj is an encrypted, decentralized cloud storage provider that utilizes its own digital token to facilitate transactions.

"Privacy is just one particular area where many startups struggle to understand what is required of them. . . .As policymakers grapple with these issues, it is important that they give startups a role in policy debates. There are things that Amazon, Microsoft, or Google can do that startups cannot, so it helps level the playing field when the voices of startups are included in policy debates."