

March 25, 2025

The Honorable Gus Bilirakis  
Chairman  
Committee on Energy and Commerce  
Subcommittee on Commerce,  
Manufacturing, and Trade  
United States House of Representatives  
Washington, District of Columbia 20515

The Honorable Jan Schakowsky  
Ranking Member  
Committee on Energy and Commerce  
Subcommittee on Commerce,  
Manufacturing, and Trade  
United States House of Representatives  
Washington, District of Columbia 20515

***RE: Statement for the Record of ACT | The App Association for Subcommittee Hearing,  
“The World Wild Web: Examining Online Harms”***

Dear Chairman Bilirakis, Ranking Member Schakowsky, and Members of the Committee:

ACT | The App Association is a global trade association for small and medium-sized technology companies. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. Today, U.S. the digital economy is worth more than \$1.8 trillion annually and supports over 6.1 million American jobs.<sup>1</sup> We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology.

App Association members are dedicated to improving the safety and security of products and services in the digital economy. The internet is a vastly complex arena, and children’s access to the internet requires the utmost level of care. We thank the Subcommittee for its careful consideration of policies addressing minors’ access to harmful online content.

Certain policy proposals that put the onus for children’s safety entirely on app stores,<sup>2</sup> however, would not be effective in protecting the most vulnerable internet users. We believe instead that these policies would shield social media services with a history of malfeasance and shift liability and compliance costs to small app companies via the app stores. Policymakers should be hesitant to support children’s online safety legislative language proposed and supported by companies facing potentially billions of dollars in

---

<sup>1</sup> ACT | The App Association, *State of the U.S. App Economy: 2023*, <https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf>.

<sup>2</sup> See, e.g., Gabby Miller, “The age verification battlefront reopens,” Politico Pro (Feb. 20, 2025), *available at* <https://subscriber.politicopro.com/newsletter/2025/02/the-age-verification-battlefront-reopens-00205079> (paywalled); <https://le.utah.gov/~2025/bills/static/SB0142.html>; <https://www.congress.gov/bill/118th-congress/senate-bill/5364>.

finer for violating children's privacy.<sup>3</sup> For small app companies, the problem with the bills is twofold: first, that the bills would offload compliance burdens away from large social media companies and onto smaller app companies; and second, that they would likely worsen current, developer-created solutions for parental control, which would in turn degrade app makers' offerings.

### **Congress Doesn't Need to Create Smart Device Parental Controls; They Already Exist and They Work**

App store age verification proposals appear at least in part motivated by a desire to put parents in control of their children's smart devices. One commercial airing during the National Football League playoffs last year showed a parent receiving a text message prompting them to approve their child's request to download an app. The ad then called for legislation to create such a feature. In fact, this is exactly how parental controls work in current practice on Android, iPadOS, and iOS devices.

When parents set up smart devices for their children now, they can configure the device so that access to certain online content is only possible via the parents' or guardians' permission (see example below). They can also choose to completely disallow certain actions, such as accessing a browser. App stores enforce these preferences, blocking any downloads that parents and guardians disallow as well as any downloads of apps designated as outside the age range of the child user of the device, regardless of parental permission. Parents may adjust the settings that apply to the device, including to allow a child that is close to their ninth birthday to download an app meant for children aged nine and above.

Under this framework, the parent is in charge of a device assigned to their child. They can parent as they see fit, and the developers providing these capabilities design their user interfaces according to parental preferences, rather than according to government officials' assessment of compliance. As such, parental control tools on offer today are in a constant process of improvement and refinement, which is better for parents and developers than freezing them in place to serve the goals of record-keeping and enforcement avoidance that come with a government regime contemplated in age verification proposals.

---

<sup>3</sup> <https://www.nytimes.com/2023/11/25/technology/instagram-meta-children-privacy.html>.

