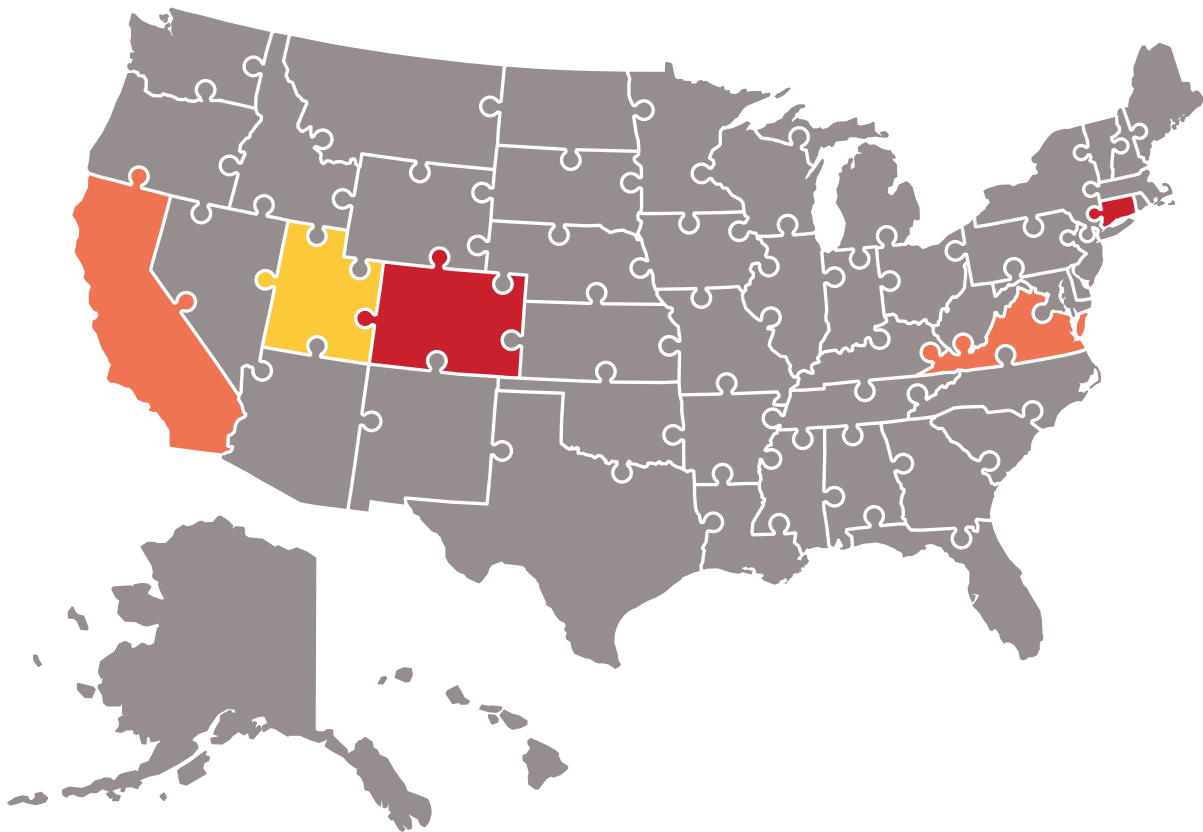




Privacy Patchwork Problem:

Costs, Burdens, and Barriers Encountered by Startups



March 2023

ABOUT ENGINE

Engine was created in 2011 by a collection of startup CEOs, early-stage venture investors, and technology policy experts who believe that innovation and entrepreneurship are driven by small startups, competing in open, competitive markets where they can challenge dominant incumbents. We believe that entrepreneurship and innovation have stood at the core of what helps build great societies and economies, and such entrepreneurship and invention has historically been driven by small startups. Working with our ever-growing network of entrepreneurs, startups, venture capitalists, technologists, and technology policy experts across the United States, Engine ensures that the voice of the startup community is heard by policymakers at all levels of government. When startups speak, policymakers listen.

Engine is grateful for the research assistance and contributions of Annie Eng and the University of Michigan Ford School of Public Policy Program in Practical Policy Engagement to this report.





Engine

CONTENTS

Executive Summary	4
Introduction	5
Methodology.....	6
Legislative Landscape	6
The privacy patchwork	6
Varying definitions	6
Consumer rights.....	7
Opt-in or opt-out?.....	7
Impact assessment	7
Scope and enforcement	7
Findings	9
Compliance costs	10
Legal, audit, and advisory costs.....	10
Technology costs	11
Business and operations costs	11
Opportunity costs	12
Startups and a federal privacy framework	13
Startups need clear, bright-line rules	13
Startups need preemption of state laws	13
Startups are put at risk by private lawsuits	14
A federal privacy law must recognize the tools startups use to reach customers	14
A federal privacy law must account for the resources startups have on hand.....	15

Startups need a federal privacy framework that works for them

Startups need a federal privacy framework that creates uniformity, promotes clarity, limits bad-faith litigation, accounts for the resources of startups, and recognizes the interconnectedness of the startup ecosystem.



