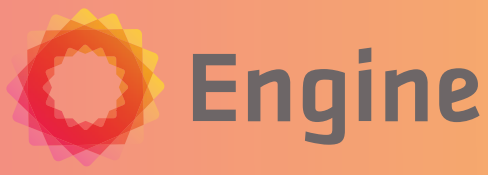

More than just a number:

How determining user age impacts startups

February 2024

POLICYMAKERS MUST GRAPPLE WITH THE INHERENT TRADEOFFS OF AGE VERIFICATION.

Policymakers are rightfully concerned about the safety and well being of young Internet users, but many of the policies they're advancing would bring significant tradeoffs. Even where policies don't outright mandate age verification, they would require Internet companies to proactively identify, estimate, or verify the age of their users, which carries direct and indirect costs that will fall disproportionately on startups.

Age verification is prohibitively expensive.

$2 MILLION +

Cost to build and operationalize in-house age verification system

The costs to build an age-verification system meet or exceed what a startup has spent building their actual product, meaning no startup will create their own age-verification system, and will instead rely on third-party providers.

$100 MILLION +

Amount established age verification providers have spent building their services

$500,000

Cost of age verification

Consider the cost of implementing age verification mandates for an example startup: a gamified coding tutor that helps individuals to learn to code or to enhance their skills. The service also has a forum for individuals to discuss bugs or coding problems they encounter with other users. The startup is based in a midwest state where the average software engineer salary is about $80,000,[i] they employ five people full-time, and have 300,000 users. It will cost them $50,000 to integrate a third-party age verification service, and $1.50 per user verified, making the total cost of age verification $500,000—equivalent to a year's payroll or nearly half of their seed round.

Age verification will diminish startups' limited resources and competitiveness.

The average seed round was $1.2 Million, an amount that falls outside of top ecosystems and for underrepresented founders.[ii] The costs of age verification eats into these resources that are needed to fund key startup activities, hiring, marketing, product development, and more. In addition to the monetary expenses of age verification, it creates practical costs for startups: adding friction to user sign-up, reducing user conversion, increasing cybersecurity risks and diminishing competitiveness with better known services.

$1.2 MILLION

average seed round

Founders say age verification is unworkable for startups.

*"Age verification requirements would present **significant complexities and costs for startups.** It's not just about the technology. It's about legal liability, user privacy, and the overall user experience. For a small team like ours, managing these complexities is a huge burden and could **jeopardize our entire business.** It's **simply not feasible** for individual app publishers or consumer products to become age verification experts and navigate the minefield of legal and technical challenges that come with it."*

- Nico Aguilar, Cofounder & CEO, Speeko

*"As a startup there's **no way it is economical** to build your own age-verification process. We would look for an off-the shelf solution, or **exit that particular market.**"*

-John Pettus, Founder & CEO, Fiskkit

*"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."* [iii]

- Jeff Wigh, Founder & CEO, Bryght Labs

Engine

For more information, visit: engine.is

INTRODUCTION

Across the country, at both the state and federal levels, policymakers have been advancing proposals in the name of keeping kids safe online. Policymakers often have the largest Internet companies in mind, but their proposals will impact much broader swaths of the Internet. Their ideas could make life harder—and more expensive—for startups that do (or even *might*) interact with young users. While the varying goals of protecting young users from things like harmful content, privacy invasions, and addictive technologies are all laudable, these proposals often carry significant tradeoffs, including on privacy, security, and expression, as well as creating costs and compliance burdens that fall disproportionately on startups.

The laws, proposed regulations, and draft legislation policymakers are considering often—either explicitly or in practice—require startups to determine the ages of the users that access their services. To learn more about the impact of these requirements, we spoke with a dozen stakeholders and subject matter experts, including startup founders, consultants to startups, and age verification and estimation providers. The startups we spoke with all had fewer than eight employees, and the largest startup had around 1.1 million users.

Determining user age can be done to varying degrees of certainty and through a range of methods that each carry their own risks, costs, benefits, and drawbacks. For startups, these unique impacts can eat away at limited budgets, increase cybersecurity risks, and diminish user experience, and it is critical that startups and policymakers alike understand the implications of age verification requirements for them and the businesses they represent.

The direct and indirect costs of determining user age are more than just a number—they will make it harder for startups to compete. While so much of the policy conversations about kids' safety happening at every level of government are driven by concerns about large companies, policymakers need to remember that the rules they write will impact the entire Internet ecosystem, including the startups that want to be good stewards of their users' data and already have to be responsive to their users' needs and concerns.