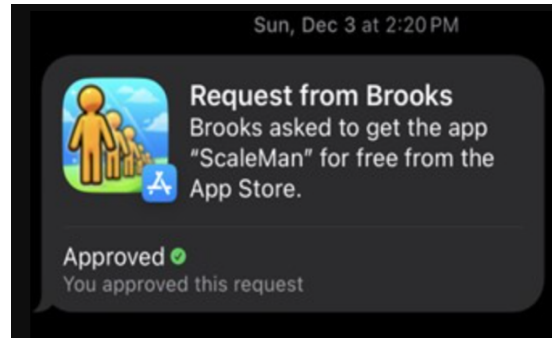


Figure 1: Screenshot of a notification sent to a parent of a request for their child to download an application to the child's device.

App developers currently must accurately indicate the age appropriateness of their apps when distributing through one of the official app stores—or else be subject to removal from the app stores. The internet is full of content that is harmful or inappropriate for minors. To mitigate the risk and limit access to harmful content, developers and device manufacturers implement tools that allow parents to configure devices for their children.

When configuring the device, parents can eliminate any possible access to the browser itself, confining their children's experience to apps that are approved for their ages (apps with browser access are strictly for 17 and over on the app stores).<sup>4, 5, 6</sup> Parents and guardians should not need to comply with layers of government red tape just to effectuate a much weaker level of control than what they currently have over their children's online experience.

To the extent the Subcommittee wishes to give parents flexible, meaningful control over their kids' online experiences via their smart devices, this already exists, and any government regime to change it would inevitably add costs for developers and headaches for parents. The failures to protect children's privacy that exist today are decidedly outside the purview of app stores and smart devices and solely on social platforms, including those the proponents of age verification mandates provide.

### **Mandatory app store age verification proposals are based on flawed assumptions about the app ecosystem and would produce a disproportionate impact on small and medium-sized tech companies**

---

<sup>4</sup> Step-by-step guide to turning on device level filters currently available for Apple iPhones and tablets: <https://support.apple.com/en-us/105121>

<sup>5</sup> Step-by-step guide to turning on device level filters currently available on Samsung Galaxy phones and tablets: <https://www.samsung.com/us/support/answer/ANS10003399/>

<sup>6</sup> Step-by-step guide to turning on device level filters currently available for Apple iPhones and tablets on the Motorola phone - [https://en-us.support.motorola.com/app/answers/detail/a\\_id/156314/~parental-controls--moto-g-play](https://en-us.support.motorola.com/app/answers/detail/a_id/156314/~parental-controls--moto-g-play)

Small and medium-sized tech companies and developers, like our members, play a crucial role in helping manufacturers turn an ordinary phone or tablet into a smart device through the creation of the apps and other layers of software that work with the physical devices. These businesses are at the forefront of creating new ways to empower parents and guardians to enable access to educational and beneficial content for their children via smart devices while keeping parents at the center of their children's online experience and maximizing their ability to protect them. In the current ecosystem, a developer of a stargazing app with five employees can list their software as appropriate for children aged 12 and above (if on iOS)<sup>7</sup> or 10 and above (if on Google Play or another platform)<sup>8</sup> for example. Parents may wish to allow access for their 12-year-old, or they could decline access. This is solely at the parents' discretion.

If age verification legislation is enacted, however, the parent has effectively no choice in the matter, the issue having been decided for them by the government. The child must be identified as "under 13," pursuant to the app store's age verification requirement. On notice as to the child's status, the developer would then be obligated to follow the requirements laid out in the new law.

In addition, the actual knowledge as to a child's under-13 status effectively removes the ability for developers to offer things like stargazing apps to general audiences. They can either choose to market to "children," subjecting themselves to verifiable parental consent (VPC) requirements under the Children's Online Privacy Protection Act (COPPA),<sup>9</sup> or they can completely shut off access to their services by children, setting the cutoff at age 18 just to be safe. Of course, the latter is much more likely to be the case, and there are two consequences of this: 1) your 12-year-old no longer has the privilege of accessing high-quality stargazing apps that traverse bona fide app review and therefore are subject to meaningful parental controls via platform-level settings; and 2) 12-year-olds are unlikely to accept this fate and will access low-quality versions of the software operating in legal grey or black markets unchecked by app store constraints and completely outside policymakers' and parents' purview. Meanwhile, the good actor stargazing apps have likely lost much of their consumer base, left exclusively with consumers who have verified explicitly and pursuant to bureaucratic mandate that they are over 18. In a less likely scenario, they may have convinced their investors to allow them to become a VPC paperwork shop first and foremost, relegating the stargazing function to the backseat of their business plan priorities.