Startups care about the privacy of their users and invest heavily in data privacy and security.

\$100,000 – \$300,000+

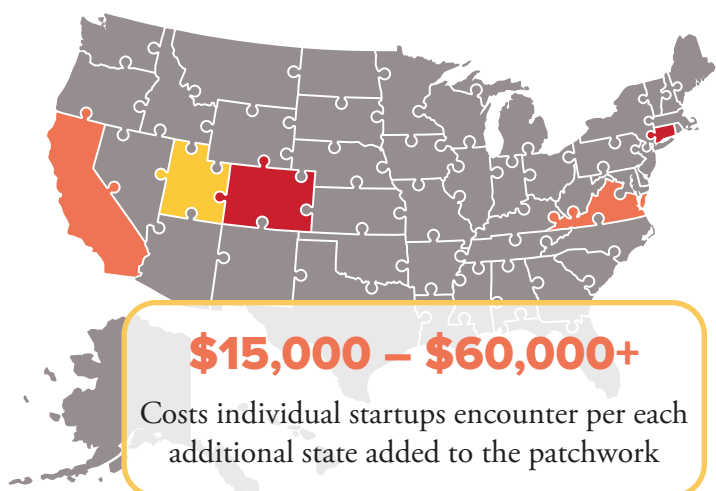
Amount individual startups invest in their data privacy infrastructure and compliance with current or soon effective privacy laws

"We care a great deal about privacy and we want to be compliant, but it can be very expensive and complex."

Ben Brooks, Founder & CEO, PILOT, New York, NY

"Working with children, our priority is protecting their data."

Katherine Grill, Co-Founder & CEO, Neolth, Walnut Creek, CA



A patchwork of privacy laws creates confusion and duplicative costs for startups.

Five states have passed and enacted comprehensive data privacy legislation and already this year more than a dozen states have introduced at least three dozen privacy laws. The rapidly shifting landscape of state privacy laws makes compliance difficult for startups and leads them to spend considerable time and resources navigating these disparate, complex frameworks.

"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."

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

"In 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...trying to figure out how to build a business in an environment with differing rules about the same issue becomes hard and expensive."

Aditya Vishwanath, Co-Founder & CEO, Inspirit VR, Palo Alto, CA

\$55,000

Average monthly resources of a venture-backed, seed-stage startup

"As a high-growth and early-stage startup trying to grow fast, you're at a major competitive disadvantage...I would have to raise an entire second Series A to navigate many of these frameworks."

Sam Caucci, Founder & CEO, 1Huddle, Newark, NJ

Startups need Congress to act.

"It would be helpful to have a nationwide standard when it comes to data privacy policy, especially since we're looking to expand into new states."

Andrew Prystai, CEO & Co-Founder, EventVesta, Omaha, NE

"One uniform, consistently enforced federal policy framework could help make running RAVN easier."

Tani Chambers, Co-Founder & CEO, RAVN, New York, NY

INTRODUCTION

Data privacy has been top of mind for consumers, policymakers, regulators, companies, and entrepreneurs for the past several years, in the wake of broad privacy rules in the EU, and action in several U.S. states. The U.S., which has long had a sectoral approach to privacy, remains without a comprehensive privacy framework, and many states have reacted by proposing, passing, and implementing their own varying—and potentially conflicting—comprehensive privacy laws. The Internet does not stop at state borders, and as more and more states pass unique privacy laws, the volume of rules for startups to keep up with is growing, threatening to bury resource-strapped startups under duplicative compliance costs, limit their scalability, and burden their chances of success. This report seeks to enumerate those impacts of the growing patchwork of privacy laws upon the startup ecosystem.

Startups should be a key consideration as policymakers advance privacy rules. They have to navigate the same legal and regulatory framework without the resources of their larger counterparts—but much of the conversation focuses on the practices of large Internet companies. To adequately include startups’ experiences in data privacy debates, policymakers need a window into startups’ responses to privacy laws, the resources they devote toward compliance, and an understanding of costs—direct and indirect—imposed on startups. This report can provide these insights for policymakers in statehouses and Congress alike.

The findings of this report could not be more clear: the U.S. needs a consistently-enforced, uniform federal privacy framework to create privacy protections for all Americans and certainty for the startups that serve them. Startups vehemently endeavor to comply with the rules that apply to them, but an inconsistent state-by-state patchwork is unworkable and unnecessarily saps limited resources that startups need for activities essential to their growth and survival. Congress has faced calls for many years from many corners—from privacy advocates to the startup community—to create a federal privacy law. Last Congress saw momentum toward a federal privacy law, and that work looks poised to continue this Congress. The findings of this report, coupled with an explosion of privacy law-related activity in statehouses across the country should add to that momentum.