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.

@EngineOrg **engine.is**

THE CURRENT POLICY DEBATE AROUND YOUNG INTERNET USERS

Key Takeaways:

- Policymakers are rightfully concerned about the safety and well being of young Internet users, but many of the proposals they're advancing would bring significant tradeoffs to online participation and expression for users of all ages as well as the ability for startups to compete.
- There's a wide range of proposed policy changes being considered, ranging from extending existing privacy protections to more Internet companies and users, to requiring platforms to block young users from seeing "harmful content," to banning young users from parts of the Internet altogether.
- At their core, the vast majority of the proposals require Internet companies proactively identifying, estimating, or verifying the age of their users, which carries direct and indirect costs that will fall disproportionately on startups.

Policymakers have a lot of ideas on the table that could make life harder—and more expensive—for startups that do (or even *might*) interact with young users. While the varying goals of protecting young users from things like harmful content, privacy invasions, and addictive technologies are all laudable, these proposals often carry significant tradeoffs, including on privacy, security, and expression, as well as creating costs and compliance burdens that fall disproportionately on startups.

How does the law work for start-ups now?

Many of the proposals would be massive shifts from the way the world currently works for startups. Currently, the landscape around how to deal with young users is relatively straightforward; if you operate a website or service that's directed to users under the age of 13 or you have "actual knowledge" that a user is under the age of 13, you have to comply with rules created by the Federal Trade Commission (FTC) under the Children's Online Privacy Protection Act (COPPA).[1] That law was passed in 1998 to give parents more control over how their children's personal information is collected and used online, especially as it relates to targeted advertising. After the first set of rules was enacted in 2000, the FTC updated the rules in 2013,[2] and the agency is currently in the process of updating the rules again.[3] At a high level, the rules require companies in scope to obtain parental consent before collecting information from young users and give parents the ability to review, delete, or prevent further use of their child's information.

COPPA is the reason you have to check the box that you're 13 years old or older every time you sign up for a general audience website or service that will collect your data online. Checking that box gives the operator of the website or service "actual knowledge" that they're not dealing with a user under the age of 13 and they don't have to worry about COPPA compliance. (And while it's true that a younger user can check the box just as easily as someone older, the bright line created by the actual knowledge standard saves operators from the fraught process of having to figure out individual users' ages, as discussed later.)

So what's the problem?

Policymakers in state legislatures, Congress, and the administration have put forward a number of varying laws and rules that would dramatically upend that relatively straightforward framework in the name of protecting kids online. And while they all ostensibly share the same high-level goal, the proposals tend to tackle different facets of the issue:

"Companies are able to collect too much data about kids." Some critics of the current landscape believe that, despite the protections and requirements created by COPPA, websites and online services are still collecting too much personal information about young users. Some say that the fact that COPPA's protections end at age 13, leaving a large swath of "young users" between the ages of 13 and 17 open to data collection and targeted advertising. Others say the problem is that Internet companies that aren't directed to children and don't have actual knowledge that a user is a child should still know that they're dealing with young users based on the context of what those users are doing online.

"Tech companies are building and marketing products that are addictive to kids." Some critics say the products and services being offered by tech companies are intentionally designed to keep users engaged with the product or service, which disproportionately impacts young, impressionable users. Some of the complaints are about companies' design decisions, like infinite scroll, where more content automatically loads when a user reaches the bottom of a page, while other complaints focus on fundamental

aspects of a product or service, like using an algorithm to make personalized recommendations. Critics argue that companies should have alternative versions of their offerings without these features and functions specifically for young users.

"Young users are seeing harmful content online." For Internet companies of any size that host user-generated content—whether that's traditional social media platforms, message apps, photo and video sharing services, and any website where users can leave comments—content moderation is a critical, inherently fraught, and time consuming and expensive undertaking.[4] It's not practical as a platform scales to, in real time, review every piece of user content to ensure it complies with the company's acceptable use policies, meaning there's no way to guarantee that one user won't share something "harmful" that another user sees. Complicating things further, there's no clear consensus on what's "harmful" to young users. When critics of Internet companies talk about "harmful" content, they cite a wide range of things, including content about eating disorders, sexual health, and sexual orientation. What's harmful for one community of users might be helpful to another, and the platform working with their community of users is going to be best equipped to make that determination.[5]

"Illegal and illicit activity online is harming kids offline." Online activity can undoubtedly contribute to offline harm, and policymakers are rightly focused on ways to reduce illegal content that harms children in the real world, including child sexual abuse material (CSAM) and the sale of illegal drugs. Internet companies already spend significant time and money finding and removing that kind of content.[6] But, as discussed above, content moderation is inherently fraught, and even in areas where illegality of content is clearest, like CSAM, there are still inherent limits to technologies used to detect that kind of content.[7]

How could the policy landscape change?

