Startups & Data Privacy

Engine

Key Takeaways

- Startups need a uniform framework that preempts state laws to streamline compliance and keep costs low.
- A federal privacy framework must limit bad faith litigation, and should be consistently and exclusively enforced by expert agencies.
- Any privacy law must contain clear, bright line rules.
- A federal privacy law must account for the limited time and resources startups can spend on compliance.
- A federal privacy law must account for the dozens of services startups use to build their companies.

Preempting state laws

Most of the problems and costs encountered by startups are borne of the patchwork of state privacy laws—the variation and the uncertainty of future changes. Preempting state laws and creating a uniform federal framework will remove variation, create certainty, and alleviate **tens of thousands** in duplicative, unnecessary costs. Federal privacy rules without preemption would instead merely create more variation by adding another layer to the existing patchwork.

Clear, bright line rules

Obligations in any federal privacy framework must create clarity to ensure startups know what they must do to comply. Provisions that e.g., require companies to evaluate on a case by case basis or infer the age of their users are the opposite of bright line rules, and would create additional uncertainty and burdens for startups. In addition, such provisions, which may require companies to collect additional data for analysis and inference, abridge most startups' aversion to collecting and storing data they do not need because of the associated storage costs and heightened risk of breach.

Minimizing compliance costs

A federal law must also be careful not to impose unbearable obligations on startups with limited resources. Most startups do not initially raise outside funding, instead rely on personal savings or bootstrapping—using revenue generated by the business. Even the average two year old startup that has started to attract outside investment is working with around **$55,000 per month**. Looking at the compliance costs startups are facing in the current privacy landscape, it's easy to see how the state privacy patchwork literally takes months off of the life of a startup.

Preventing meritless lawsuits

Creating a broad private right of action in a federal privacy law would allow individuals to sue companies for alleged violations of the law. A broad private right of action would lead to uneven enforcement and additionally enable bad actors to exploit the high cost of privacy litigation to extract settlements from startups using meritless suits. Instead, a federal privacy law must be consistently and exclusively enforced by expert agencies.

Recognizing the tools startups use to grow

Startups utilize dozens of services to find, engage, and communicate with their current and potential customers. Some startups also sell advertising space on their sites to generate revenue, enabling startups to offer their services to their users for free. If policy frameworks draw stark divides between first and third parties, startups—and other new services—that are just launching and growing a user base will be inherently at a disadvantage. In addition to obligations for startups directly under data privacy laws, the key services they rely upon to reach customers and generate revenue are also impacted by those laws as well, which means startups could see increased costs and decreased quality of the tools they need. In formulating a federal privacy framework, policymakers must keep the impacts for startups in mind—including the interconnectedness of the Internet ecosystem.