METHODOLOGY

To unpack the impacts of disparate state privacy laws, this report has three main components: an overview of the current state privacy patchwork, a breakdown of the compliance costs associated with those laws, and startups discussing the impact of the data privacy policy landscape in their own words.

To understand how startups are approaching compliance with the varying, growing, and likely to keep growing number of state privacy laws, we spoke with over a dozen startups, entrepreneur support organization leaders, outside legal counsel to startups, and data privacy and security consultants that work with startups. The conversations took place between October 2022 and February 2023. The startups quoted throughout the report are not necessarily the same startups that contributed cost figures to the findings section of this report. The startups we spoke with were less than two-years-old to over 14, with some having raised no outside investment and others having raised millions of dollars in venture capital. The startup counsel we spoke with worked with both early-stage and growth stage startups, from both top law firms and bespoke firms tailored to startups, located in top startup hubs and smaller startup ecosystems.

To help quantify the costs and other impacts of the state privacy patchwork, this report breaks down compliance costs into several component parts: legal, audit, and advisory costs; technology costs; business and operations costs; and opportunity costs. The activities and expenses associated with each of those categories are discussed in further detail where they appear. Startups offered both actual costs—those they had already incurred, contracted for, or committed to—and expected costs—those they had budgeted, sought estimates for, or otherwise knew to expect based on previous experiences. Segmenting costs in this way offers insight into the different types of impacts on startups, and delivers a concrete, startup-level view of compliance with disparate state privacy laws—offering a tangible addition to macro-level estimates of costs of the state privacy patchwork problem.

LEGISLATIVE LANDSCAPE

At the federal level, there are several sectoral privacy frameworks that cover, e.g., health, financial, or education data. The Children’s Online Privacy Protection Act imposes specific requirements for Internet services directed toward those under age 13. There is no federal data privacy statute that governs data and personal information in a comprehensive way. In this absence, several states have proposed and passed legislation to provide this governance for their citizens. While the goals of each state law are similar, and purport to do similar things, they are not the same. This section briefly explores this landscape.

The privacy patchwork

Five states—California,¹ Virginia,² Colorado,³ Connecticut,⁴ and Utah⁵ —have passed and enacted comprehensive data privacy legislation. Within the first few weeks of the 2023 state legislative calendar, more than a dozen states have introduced at least three dozen privacy laws, which have seen varying levels of movement toward passage. Each of the enacted laws are in effect or will take effect later this year, and startups are parsing and preparing for what that means for them. These activities and their costs are explored in the findings section.

Varying definitions

Even if they are oftentimes inspired by one another, the state laws are not the same, which is why the privacy landscape is often referred to as a “patchwork.” This creates complexity and makes parsing the obligations for startups difficult. For example, the enacted state laws define sensitive personal information differently—from which certain consumer rights and obligations arise. The states consider many of the same types of information sensitive—e.g., race, ethnicity,

mental or physical health or diagnoses, sexual orientation, religious beliefs, citizenship status, genetic or biometric information—but have notable differences. Geolocation data is considered sensitive in most states but not Colorado. But that data becomes sensitive if used to infer other sensitive information like religion or health status through e.g., visits to a church or healthcare provider. And California considers additional information to be sensitive, like contents of email, financial data, or certain government ID information.

Consumer rights

The laws grant many of the same consumer rights, but not all of them. Rights to access, delete, port, and opt-out of sale are included in each state (but the application of those rights might vary). Most states also have rights to correct information but not Utah. The timeframe companies have to respond to requests is a relatively consistent 45 days across most states (and include the possibility of extensions), but some states require acknowledging and responding to certain requests on much shorter timelines. Facilitating these consumer rights is likely to take time and resources for startups, given they may not presently have the infrastructure in place to handle such requests or ensure that bad actors do not exploit the rights to gain access to customer information. Compounding these potential burdens, what constitutes a “sale” varies among the states, and California introduces the right to opt-out of sharing—which is a new concept.

Opt-in or opt-out?

The laws have different opt-in thresholds, some of which hinge on sensitive information definitions (that again, also vary). For example, in Virginia, Colorado, and Connecticut, consumer opt-in is required to process sensitive information. In Utah, consumers can opt-out, and California consumers can limit use of such information.