Depending on the problem policymakers are trying to solve, there's a wide range of proposed changes on the table at the federal and state levels:

Expand existing childrens' data protections to cover more companies and users. Many lawmakers are looking for ways to stretch existing protections for kids online to more users. One proposal—the Children and Teens' Online Privacy Protection Act,[8] which was passed by the Senate in July 2024—would take existing federal protections for childrens' online data and expand them in multiple ways, including revising the age for COPPA protections from under 13 to under 16 and allowing the FTC to effectively create a new knowledge standard for whether companies should know they're dealing with young users. At the state level, Virginia and Connecticut have advanced legislation that would create more requirements and prohibitions around young users' data. Connecticut's law—which the state legislature passed last summer—limits the kinds of data a company can collect from young users and prohibits the sale of kids' data and processing it for targeted advertising.[9] Proposals in Virginia—which did not make it across the finish line before the end of the legislative term—would have extended existing state privacy protections for children to users between the ages of 13 and 17.

Require companies to get young users' parental consent to create accounts. Several states have considered—and some have passed—legislation that would require Internet companies to get parental consent before users under the age of 18 can create accounts. The proposals often lay out mechanisms for obtaining and verifying parental consent with varying levels of specificity, including collecting parents' government issued IDs or creating a central phone line where parents can call and give their consent. One passed law in Arkansas would require Internet companies to use a third-party vendor to verify all of their users' ages and obtain parental consent for minors using the service; that law was recently blocked by a federal court after being challenged by industry group NetChoice on First Amendment grounds.[10] Recently passed laws in Utah require parental consent for users under the age of 18, require companies to allow parents to access their children's accounts, and restrict minors' access to social media between 10:30 p.m. and 6:30 a.m. as a default.[11] NetChoice has also sued to block the Utah laws from going into effect.[12]

Prohibit companies from showing young users "harmful content." Many policymakers are focused on the harm that Internet usage can cause to young people's mental health. One proposal—the Kids Online Safety Act,[13] which passed the Senate along with the the Children and Teens' Online Privacy Protection Act—would, among other things, create a duty for Internet companies to take "reasonable care" to prevent users under 17 from seeing "harmful" content. The bill's definition of harm includes anything that contributes to mental health disorders including anxiety, depression, and eating disorders, online bullying and harassment, and anything that promotes tobacco, gambling, and alcohol. The bill would be enforced by the FTC, creating the opportunity for differing answers to the question "what online content can endanger a teenager's mental health?", depending on what political party controls the agency. Other parts of the bill—including prohibitions on harmful "design features"— may be enforced by states' attorneys general, creating disparate enforcement based on the politics of the state. Civil liberties groups have warned about the impact the bill will have on kids, especially those who don't otherwise have access to resources about things like

eating disorder recovery or LGBTQ+ health.[14] At the state level, several states-including Montana, Tennessee, and Pennsylvania-have considered legislation that would require device manufacturers to block minors' access to harmful and obscene material, including pornography.

Require companies to estimate users' ages and offer a version of their product or service to young users. Often called "age-appropriate design codes" and modeled after requirements that were first created in the United Kingdom, several states have considered legislation that would require Internet companies to estimate their users' age, which then triggers several obligations, including different privacy settings, a different privacy policy that is accessible to children, enforcement of community standards, and restrictions on product design that encourages young users to share their information. California passed the first version of the law in the U.S. in 2022, which has since been blocked in federal court after NetChoice challenged the law on First Amendment grounds.[15] Despite the constitutional issues with the proposals, states like Maryland and Vermont each passed a version earlier this year. Maryland's governor signed it into law, while the Vermont Governor vetoed the legislation citing the ongoing California litigation.[16]

