TRUSTED FUTURE

ISSUE BRIEF May 2025

EMPOWERING PARENTS WITH TRUSTWORTHY OPTIONS TO SIMULTANEOUSLY PROTECT KIDS PRIVACY AND SAFETY.

Legislative proposals should avoid simply shifting responsibility from the app developer who knows their customer and content best to the app stores that distribute them.

By Jim Kohlenberger

Amid a series of high-profile stories about children accessing age-inappropriate content online, there is renewed energy to ensure that parents have the tools they need to ensure that their children only access age-appropriate content online. Unfortunately there are a number of legislative proposals at both the state and national level that could make matters worse without actually solving important issues for parents and policymakers alike.

To get at smarter more effective solutions to protect children's privacy and safety online, there are some key questions policymakers need to ask to make sure we don't inadvertently take steps backwards:

- Is the proposal effective?
- Is it consistent with what parents really want?
- Could proposals meant to protect kids actually harm their privacy?
- Are policymakers aware that there are tools built into app stores that put parents directly in charge of the apps their kids download without sacrificing their privacy?
- Shouldn't every app developer and content producer be responsible for knowing their customers and for providing a safe, trusted and age-appropriate environment for all their users?
- Can these proposals withstand court challenges when every other age verification bill has been struck down in court?
- Might there be an alternative and smarter way to tackle these very real online challenges that further empowers parents, and is even more effective, by taking a smarter and more holistic approach to protect kids' privacy and safety online?

In this article we aim to answer these key questions and highlight some of the obvious problems with app store age-verification bills by looking at the broader context and motivations behind the legislation and proposing a smarter, more effective framework for policymakers to follow.

BACKGROUND

It's no secret that our children are now part of the most connected generation in history. At school, teachers harness technology as a learning accelerator and opportunity equalizer – giving young minds access to the entire universe of human knowledge. But at home, as social media plays an increasingly pervasive role in their children's lives, conscientious parents have serious questions about a growing set of challenges that many believe put their children's privacy, safety and well-being at risk.

To better understand the opportunities and challenges that parents are confronting today, Trusted Future conducted a comprehensive national survey of parents' attitudes about technology. It found that parents are overwhelmingly (90%) concerned about protecting their children's privacy, identity and safety online – and found parents' top priority from policymakers (63%) is adopting strong baseline privacy protections for children.

In addition, we found parents want to play an active role in their child's online experience. Nearly 9 in 10 parents (86%) believe talking with their kids about their family's rules and expectations is one of the most effective strategies for helping them establish good online habits. In addition, according to a survey by the Family Online Safety Institute, 87% of parents already use tech tools to oversee their children's digital lives. For example, many are taking advantage of the plethora of tools being built into smartphones to protect children's privacy and safety. These tools allow them to set limits for the amount of time their children can spend with specific apps, block mature content, restrict in-app purchasing, set limits on who their kids can chat with, automatically detect and block explicit content, limit apps that attempt to track their children's online activity, and utilize tools that puts parents in charge of app download approvals. These trustworthy parental controls are being used to reinforce good habits — and create safer online spaces for kids to learn and play. That's great news.

Nonetheless, parents continue to express significant concerns regarding the access to and impact of social media. Although the science is still unsettled, a 2023 Surgeon General's report warned that social media presents a "profound risk of harm" to the mental health and well-being of children and adolescents. While major social media platforms say they protect underage kids by requiring any user to be at least 13 years of age, as required by law, the Surgeon General found that a whopping 40 percent of children between 8 and 12 are nonetheless using social media platforms today. Building on these concerns, a coalition of 33 state attorneys general sued Meta (owner of Facebook and Instagram) for knowingly allowing underage users to hold accounts, and failing to implement an effective age verification system. The state attorneys general complaint says Meta had received over 1.1 million reports of users under the age of 13 on its platform since early 2019, but rather than discontinuing the accounts, it continued to collect information from the underage children, and profited from advertisements targeted at them. According to a Harvard study, in 2022 alone, social media platforms generated $11 billion in revenue from advertising directed at children and teenagers, including nearly $2 billion in ad profits derived from users age 12 and under. One of the authors of the study says, the "study suggests [social media companies] have overwhelming financial incentives to continue to delay taking meaningful steps to protect children."

THE PROBLEMS WITH CURRENT PROPOSALS

It is true that no age verification technology is perfect, or without significant drawbacks. But rather than policing their own sites, and working responsibly to implement effective solutions to remove underage children from their platforms, the major social media companies are now instead lobbying to shift their responsibility to device manufacturers, and their app stores, to do the age verification instead. They even launched a new lobbying coalition to further their efforts. According to Politico, "To protect kids online, Mark Zuckerberg says Congress should focus on Apple and Google — not Facebook and Instagram." Politico reports, "The Meta CEO, owner of the two social media sites, is flooding Washington with ads aimed at convincing lawmakers to require his rivals' app stores to verify shoppers' ages and require parental consent for kids to download social media apps."