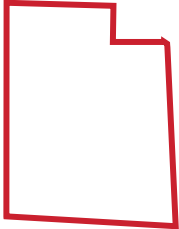
For startups, other noteworthy consumer opt-out rights found in the state laws include rights to opt-out of targeted advertising and rights to opt-out profiling or automated decisionmaking. Many startups leverage targeted advertising to reach new users and while others may generate revenue by selling ad space. Likewise, many startups have automated processes integrated into their products or, for some, it might even be their core service. Several states’ laws contemplate such an opt-out right, while Utah’s does not. And still others, like California, leave similar key questions to regulators.

Impact assessments

Most of the state laws require companies to conduct data impact assessments. At present, several startups are likely to be unfamiliar with the concept, which comes from the EU privacy rules, while larger startups and tech companies are more likely to be familiar. For smaller startups, preparing and submitting multiple, different assessments to the various states could create new costs.

Scope and enforcement

As outlined below, who the laws apply to vary by state, but several have adopted similar thresholds. For startups, the many disparities found in the laws have a lot of practical impacts and lead to increased compliance costs, confusion and uncertainty. Thankfully for startups, most of these laws allow companies to cure within a certain time period unintentional violations they are notified about. And most laws are enforced by the government or otherwise limit private rights of action.

State	Effective Date	Applicability thresholds	Right to cure violations, Cure period	Private Right of Action
California 	CCPA: Jan 1 2020 CPRA: Jan 1, 2023	Does business in CA and has \$25 million+ in revenue or “buys, sells, or shares” personal information of 100,000+, or derives 50%+ of revenue from selling or sharing personal information, or certifies compliance to regulator regardless of above	Yes, at enforcers’ discretion or 30 days for data breaches	Yes, limited
Virginia 	Jan 1, 2023	Conducts business in VA or produces products or services targeted to VA residents and “controls or processes” personal data of 100,000+, or 25,000+ and derives 50%+ of revenue from “sale of personal data”	Yes, 30 days	No
Colorado 	July 1, 2023	Conducts business in CO or delivers products or services intentionally targeted to CO residents and “controls or processes” personal data of 100,000+, or 25,000+ and derives revenue or receives discounted goods or services from “sale of personal data”	Expires Jan 1, 2025, 60 days	No
Connecticut 	July 1, 2023	Conducts business in CT or produces products or services targeted to CT residents and “controls or processes” personal data of 100,000+, or 25,000+ and derives 25%+ of revenue from “sale of personal data”	Yes, 30 days	No
Utah 	Dec 31, 2023	Conducts business in UT or produces products or services targeted to UT residents, has 25 million+ in revenue and “controls or processes” personal data of 100,000+, or 25,000+ and derives 50%+ of revenue from “sale of personal data”	Expires Dec 31, 2024, 60 days	No

FINDINGS

Startups we spoke with view data privacy and security as a business prerogative, and invest heavily—especially as a percentage of the few resources they have on hand—in doing right by their users, customers and clients. The careful thought given to data privacy by startup leaders is heartening but also underscores deep trade-offs they face when navigating the privacy landscape. The findings of this report reveal that complying with a growing patchwork of unique state privacy laws is an expensive, difficult task that must be solved with one uniform, consistently enforced federal privacy framework to support startup growth and ensure data privacy protections nationwide.

All of the startups we spoke with viewed securing user data and respecting the privacy of their users as priorities, but, despite taking significant steps to those ends, they often expressed confusion and uncertainty about their obligations under the law. Startups in industries falling within existing sectoral federal privacy regulations, like health, education, or finance, knew what they must do to be compliant with those rules, but they were not as confident in their ability to keep up with new and evolving state privacy rules.

“Working with children, our priority is protecting their data [...] we worked with our counsel at Latham and Watkins to create our terms of service and work with our school customers on any state-specific addendums. Having various laws makes this process a little harder, so it would definitely be nice if there was just one standardized privacy law.”⁶

- Katherine Grill, Co-Founder & CEO, Neolth, Walnut Creek, California

Neolth leverages technology to equip students and schools with mental health resources.

All startups we spoke with lamented the evolving patchwork of state privacy laws as confusing, hard to keep up with, costly, and burdensome. In some cases, startups avoided intentionally seeking to serve users or businesses in states with unique data privacy laws because they could not afford to evaluate if their current data privacy and security practices were sufficient for compliance. The reflex is similar to that of many startups following the European Union’s General Data Protection Regulation—who used geoblocking technologies to avoid EU users.⁷ Similar technologies to block traffic from various intra-country jurisdictions like states do not really exist. Instead, startups avoid advertising to users or forgo otherwise lucrative business contracts in certain states in the hopes of staying below the applicability thresholds of those states’ data privacy laws.