Require companies to proactively monitor for illegal user activity that harms kids offline. Fueled by concerns about children being physically harmed in the offline world, including by CSAM and the sale of illegal drugs, some lawmakers are putting forward proposals that would effectively force companies to scan and remove certain types of user content. At the federal level, the Senate Judiciary Committee has repeatedly advanced proposals that would push companies to scan user content for CSAM (the EARN IT Act) and illegal drugs (the Cooper Davis Act). Technologists and civil liberties advocates have warned that these proposals carry significant privacy and security tradeoffs,[17] in addition to threatening constitutionally protected speech that will get caught in the inherently imperfect filters that tech companies would use to comply with the laws.[18] In 2024, California passed its own CSAM measure which creates legal liability for websites that "knowingly" facilitate child exploitation,[19] which many have warned will push companies to stop or scale back the work they already do to proactively find and report CSAM in an attempt to avoid liability for any CSAM content they might miss.

Ban minors from large swaths of the Internet. Some of the most extreme proposals prohibit young users from social media platforms entirely. Texas considered, but ultimately did not move, a bill during the last legislative session that would have required Internet companies to collect driver's licenses to verify that no one under 18 is using their service.[20] More recently, Florida enacted a law that prohibits social media platforms from allowing users under the age of 14 to create accounts, and requires parental consent for 14 and 15 year old users.[21]

What would proposed policy changes mean for startups?

Any of the proposals discussed above would dramatically change the way startups interact with their users. One major change that many of the proposals include is putting the onus on Internet companies to figure out the age of their users. To figure out which users are "young" (under 13, under 16, or under 18, depending on the proposal), a startup would have to figure out the age of all of its users, which typically requires purchasing and integrating third-party parental consent, age verification, or age estimation software.

But there are other costs to these proposals, especially around the additional data collection necessary to do parental consent, age verification, age estimation, and, for the state-level proposals, geolocation. Any additional data collected by a startup needs to be processed, stored, and shared, if necessary, securely, and a startup collecting, for instance, a dataset of its users' government-issued IDs, has to worry about being an attractive target for a data breach. There's also the cost of asking users for that data, especially as a new and relatively unknown company. A startup that requires users to submit their drivers licenses as part of signing up for a service has to worry about whether users feel comfortable handing that sensitive information over, or whether they'll seek out an alternative offered by a larger, more established company.

Depending on the proposal, startups would face additional significant compliance burdens once they determine users' ages, ranging from proactively monitoring and filtering out "harmful" content before it reaches young users, changing the way a company collects data about young users, changing existing products and services to offer additional versions specifically to young users, or removing young users altogether. All of these would carry significant costs, both in terms of literal costs to operationalize but also costs to growth, user participation and expression, and opportunity costs.

All of these direct and indirect costs will make it harder for startups to compete. While so much of the policy conversations about kids' safety happening at every level of government are driven by concerns about large companies, policymakers need to remember that the rules they write will impact the entire ecosystem, including the startups that want to be good stewards of their users' data and already have to be responsive to their users' needs and concerns.

COSTS AND BUSINESS IMPACTS ON STARTUPS OF DETERMINING USER AGE

Key Takeaways:

- Outside of user self-declaration, no startup will create their own age-verification system, and will instead rely on third-party providers. Building a reliable in-house system would require the same resources as they've invested developing their actual product.
- Third-party verification systems cost thousands of dollars to procure and tens of thousands and several weeks to integrate.
- Constructive knowledge standards are unworkable for startups, and barriers to entry for markets with such legal exposure would be insurmountably high.
- Adding additional friction to user sign-up, like age verification, reduces user conversion and diminishes startup competitiveness.

The several laws, draft legislation, and proposed regulations discussed above require startups to determine the ages of the users that access their services. Determining user age (often called age assurance or age verification by standard setting organizations)[22] can be done to varying degrees of certainty and through a range of methods each of which pose their own risks, costs, benefits, and drawbacks. For startups, these unique impacts can eat away at limited budgets, increase cybersecurity risks, and diminish user experience, and it is critical that startups and policymakers alike understand the implications of age verification requirements for them and the businesses they represent.

How do online services determine user age?