So why would social media companies want to shift the responsibility for policing their sites? Is it just that the investment in the technology is too expensive or too hard? The New York Times has suggested that the coordinated legal approach by the state attorneys general is reminiscent of the government's pursuit of Big Tobacco in the 1990s – which led to an unprecedented financial settlement. When just one thirteen year old's class-action lawsuit seeks $5 billion in damages against Meta, some speculate that the social media company is trying to get out from under a potential multi-billion-dollar legal liability, by transferring the liability and responsibility for age verification to other companies.

Regardless of the motive, their lobbying efforts are having success. In March, Utah became the first state to adopt the social media backed proposal to require smartphone manufacturers to do age verification instead of the social media apps verifying it themselves. Texas isn't far behind with Senate Bill 2420, its App Store Accountability Act. And now, a new piece of legislation has been introduced in Congress by Representative John James (R-MI), to largely do the same thing. These bills aren't just being backed by Meta, but also by companies like Tinder's parent company, the Match Group, and Pornhub – one of the largest distributors of online pornography – who also have had age verification challenges.

So what do the bills do, and will they work? At a high level, Meta describes the bills as preventing kids from downloading apps from app stores without parental approval – which sounds pretty positive. But that's not actually what either the Utah, the Texas, the Congressional or the many other similar state bills do. For example, both Google and Apple already have built-in functionality that puts parents in charge of their children's app download approvals – what proponents claim the bills are designed to do. Instead, what these social media backed bills actually do is force your phone to share your child's specific age with all app developers, not just those your child wants to use but also those with risky content – effectively giving your data to millions of companies. And they require it to be shared without parental consent or rules on how information about your child can be used. It takes away a parent's ability to choose whether sensitive information about their kids is shared, even though 89% of Americans told the Pew Research Center that they are already concerned about the information that social media platforms have about their kids. When parents already have concerns about the vast quantities of data social media already collects about their kids, why should legislators require them to have even more?

These proposals don't just impact parents and kids. They require your phone to check the age of every user – likely using a government issued ID which children don't even have yet – and it requires it for every download even though only a small fraction of apps in apps stores host age-sensitive content. So, for example, if a 60-year-old wants to download a weather app, they'd still have to verify their age first. It's sharing private information for every person, on every download.

It's also not an effective solution for kids. Clever kids can easily circumvent an app store-based process merely by creating a social media account using any web browser on any laptop or computer outside of limits placed on your phone – underscoring why we need a more comprehensive approach. And age assurance is especially hard when a device being used by several children is common – for example, a family tablet that is shared by a 14-year-old and a 10 year-old. It's no wonder experts who have reviewed these "app store accountability" bills argue that while they may be well intentioned, they are unworkable, misguided, create significant children's privacy risks, all without being effective or actually addressing the harms that policymakers are seeking to address.

The bills also raise serious constitutional issues suggesting they are likely to be struck down in court. When court after court – although sympathetic to the goals – keeps blocking state age verification laws aimed at requiring parental permission for minors to have social media accounts, (Ohio, Arkansas, etc) we need to find newer smarter ways to protect children.

There really are no silver-bullet solutions to what have historically been a complex set of issues. But there are ways to address these challenges by taking a more comprehensive and thoughtful approach to protect kids' safety, privacy, and parental rights in a way that is based on collaboration and recognizes everyone's shared responsibilities.

Because the limited number of apps and websites that host age-restricted material know their content best, they are best positioned to put the right age restrictions in place. Think of a shopping mall: it's the movie theater within it that is responsible for checking IDs before letting people into an adult-rated film, and it's the mall restaurant who verifies age before serving alcohol. We don't require the mall owner to check every person's ID to enter the mall, especially if someone is just going to the food court. It is the responsibility of the service provider to know their customers, and to provide a safe, trusted and age-appropriate environment for their users.

A BETTER PATH FORWARD

Instead of requiring the age of every user to be checked at the door of the app store and shared with every developer without user consent (as the Utah bill does), we should put parents in charge of deciding whether private information about their kids should be shared. Further, the age-range information should only be shared with platforms that need it instead of with millions of companies that may not. It helps ensure parents are in charge of decisions around the apps their children download (as they are today using app store tools), and make these tools easy to use and readily available. This ensures parents have the ability to choose how and whether limited age-range information about their children (for example whether they are a teen or minor) is shared. To keep kids safe online, we need policies that reflect how technology actually works, and that put parents in charge.