“...a significant challenge for us has been data privacy. It would be helpful to have a nationwide standard when it comes to data privacy policy, especially since we’re looking to expand into new states. Part of the reason that we have not expanded into certain states like California is because of the resources required to handle California Consumer Privacy Act (CCPA) compliance, which is something that we have to think about every time we look at entering a state that has its own, unique privacy compliance requirements.”⁸

- Andrew Prystai, CEO & Co-Founder, Event Vesta, Omaha, Nebraska

Event Vesta is an event discovery and promotion platform that improves connectivity between event organizers and attendees.

Similarly, attorneys and advisors find the quickly-changing legal landscape around privacy tough to keep up with. Several described the amount of time they had to spend researching and keeping up to date on the latest developments in state data privacy regulations, noting that it went far beyond anything they could reasonably bill a client for. As one attorney for early-stage startups added, “if it takes us that long with all these changes, I can’t understand how [policymakers] expect a startup founder to know what to do.”

Compliance costs

Startups took disparate approaches to compliance with varying data privacy and security regimes they are or might be subject to, but all shared common themes. Many compliance-associated activities could be done once because they are found in several laws—like reconfiguring data storage to create the ability to delete user data—while other activities needed to be done for each new law—like audits, impact assessments or evaluating and updating privacy policies. This report reflects these realities by reporting both one-time costs, and marginal, per-state costs of privacy law compliance faced by most startups. (A minority of startups—usually those later-stage or in regulated industries—reported spending more, sometimes much more, than these figures.)

\$100,000 – \$300,000+
Compliance costs

\$15,000 – \$60,000+
Additional per-state costs

To help break down the cost of compliance and lay out the types of compliance activities startups undertake, we separate them into component parts for discussion.

Legal, audit, and advisory costs

For a startup, legal, audit, and advisory costs associated with privacy law compliance primarily includes the cost to hire legal talent, retain outside counsel, engage privacy consultants, or commission auditors. Startups secure these services to understand obligations under varying data privacy laws; update their privacy policies and internal controls; verify legal compliance; or attain certifications like SOC 2. Outside of the associated pecuniary costs, these activities are time-consuming and potentially distracting for startup leadership teams, with startups reporting it taking from as little as two months to as long as two years to complete such activities.

Perhaps the most basic and outward-facing compliance task for a startup is creating and updating their privacy policy. To create or update a privacy policy, startup attorneys said they typically charge around \$1,500 for very basic policies to around \$6,000 for more tailored policies. Attorneys in smaller markets charged around \$400 an hour for additional work, while attorneys in startup hubs or at larger firms billed at \$1,000 or more an hour. These figures were confirmed by startups with legal bills for privacy policies and related activities ranging up to \$15,000.

In parallel to legal counsel, many startups sought advisory services—perhaps also from an attorney, but usually from a privacy consultant or auditor—to evaluate their business, understand their obligations under the law, and perform risk assessments. Most startups reported these costs ranging between \$20,000 and \$50,000. In response to the recommendations of an advisor, startups usually found they may need to implement legal, technical, or business-model changes, adding additional expense on top of those costs. And while companies do not start from scratch with each new state or jurisdiction where the company encounters a new privacy law, it is still costly to (re)evaluate obligations and implement changes. For new, additional states, some startups reported identical advisory costs, while others said slightly less on a marginal basis, estimating it will cost them \$10,000 per each additional state just to start reviewing and modifying policies for compliance. Finally, rather than a fee-for-service arrangement associated with a particular set of compliance activities, some startups had privacy consultants on retainer to be responsive to their needs—with those startups reporting this cost them \$6,000 to \$10,000 per month (up to \$120,000 per year).

Of course, these ranges can vary significantly based on the startup and their industry subsector as well. One startup in a regulated industry estimated they had spent \$5 million on legal and advisory services over the life of the company through developing and updating privacy policies for various state and federal regulatory regimes, performing quality controls and risk assessments, and regularly engaging with auditors and regulators.

Technology costs

As part of complying with new privacy laws, startups often must make changes to their existing systems, develop new technology, or acquire and integrate third-party software products. Generally, decisions to re-design, build, or integrate new technology are products of consultations or audits discussed above, meaning startups may have already spent tens of thousands of dollars before getting to the brass tacks of putting those recommendations into practice.

Many startups reported using third-party software solutions to help automate and manage compliance. These startups reported costs just for the software to be \$8,000 to \$20,000 per year, which must be integrated into their processes and managed by their staff.

And many startups dispatched their own engineers to redevelop systems where needed. Engineers are some of the most important hires startups make, and some founders report paying themselves minimum wage so that they effectively stretch their resources and pay competitive salaries to their engineers, which tend to range from about \$75,000 all the way up to more than \$300,000 annually. The average software engineer pay in smaller ecosystems is around \$40 per hour, \$75 per hour in top ecosystems, and could reach up to \$150 an hour for more senior engineering talent.⁹ One startup emphasized using at least four engineers to redevelop a system, while another estimated it took 1,000 engineering hours to complete an overhaul for compliance.