Self-declaration. Declaring age is the most common and most straightforward age assurance method, often done by asking a user to check a box confirming they are above a certain age or enter their birthday (to check if they are above a certain age). For startups this is straightforward, low-cost, and easy to implement, with little negative impact on user conversion. Adding another line on a form or a pop-up to enter a birthday would take an experienced developer (likely making around $75/hr)[23] as little as an hour to implement. This method is also privacy respecting—a startup doesn't need to know who the user is—just that they are above a certain age. Precise birth date data does not need to be maintained, because startups are often checking that a user is above a certain age, like 13, 18, or 21—limiting cyber risks. However, asking a user their age is obviously susceptible to individuals lying about it—as some have admitted to in congressional testimony.[24]

Government ID, credit card, or other credential verification. Asking a user to produce proof of their age—by asking for them to upload an ID or enter a credit card—is more certain, but carries additional risks, costs, and drawbacks for startups and their users. In practical terms, there are implications for equal access among adults that should otherwise be able to use—immigrants, the poor, and others might not have an ID or credit card they could use for verification.[25] There are also privacy risks. By providing an ID, there is no way for a user to remain anonymous, and a user is also likely to incidentally hand over other sensitive information present on many types of ID, like their home address.

Startups, especially early-stage startups, are unlikely to be household names, and these additional verification steps turn away users that don't want to provide their ID or credit card as their first interaction with an unfamiliar service. Adding additional steps to sign-up can cut conversion rates in half—requiring a user to hand over sensitive information would accelerate that decline.[26] Startups need to grow in order to continue receiving investment, and age verification poses a clear headwind.

Moreover, startups don't want to encounter or hold the information in the first place because it makes them a more lucrative hacking target.[27] Often, they can delete it after, but that can take a few days, or over a month under some proposals. Requiring operators to prove to a regulator they know a given user's age—not just maintaining the signal—would require maintaining the information. Suffering a data breach would likely doom an early-stage startup. The per-record cost of a data breach in 2024 was $165.[28] Presuming an early-stage startup has 20,000 users, a breach could cost $3.3 million, more than their entire seed round in most parts of the country.[29] The costs for downtime and reputational impacts would additionally be near impossible to overcome, which is why most shut down following breaches.[30]

Relying on a third-party age verification provider does not solve these fundamental cybersecurity risks—it merely transfers them to the third party. Neither does it absolve the company from being blamed for problems caused by

their provider, as seen by the July Microsoft-Crowdstrike debacle, for example. And it does not change the potential for extremely negative consequences for Internet users whose information is put at risk. These risks aren't hypothetical, either. In June it was reported that cybercriminals could have had access for more than a year to sensitive user identity information from an identity verification provider used by large technology platforms, leaving those users vulnerable to identity theft or other harms.[31]

There are few different 'levels' of age verification using a credential like government ID. In the least intensive, the Internet service is primarily concerned with the date of birth, and whether or not it is beyond a certain cutoff. Others will additionally run the image of the ID against an authoritative source to confirm its authenticity. Still others do facial matching where the user takes a selfie in addition to a photo of the ID, and artificial intelligence decides if they're a match.

To build a product like this in-house, one estimate puts basic costs in the $25,000-50,000 range,[32] just to build a minimum viable product. Data, training and testing costs to ensure accuracy, and once reliable, integration and maintenance costs would all meaningfully increase that number to the hundreds of thousands or millions.[33] Those figures are on par with what startups spend building their product—and they don't have extra time or resources to build a second that doesn't lead to revenue growth.[34]

Those factors—and some state laws' requirements—[35] lead startups to rely on third-party verification vendors, which still must be integrated, also negatively impact user conversion, and increase per-user costs. Generally, integration of third-party technology can be expensive for startups, costing up to $10,000,[36] and taking several weeks. Routing to a third-party verification service might increase user trust, but still carries the time and invasion-of-privacy disincentive that may turn away users. Depending on how they are billed, these services may cost in the tens of cents to several dollars per verification, or several thousand per year.[37] Many startups, especially early-stage startups, operate at a loss until they reach scale, so every additional cost eats into their runway, reducing the life of the company. In our conversations for this report, startups' estimates ran higher, as high as $60,000, with variation depending on size, complexity of the service, and how they go to market.