---

<sup>7</sup> <https://developer.apple.com/help/app-store-connect/reference/age-ratings/>

<sup>8</sup> <https://www.esrb.org/ratings-guide/>.

<sup>9</sup> COPPA applies to operators of commercial websites and online services "directed to children under 13," <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions>.

Adding to the VPC compliance costs, app store age verification proposals would put the ball in the developer's court to maintain a paper trail on parents' consent to simply download the app (COPPA is not predicated on "downloads," it is predicated on collection of information—two completely separate things). Under these proposals, the app store's flag indicating parental consent only applies to the initial download. Parents often revoke consent, but this revocation must be effectuated between the parent and the developer under the proposal, since app stores have no functional ability to delete software from an individual's device. Under current law, parents effectuate this permission withdrawal by deleting the app—and decline permission for future downloads. But under app store age verification proposals, the developer would be the record-keeper for the entire age verification-predicated parental consent mechanism (even though deleting the app is a far easier method). This is an inevitable consequence of mandating age verification as a precondition of using the internet in the first place, since each link in the chain knows the age of the person and must act according to that knowledge. It follows that attempts to limit liability solely to app stores cannot succeed and would ultimately create significant legal uncertainty for small businesses in the app economy.

Whether the developer decides to exclude any consumer under 18 or not, under current proposals, the stargazing app would be less credibly competitive with larger rivals with big compliance budgets. It would be saddled with a new reality of frustrated parents, red tape, and legal uncertainty. This would be true for virtually all apps with high educational utility, including those used by school districts and therefore subject to the Family Educational Rights Privacy Act (FERPA), designed for kids, teens, and adults. It is currently unclear how age verification legislation would conflict with or work around school district norms and FERPA requirements, and it is unlikely the resulting legal uncertainty could be waved away with savings clauses or rules of construction. The introduction of this level of legal uncertainty weighs far more heavily on small businesses like the five-employee stargazing app, providing a relative advantage to its larger competitors with legal departments and compliance resources.

App store age verification proposals undermine the ongoing progress that our businesses and developers are making instead of supporting the innovative spirit of the digital ecosystem.

*App store age verification proposals incorrectly assume that homes are multi-device homes, and that all children and youth have their own devices.* One chief assumption in many of the app store age verification proposals is that all children and all homes are multidevice homes. It is quite common for parents to use their own logins for a household laptop or tablet that they allow their kids to use. In instances like this, children may bypass all of the consent requirements that could be established by these proposals.

*App store age verification proposals incorrectly assume children's devices are on the same operating systems as their parents'.* To the contrary, it is common for parents and kids to have devices that run on different operating systems with different app stores. Any purported advantage over social media platforms an app store has in being able to verify users is inapplicable in cases like this, since the minor's app store is not the same as the parents'. App stores are not generally in a better position than social media companies to verify users' ages and this is even more demonstrably the case when parents and kids use different app stores.

*App stores and social media platforms are not one in the same, and not all apps are social media apps.* Social media apps have specific challenges with the ongoing use by children under the COPPA threshold using their platforms. This letter from Senators Bill Cassidy and Ed Markey details the lengths to which some platforms go to skirt the law's requirements and helps explain why age verification proposals would help bad actors evade this responsibility even as it would add costs for small business app developers and red tape for parents.<sup>10</sup>

*Social media companies have their own communities.* Social media companies are businesses that require each and every user to create an account to have access to a digital community. In these communities, users can communicate with each other through messaging, shared photos, comments on posts, among other things intentionally created for both teen and adult crowds, and the social media platforms own the responsibility to protect their users. Whether a user is accessing their account via a browser or an app, their access is accomplished via their account or accounts with the social media company, not via the app store. This means that whatever gating measures an app store employs, the relationship between the user and the social media platform is ultimately the only cross-context way of limiting their access to it. Thus, the social media company inevitably should be the entity responsible for restricting account creation of minors and compliance with data governance laws and limiting targeted advertisements.