Software engineers are critical to developing, building, and growing startups, and how they spend their time is intimately tied with a startups' success and ability to make and market new products. Given the resource constraints of many startups, they may not have six months of engineering time to feasibly steer away from activities central to their existence. And insofar as additional state laws added to the privacy patchwork require engineers' time, they will have a direct impact on startups' core activities.

Business and operations costs

Complying with various state privacy laws implicates business and operational costs, for example around hiring, training, relationships with vendors, business practices, customer acquisition, and sales cycles.

Many startups described needing to reevaluate existing relationships and update contracts with vendors as a result of changes to privacy rules. Often this didn't carry a significant separate monetary cost unless legal counsel needed to be consulted for review. Instead the main cost startups described involved time to evaluate the contracts and implement technical or business changes to be in line with the updated terms.

Most startups emphasized that it takes time and costs money to train their employees with regard to data privacy and security. Some startups approached hiring differently as a result of the evolving legal landscape around data privacy, consciously seeking more senior software engineers and staff with deeper knowledge of privacy rules—and therefore paying higher salaries than otherwise. And these startups noted the pool of talent that is up-to-date on privacy rules is relatively small. With the privacy landscape in flux, it is likely to shrink smaller still.

Startups need to reach potential customers and evaluate their services, and many highlighted impacts or feared impacts of data privacy legislation on those critical business needs. Many startups said they use digital advertising and other marketing tools to find new customers and recognized that privacy laws may impact the effectiveness of those channels in the future. And startups use analytics to evaluate how well their service is performing and to pinpoint areas in need of improvement. Startups reported seeing privacy measures interfering with those basic business insights despite their belief that these insights don't come at the cost of user privacy because they needn't extend to the level of an identifiable individual user.

Other business costs included the additional barriers at the point of sale for startups entering into contracts with clients. This was true for all startups working with enterprise clients, but especially acute for those selling to large entities. For example, an enterprise software startup looking to contract with a Fortune 500 company must work with that company's legal department and certify their compliance with relevant privacy laws. Startups lamented the amount of time these sorts of reviews took—from two to six months, sometimes longer. This strikes at the very vitality of startups since many measure their runway (the amount of time until they run out of capital) in months, not years. In addition to the time that these processes take, they can be very costly, amounting to 10 percent to 15 percent of the value of the contract. Another startup in a more regulated industry emphasized that compliance costs amounted to 20 percent of their contract value.

These costs have impacts on startup competitiveness. Startups spend much more on compliance as a percentage of revenue than their larger competitors,¹⁰ putting them at a resource disadvantage. These tens of thousands missed on a per-contract basis could go toward hiring, R&D, customer acquisition, and other activities to scale their startup. As another consequence of the many varying privacy laws, as large enterprises look to reduce their risk profile, they are looking to contract with fewer vendors, benefiting already large players while startups lose out.

Opportunity costs

All startups and advisors we spoke with unanimously agreed that the opportunity cost of expending effort and resources to meet compliance for multiple states was tremendous, underscoring that there were more productive, value-creating tasks that could be focused on with the time, capital, and other resources spent on compliance without sacrificing meaningful privacy protections for users. Several startups highlighted hiring more full-time employees, conducting research and development, and growing their sales teams to scale the business. And one startup attorney said there were “a hundred other things” that startups would rather do than have to pay their lawyer. Critically, many startups pointed out that these costs could be mitigated if there were one federal privacy framework instead of a shifting landscape to keep up with.

Several founders additionally highlighted major opportunity costs related to fundraising. Founders spend a significant amount of time fundraising, which is needed fuel to support their startups. Startups leaders said time spent on compliance could take away from that, but more pressing is that investors want to see their capital put toward growth rather than legal or other duplicative compliance costs.

STARTUPS AND A FEDERAL PRIVACY FRAMEWORK

Startups need a uniform, consistently-enforced federal privacy framework. Every startup and advisor we spoke with as a part of this project highlighted a federal framework as a solution to the problems they and their startup clients face. In 2022, Congress came closer than ever to passing a comprehensive federal privacy law, but it got hung up on many familiar sticking points. The findings of this report lend insight to startup perspectives on these pressing issues in today's privacy debates, which are discussed in this section.

Startups need 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.

“

“ChessUp came from the idea of making the learning experience of chess much more accessible and immediate, allowing kids to play a game right out of the gate...with their family and not have to worry about the skill differences.”¹¹ ... “Our experience is built around making chess easier and more approachable to learn. We want the experience to connect to our product to be brief and convenient as well. As a company, we don't want to be in the position of having to collect and retain information about our users' ages or implement age restrictions. That would create a burden for us and be privacy-invasive for our users.”¹²

- Jeff Wigh, Founder & CEO, Bryght Labs, Overland Park, Kansas

Bryght Labs is a connected gaming startup dedicated to making STEM-based games more accessible and the maker of ChessUp.