Age estimation or inference. Companies can use a variety of methods to infer or estimate the age of their users. These methods may be built or used by large companies, but are unworkable for startups. One method involves monitoring user actions on the service for indications they might be a minor, and checking that against the age the user declared they were at sign-up. For example, if a user is interacting with or posting a lot of 'my little pony' content, the service may infer that that user is a minor. This additional data collection and monitoring invokes privacy concerns and strikes many as creepy. (Including lawmakers—ironic, given laws and legislative proposals at least in part precipitate the need for additional age assurance.)[38] Given scale, and the cost to build a system, store, and analyze additional user content to ascertain age, this method is really only practical for large companies. Still, it might be required for all companies by some past proposals containing legal standards that amount to telling companies "you should have known" a given user's age based on their profile or actions.[39]

Other age estimation methods include the use of individual attributes—like their face, palm, voice, or gait—to deduce their likely age using AI. No startup (outside of one aiming to provide age assurance-as-a-service) would ever develop their own age estimation systems, because the costs would be prohibitive and uneconomical. Some established age assurance as a service firms have spent well over $100 million developing their platforms.[40]

There are obvious privacy risks to sharing biometric information. Most third-party providers delete the information within short time frames (usually around one day) but it is still transferred, processed, and stored for an amount of time, making it theoretically vulnerable. Moreover, it is likely to be unclear to an end user what the data practices of a given verification provider are when they are likely to encounter many across the Internet. The same drawbacks for user conversion are present, making it unlikely any startup would use this method unless required by law.

Parental consent. The Children's Online Privacy Protection Act (COPPA) creates requirements for services directed to children under age 13, including that those services obtain verifiable parental consent before collecting personal information of users they have actual knowledge are under 13.[41] The law is generally understood as splitting the Internet between services directed to kids and those only available to those over age 13. Startups that offer services directed to children know about the heightened costs and legal risks that come with entering a regulated space.

Parental consent can take a few different forms in practice, many of which are outlined in the COPPA Rule.[42] (Some services also avoid requirements to obtain parental consent through carefully designed signup flows that do not collect any personal information besides an age self-declaration in order to limit service functionality for under 13s.) Many sites obtain parental consent via email (called the "email plus" method), but this method may only be used if the personal information of the child is not shared (by the service or the user). Other methods of consent include collecting signed forms from a parent, or having the parent call a phone number or video-conference. Parents could also enter a credit card in connection with a transaction.

Each of those methods is obviously tedious—and costly—for services. Initial estimates of costs around verification amounted to $35,000 in engineering costs and $70,000-120,000 in ongoing annual costs.[43] The 2013 update to the COPPA rule is thought to have increased those costs further.[44]

And they're tedious also for parents, who often just want to get their kid onto the service, even if they might appreciate the step that lets them know what their kid is doing online.

Other attestation. Some large services have recently integrated 'social vouching,' where other users the service already knows are above a given age can vouch for the age of the new user.[45] Most startups don't have a critical mass of users or aren't big enough to need or practically use this method, though variations, like invite-only based apps could integrate this by prompting users only to invite others of a certain age. This poses similar flaws as self-declaration.

ENDNOTES

i. *See, e.g., the State of the Startup Ecosystem*, Engine (Apr. 2021), https://static1.squarespace.com/static/571681753c-44d835a440c8b5/t/60819983b7f8be1a2a99972d/1619106194054/The+State+of+the+Startup+Ecosystem.pdf.

ii *Id.*

iii. *See Comments of Engine Advocacy in response to Commercial Surveillance ANPR, R111004*, §V Engine (Nov. 21, 2022), https://engine.is/s/Engine-FTC-Privacy-ANPRMComments.pdf.

1 Pub. L. No. 105-227, tit. XIII (1998), https://www.govinfo.gov/content/pkg/PLAW-105publ277/pdf/PLAW-105publ277.pdf#page=729.

2 Children's Online Privacy Protection Rule, 16 C.F.R. Part 312 (2013), https://www.ftc.gov/system/files/2012-31341.pdf.

3 Children's Online Privacy Protection Rule, 89 Fed. Reg. 2034 (Jan. 11, 2024) (to be codified at 16 C.F.R. Part 312), https://www.govinfo.gov/content/pkg/FR-2024-01-11/pdf/2024-28569.pdf.

4 *See, e.g., Startups, Content Moderation, and Section 230*, Engine (2021), https://static1.squarespace.com/static/571681753c-44d835a440c8b5/t/61b26e51cdb21375a31d312f/1639083602320/Startups%2C+Content+Moderation%2C+and+Section+230+2021.pdf.

5 *See, e.g., Comments of Engine Advocacy in response to Request for Comment on Kids Online Health and Safety, Docket no. NTIA-2024-0008-0001,* Engine (Nov. 16, 2023), https://static1.squarespace.com/static/571681753c44d835a440c-8b5/t/655688597cf5942ae3092cbf/1700169817827/Engine+response+to+NTIA+RFC+on+Kids+Online+Health.pdf/.

