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 their own privacy laws coming into effect, more states are considering their own, and the Federal Trade Commission has initiated a rulemaking process for privacy rules. Many of these efforts have the same overarching goal but contain relevant differences and startups are left to grapple with those varying requirements and obligations that increase compliance and legal costs.

Key takeaways:

- Startups can benefit from reasonable, commonsense privacy and data security rules that promote trust in the Internet ecosystem.
- Startups need one uniform, consistently-enforced set of rules around user privacy to provide predictability and stability as they launch and grow, especially as several varying state privacy laws take effect.
- 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 unnecessary compliance costs or legal risks that they cannot afford.

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.

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. Five states have data privacy laws that will enter force this year and more states are set to act. The 117th Congress came closer than ever to passing a comprehensive federal privacy framework, but familiar sticking points hindered progress, including whether 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 additionally 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

People Clerk
(Miami, FL)
Camila Lopez, Co-Founder

People Clerk helps users of all backgrounds navigate small claims courts.

"We haven't had any issues with putting all necessary safeguards in place to protect our clients' information, but it is difficult navigating compliance with the different privacy laws out there. Currently, the rules can vary significantly on a state-by-state level. On top of that, our attorneys keep telling us that they're still changing fast, which means it's hard to have a stable, up-to-date privacy policy you feel confident is fully compliant."