”

Startups need preemption of 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 what startups felt were duplicative, unnecessary costs. If a federal framework does not preempt state privacy laws, then none of these benefits will accrue. It would instead merely create more variation by adding another layer to the existing patchwork, and not create any additional certainty as states could still implement unique or even conflicting privacy rules.

“

“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. It's pretty frustrating.”¹³

- Camila Lopez, Co-Founder, People Clerk, Miami, Florida

People Clerk is a legal technology platform that provides users with guidance through small claims court procedures.

”

Startups are put at risk by private lawsuits

Startups encounter abusive rent-seeking litigation in many areas of the law, especially those with high defense costs and high potential damages.¹⁴ Creating a private right of action in a federal privacy law would empower individuals to sue companies for alleged violations of the law. A 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.¹⁵ Instead, a federal privacy law must be consistently and exclusively enforced by expert agencies.

Startups have few resources and have many reasons to avoid long litigations—and bad actors know it and use it to their advantage. Startups can't afford the potentially millions of dollars in legal fees to litigate a case through and are better off paying the plaintiff to go away even if the startup knows they would otherwise win. And even if they did see the case through to defeat the plaintiff's claims—each party pays their own legal costs, making protracted litigation a lose-lose prospect. What's more, protracted litigation is distracting for startup leadership, and it is nearly impossible for startups involved in active litigation to pass diligence needed to raise capital or experience a successful exit.¹⁶

A federal privacy law must recognize the tools startups use to reach customers

Startups utilize dozens of services to find, engage, and communicate with their current and potential customers—from digital advertising infrastructure to social media to email to chat widgets and beyond. 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. And startups use tools to evaluate the effectiveness of those ads and the performance of their services. Recent research shows the volume of tools used for these functions and demonstrates their importance to startups.¹⁷

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 (usually under the higher-threshold, greater obligations parts of the law). As a result, startups experience 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 impacts felt through the tools they use.

“*[Some]thing that is important for us to grow our company is the availability of user analytics, which helps us know how our product is performing and how to better serve our users. Measures designed to promote user privacy can pose challenges for basic business insights, like usage and retention. ... a more nuanced approach to data collection ... would allow us to better serve our customers while respecting their privacy preferences.*”¹⁸

- Mandy Poston, Founder & CEO, Availyst, Philadelphia, Pennsylvania

Availyst is a delivery platform for local grocery, takeout, convenience, and spirit options.

A federal privacy law must account for the resources startups have on hand

Startups have 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 in resources, money meant to last for 18 months to two years.¹⁹ 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.

“

“We care a great deal about privacy and we want to be compliant, but it can be very expensive and complex. ... Various states also have their own privacy laws. Harmonizing those laws nationally would make it much easier for business owners like me and those we work with. ... There's also very little guidance on how to set things up initially and how to have good security and privacy without the costly certifications. These are all issues that have hindered our business. Privacy law is built around sophisticated multinational large businesses, so as a startup we have to learn how to work within a system that isn't made for us.”²⁰

- Ben Brooks, Founder & CEO, PILOT, New York, New York

PILOT provides tech-driven virtual group coaching programs to companies that are easy to implement, affordable, and get good results.

”

A federal law must also be careful not to impose obligations upon startups that they cannot afford to implement. Compliance thresholds—especially for the most burdensome or costly obligations—must be set sufficiently high to avoid scoping-in startups.

“

“...one uniform, consistently enforced federal policy framework could help make running RAVN easier, especially as a fintech startup. Compliance can be very costly and is one of the reasons we've delayed our technical product. However, if an overarching framework is developed, it would need to consider small businesses and startups and preferably segment the requirements accordingly. Creating a framework built around regulating large companies and big tech could be harmful to smaller companies and startups like RAVN.”²¹

- Tani Chambers, Founder & CEO, RAVN, New York, New York

Ravn is a wealth-building platform tailored to Black women.

”