*Many of the social media companies are also websites.* This means that that even if the social media companies leave an app store, laptop and smartphone users could still create social media accounts on these specific companies' websites. App store age verification proposals do not take this into account.

*The contract canard.* Some have raised the argument that because contracts are often unenforceable against minors, app stores must be obligated to obtain parental consent for the download of an app onto a minor's device.<sup>11</sup> This argument is a red herring. Mandating an agreement *between a parent and an app store to download an app* does not solve the problem of *parents failing to enter into agreements with social media platforms on behalf of their minor children*. Parental consent to download a social media app does not create a

---

<sup>10</sup>[https://www.markey.senate.gov/imo/media/doc/markey\\_cassidy\\_letter\\_to\\_meta\\_on\\_states\\_coppa\\_complaint\\_-\\_120523pdf.pdf](https://www.markey.senate.gov/imo/media/doc/markey_cassidy_letter_to_meta_on_states_coppa_complaint_-_120523pdf.pdf)

<sup>11</sup> <https://le.utah.gov/committee/committee.jsp?year=2025&com=SSTTPT&mtgid=19653>.

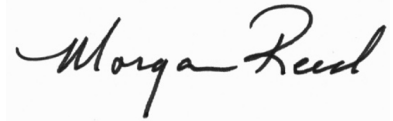
contract between a parent and the social media platform. The mere provision of consent to download the app, for example, does not cover any of the minor's activity while on the social media platform. Nor does it cover any changes to a parent's consent or updates to permissions within the social media platform for the minor. Parents must work under an agreement directly with the social media platform to accomplish these changes. Moreover, the minor's social media account exists independently from the app itself. It can be accessed on the open internet, not just via the app—and even if the account were only accessible via the app, consent to download at the app store level is not the same thing as consent to a set of terms of service within an app. That still has to be accomplished separately, unless the vision is for the app stores to merge completely with the social media platforms, which seems unlikely.

From small business app developers' perspective, treating app store-level permission as agreement to an app's terms of service imposes a form of liability that is currently out of the app stores' purview, and for good reason. In order to ensure it can comply with mandates to carry out functions over which it does not have control currently, a covered app store would probably have to take measures to exert more control over apps' relationships with users. In reality, this could take the form of things like constant audits of social media platforms (and relevantly for the App Association, all other app developers) by app stores. In summary, the notion that consent to download equals privity of contract covering the entire relationship between a minor's parents and the owner of an app appears to be based on a conflation of the two concepts. Unfortunately, treating app stores as in control of relationships between users and app developers would lead to legislation that does not fix, and could actually worsen, the stated problem—that minors experience a host of threats and issues on social media platforms.

Although legislating app store age verification is likely to be harmful to the ecosystem, Congress is right to focus on updating COPPA. This Subcommittee has laid the groundwork for COPPA reform and adjusting the law's requirements so as to allow for flexible and technology-driven approaches to obtaining VPC would go a long way toward addressing the issues sought to be addressed in this hearing. Parents must be in better control of their kids' online experience and Congress has a role in providing a better legal backdrop for this in updating VPC and COPPA more generally.

Thank you for your time and consideration. We trust that the Subcommittee will carefully evaluate the points raised while focusing on alternative ways to support both the protection of minors and the growth of the app economy.

Sincerely,

A handwritten signature in black ink that reads "Morgan Reed". The signature is written in a cursive style with a light grey rectangular background behind it.

Morgan Reed  
President  
ACT | The App Association