Parents understand these choices. A recent AudienceNet survey, for example, found that 93% of parents agree that social media, gaming and other adult-oriented content platforms should be the ones who verify users' ages before granting access. By contrast, when asked who holds the bigger responsibility for preventing minors from accessing adult content online, only 7% of parents pointed to device manufacturers who operate app stores.

With the right combination of public policy, tools, technologies, and educational efforts we can create a safe, effective, and more trusted privacy-preserving set of solutions that keep parents in charge.

But we don't need to wait, there are steps companies, parents and policymakers can and should take today to help create a more positive digital environment for our kids. They can:

- **Preserve children's privacy by ensuring that data about children – including age – is only sent when parents give consent.** We should ensure parents retain the ability to choose how and whether limited age-range information about their children (for example whether they are a teen or minor) is shared in a privacy-preserving way with the small number of developers who create apps that need the information to deliver only age-appropriate content. By putting parents in charge of their children's privacy, and preventing a child's specific age from being shared with millions of other developers, we can help keep their privacy safe.

- **Improve national baseline privacy protections for children.** With 90% of parents concerned about protecting privacy and the identity of their children online, and 4 out of 5 parents (85%) specifically concerned about protecting the privacy of their children's age, policymakers should adopt strong and comprehensive national privacy protections for kids as the first step as they look for strategies that can further safeguard children without putting their privacy at risk. The bipartisan Children and Teens' Online Privacy Protection Act (COPPA 2.0), for example, not only strengthens children's privacy online but also bans targeted advertising to children and teens, and prevents the harvesting of data to track children. As one Senator said, it is "the tool that will give parents the peace of mind they need and keep their children's personal information secure." Congress, not states or the Supreme Court, should lead the way in creating a national privacy framework, in finding the right balance in children's safety issues, and in avoiding a patchwork of state verification laws that frustrate parental choices.

- **Innovators should adopt appropriate safety measures, guardrails and tools that put parents in control.** Parents, not platforms nor politicians, need to be the primary gatekeepers of their children's digital lives – and we need to empower them with the tools that meet their family needs, and enable teens to thrive online. Parents already utilize a whole variety of tools on smartphones that allow them to protect their kids in ways that meet their own particular family needs and values. For those who may not know about these tools, we need innovators, educators, and parental advocacy groups to work together to help parents become more aware of existing parental control tools (like those that enable parents to control which apps their kids download) and help them play an active role in protecting their children's privacy and safety in ways that best meet their own family's needs. Because developers know their apps best, we also need app developers to create new tools and experiences – using the new age-range signals that parents can choose to share about their children – so that children have an age-appropriate experience.

- **Engage kids to help ensure they thrive online.** Just like no tool fits every hand, no solution fits every family. Choosing parental control tools that fit a family's needs depends on the devices that kid uses and the boundaries a parent has decided to set for the family. The Family Online Safety Institute's survey on these issues, for example, found parents see themselves as having the most responsibility for managing their children's access to age-appropriate content – more so than technology companies or the government. For many parents, proactively engaging with their children is an important part of parenting and figuring out what works best for their family considering their children, values and routines. Trusted Future's survey found that 75% of parents believe that having the "tech talk" with teens is now just as important as having the "sex talk." For these parents, having a strong parent-child relationship with good communications is key to helping children, and they now have age appropriate resources to help them with those conversations to ensure their children can thrive online. And to help parents navigate this new digital domain, Trusted Future has developed a set of common-sense guidelines and tips parents can use to foster greater trust in the technologies they use every day and better protect their children's privacy, safety, and security.

- **Empower children with cyber savvy skills.** More broadly, we should do more to boost digital literacy and digital skill building efforts in the classroom to help kids learn about the online world in a way that helps them become productive digital citizens – because there is more to making the Internet a good place for children than just protecting them from objectionable content. They need to be empowered with basic cyber savvy skills allowing them to recognize potential threats, use strong passwords, and know how to avoid strangers, scams, and malicious links. They need to gain an understanding of responsible online behavior, and learn about how to tell what information can be trusted online.

CONCLUSION

Protecting children’s data privacy and safety is now an urgent and collective imperative. But we need to make sure policymakers are asking the right questions so we get to smart, effective, trustworthy solutions that are effective, protect privacy, can withstand court scrutiny, give parents the tools to decide what apps their children download, and – above all – protect children’s privacy by putting parents in charge of the decision as to whether they want private information about their children shared with strangers.

By implementing smart policies and safeguards that strike a balance between protection and exploration – between privacy and safety – parents can encourage their children to explore and learn in a safe, age-appropriate environment that also protects their privacy. It’s the path that can lead us toward a more trusted future.

TRUSTED
FUTURE