ENDNOTES

- 1 Cal. Civ. Code § 1798 (2018) https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5; see *related FINAL REGULATIONS TEXT* California Privacy Protection Agency (Feb. 2, 2023), https://cpa.ca.gov/meetings/materials/20230203_item4_text.pdf.
- 2 Va. Code § 59.1-575 (2021) <https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/>.
- 3 Colo. Rev. Stat. § 6-1-1301 (2021) https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf; see *related VERSION 3 OF PROPOSED DRAFT RULES*, Attorney General of Colorado (Jan. 27, 2023), https://coag.gov/app/uploads/2023/01/CPA_Version-3-Proposed-Draft-Regulations-1.27.2023.pdf.
- 4 Conn. Pub. Acts 22-15 (2022) <https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF>.
- 5 Utah Code § 13-61 (2022) <https://le.utah.gov/~2022/bills/static/SB0227.html>.
- 6 #StartupsEverywhere Profile Katherine Grill, Co-Founder & CEO, Neolth, Engine (Mar. 18, 2022), <https://www.engine.is/news/startupseverywhere-walnutcreek-ca-neolth>.
- 7 See, e.g., GDPR Shield, <https://gdpr-shield.io/>; see generally *Comments of Engine Advocacy in response to Commercial Surveillance ANPR*, R111004, §II Engine (Nov. 21, 2022), <https://engine.is/s/Engine-FTC-Privacy-ANPRM-Comments.pdf>.
- 8 #StartupsEverywhere Profile: Andrew Prystai, CEO & Co-Founder, Event Vesta, Engine (Oct. 29, 2021), <https://www.engine.is/news/startupseverywhere-omaha-ne-eventvesta>.
- 9 Per our conversations with startups for this research. These figures generally adhere to averages reported in robust data sources, e.g., *Ecosystems*, Startup Genome, <https://startupgenome.com/ecosystems> (reporting average software engineer salaries for various ecosystems); and *the State of the Startup Ecosystem*, 15-16 Engine (Apr. 2021), <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/60819983b7f8be1a2a99972d/1619106194054/The+State+of+the+Startup+Ecosystem.pdf> (reporting average annual software engineer salaries for four select ecosystems of various sizes).
- 10 See, e.g., *2022 Global Privacy Benchmarks Report*, TrustArc (2022), <https://trustarc.com/pdf20/2022-global-privacy-benchmarks-report.pdf>.
- 11 #StartupsEverywhere Profile: Jeff Wigh, Founder & CEO, Bryght Labs, Engine (Feb. 4, 2022), <https://www.engine.is/news/startupseverywhere-overlandpark-ks-bryghtlabs>.
- 12 *Comments of Engine Advocacy*, *supra* note 7, at §V.
- 13 #StartupsEverywhere Profile: Camila Lopez, Co-Founder, People Clerk, Engine (Nov. 4, 2022), <https://www.engine.is/news/startupseverywhere-miami-fl-peopleclerk>.
- 14 See, e.g., *Startups, Content Moderation, & Section 230*, Engine (Dec. 2021), <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/61b26e51cdb21375a31d312f/1639083602320/Startups%2C+Content+Moderation%2C+and+Section+230+2021.pdf>; *Startups & the U.S. Patent System: Prioritizing Quality and Balance to Promote Innovation*, 9 Engine (July 2021), <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/60f8579bae6a2d324b7440a2/1626888093336/Engine+Patent+Quality+Booklet+2021+7.21.pdf>.
- 15 *The Coming “Privacy Troll” Problem*, Engine (May 31, 2019), <https://engineadvocacyfoundation.medium.com/the-coming-privacy-troll-problem-4363695220d6>.
- 16 See *related Robin Feldman, Patent Demands & Startup Companies: The View from the Venture Capital Community*, UC Hastings Research Paper (Oct. 28, 2013), <http://dx.doi.org/10.2139/ssrn.2346338>. (“100% of venture capitalists indicated that if a company had an existing patent demand against it, it could potentially be a major deterrent in deciding whether to invest.” Similar deterrents to investment or M&A are present as the result of any pending litigation.); See generally *Exits, Investment and the Startup Experience: the role of acquisitions in the startup ecosystem*, 8-9 Engine (Oct. 2022), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/6356f5ccf33a6d5962bc7fd8/1666643406527/Exits_Investment_Startup_Experience_role_of_acquisitions_Report_Engine_Startup_Genome.pdf.
- 17 *Tools to Compete: Lower Costs, More Resources, and the Symbiosis of the Tech Ecosystem*, Engine and CCIA Research Center (Jan 2023). https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/63d2b8d-5bec96f502264fd1f/1674754266044/FINAL_CCIA-Engine_Tools-To-Compete.pdf.
- 18 #StartupsEverywhere Profile: Mandy Poston, Founder & CEO, Availyst, Engine (June 24, 2022), <https://www.engine.is/news/startupseverywhere-philadelphia-pa-availyst>.
- 19 See, e.g., *State of the Startup Ecosystem*, *supra* note 16, at 19-20.
- 20 #StartupsEverywhere Profile: Ben Brooks, Founder & CEO, PILOT, Engine (July 29, 2022), <https://www.engine.is/news/startupseverywhere-newyork-ny-pilot>.
- 21 #StartupsEverywhere Profile: Tani Chambers, Founder & CEO, RAVN, Engine (Jan. 20, 2023), <https://www.engine.is/news/startupseverywhere-newyork-ny-ravn>.