6 *See, e.g.,* Malena Dailey, *Content Moderation By The Numbers*, NetChoice (Nov. 2021), https://netchoice.org/wp-content/uploads/2021/11/Content-Moderation-By-The-Numbers-v5.pdf.

7 *See, e.g.,* Tim Bernard, *The Present and Future of Detecting Child Sexual Abuse Material on Social Media*, Unitary (Oct. 16, 2023), https://www.unitary.ai/articles/the-present-and-future-of-detecting-child-sexual-abuse-material-on-social-media#:~:text=The%20baseline%20technique%20for%20detecting,to%20automatically%20identify%20violative%20content.

8 Children and Teens' Online Privacy Protection Act, S.1418, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/senate-bill/1418/text.

9 Conn. Pub. Acts. 2023, No. 23-56, https://www.cga.ct.gov/2024/ACT/PA/PDF/2024PA-00056-R00SB-00003-PA.PDF.

10 *Judge Blocks Arkansas Law that Would Have Placed Unconstitutional Age-Verification and Parental Consent Requirements on Social Media*, ACLU (Sept. 1, 2023), https://www.aclu.org/press-releases/judge-blocks-arkansas-law-that-would-have-placed-unconstitutional-age-verification-and-parental-consent-requirements-on-social-media-users.

11 *See generally Utah Protecting Minors Online*, https://socialmedia.utah.gov/.

12 Krista Chavez, *NetChoice Sues Utah to Keep Kids Safe Online and Protect Constitutional Rights*, NetChoice (Dec. 18, 2023), https://netchoice.org/netchoice-sues-utah-to-keep-kids-safe-online-and-protect-constitutional-rights/.

13 Kids Online Safety Act, S.1409, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/senate-bill/1409/text.

14 *See, e.g.*, Matt Lavietes, *Senator appeared to suggest bipartisan bill would censor transgender content online*, NBC News (Sept. 5, 2023), https://www.nbcnews.com/nbc-out/out-politics-and-policy/senator-appears-suggest-bipartisan-bill-will-censor-transgender-conten-rcna103479.

15 Alvaro Marañon, *NetChoice v. Bonta: First Amendment Challenges to Age-Gating Mandates*, Project DisCo (Oct. 16, 2023), https://www.project-disco.org/privacy/netchoice-v-bonta-first-amendment-challenges-to-age-gating-mandates/.

16 *See, e.g.,* Gabby Miller, *Maryland Kids Code Signed Into Law, But May Face Legal Challenges*, Tech Policy Press (May 10, 2024), https://www.techpolicy.press/maryland-kids-code-becomes-law/; Keely Quinlan, *Vermont Gov. Phil Scott vetoes intensive data privacy bill, citing high 'level of risk'*, StateScoop (June 14, 2024), https://statescoop.com/vermont-phil-scott-vetoes-data-privacy-bill-2024/.

17 *See, e.g.*, Josh Withrow, *Coalition Letter Opposing S. 1080 Cooper Davis Act*, RStreet (May 31, 2023), https://www.rstreet.org/outreach/coalition-letter-opposing-s-1080-cooper-davis-act/.

18 *See, e.g.*, Coalition Letter in Opposition to the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2024, CDT (May 2, 2023), https://cdt.org/wp-content/uploads/2024/05/May-2024-EARN-IT-Act-opposition-letter-FINAL.pdf.

19 *See, e.g.*, Adi Robertson, California governor signs ban on social media 'aiding or abetting' child abuse, The Verge (Oct. 9, 2023), https://www.theverge.com/2024/10/9/23909903/california-ab1394-child-abuse-social-media-regulation-signed-gov-

ernor.

20 An act relating to prohibiting use of social media platforms by children, H.B. 896 (Texas), 88th Leg. (2023), https://capitol.texas.gov/tlodocs/88R/billtext/pdf/HB00896I.pdf#navpanes=0.

21 *See, e.g.,* Kalhan Rosenblatt, *Florida Gov. Ron DeSantis signs bill that bans children under 14 from having social media accounts,* NBC News (Mar. 25, 2024), https://www.nbcnews.com/tech/florida-ron-desantis-signs-bill-social-media-kids-ban-rcna144950.

22 *See, e.g.*, *Age assurance systems framework,* ISO/IEC WD 27566-1, https://www.iso.org/standard/88143.html#lifecycle; IEEE Standard for Online Age Verification, IEEE, https://sagroups.ieee.org/2089-1/.

23 *See, e.g., Privacy Patchwork Problem: Costs, Burdens, and Barriers Encountered by Startups,* Engine (Mar. 2023), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/6414a45f5001941e519492ff/1679074400513/Privacy+Patchwork+Problem+Report.pdf.

24 *See, e.g.*, *Protecting Our Children Online: Hearing before the S. Comm. on the Judiciary*, 118th Cong. (2023) (testimony of Emma Lembke), https://www.judiciary.senate.gov/imo/media/doc/2024-02-14%20-%20Testimony%20-%20Lembke.pdf.

25 *See, e.g., UMD Analysis: Millions of Americans Don't Have ID Required to Vote*, UMD Today (Apr. 13, 2023), https://today.umd.edu/umd-analysis-millions-of-americans-dont-have-id-required-to-vote#:~:text=More%20than%2011%20million%20people,unexpired%20government%20issued%20photo%20ID.

26 *See, e.g.*, Sudhanshu Agarwal, *9 Signup Tips To Skyrocket The Conversion Rate*, loginradius, https://www.loginradius.com/blog/growth/sign-up-tips-conversion-rate/.

27 *See, e.g., Privacy Patchwork Problem, supra* note 22 at 12-13.

28 *Cost of a Data Breach Report*, IBM (2023), https://www.ibm.com/reports/data-breach.

29 *See, e.g.*, *the State of the Startup Ecosystem*, Engine (Apr. 2021), https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/60819983b7f8be1a2a99972d/1619106194054/The+State+of+the+Startup+Ecosystem.pdf.

30 Robert Johnson III, *60 Percent Of Small Companies Close Within 6 Months Of Being Hacked*, Cybercrime Magazine (Jan. 19, 2023), https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/.

31 *See,* Shoshana Weissmann, *Identity verifier used by Big Tech amid mandates has made personal data easily accessible to hackers*, RStreet (June 26, 2024), https://www.rstreet.org/commentary/identity-verifier-used-by-big-tech-amid-mandates-has-made-personal-data-easily-accessible-to-hackers/.

32 *See, e.g.*, 2024 Cost to build a photo verification app, *Crowdbotics* (2024), https://www.crowdbotics.com/cost-to-build-app-type/photo-verification-app#.

33 Henry Sheykin, *How Much Does It Cost To Begin Digital Identity Verification: Unveiling the Startup Costs*, Fin Models Lab (Aug. 19, 2023), https://finmodelslab.com/blogs/startup-costs/digital-identity-verification-startup-costs.

34 *Supra* note 28 at 17-18.

35 Social Media Safety Safety Act, S.B. 396 (2023) Ark. Acts 689, https://www.arkleg.state.ar.us/Bills/Detail?id=SB396&ddBienniumSession=2024%2F2024R.

36 *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.

37 *See, e.g., Top Age Verification Software in 2024*, Slashdot, https://slashdot.org/software/age-verification/#:~:text=On%20the%20lower%20end%2C%20you,facial%20recognition%20or%20biometric%20authentication.

38 *TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms: Hearing before the House Comm. on Energy & Com.*, 118th Cong. (2023) (remarks of Rep. Earl L. "Buddy" Carter), https://energycommerce.house.gov/events/full-committee-hearing-tik-tok-how-congress-can-safeguard-american-data-privacy-and-protect-children-from-online-harms.

39 Children and Teens' Online Privacy Protection Act, S.1628, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1628/text.

40 *Digital identity as a force for good*, Yoti (2021), https://www.yoti.com/wp-content/uploads/Yoti_Overview-2021.pdf

41 *Supra* notes 1,2.

42 *Id.*

43 *Recent Developments in Privacy Protections for Consumers: Hearing before the House Subcomm. on Telecomm., Trade, and Consumer Prot. of the Comm. on Com.*, 106th Cong. (2000) (prepared statement of Parry Aftab), https://www.govinfo.gov/content/pkg/CHRG-106hhrg67635/pdf/CHRG-106hhrg67635.pdf.

44 *Supra* note 2.

45 *E.g., Introducing New Ways to Verify Age on Instagram*, Instagram (June 23, 2022), https://about.instagram.com/blog/announcements/new-ways-to-verify-age-on-instagram.