December 2, 2025

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

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

The Honorable Brett Guthrie
Chairman
Committee on Energy and Commerce
Washington, District of Columbia 20515

The Honorable Frank Pallone
Ranking Member
Committee on Energy and Commerce
Washington, District of Columbia 20515

RE: Hearing on *Legislative Solutions to Protect Children and Teens Online*

Dear Chairman Bilirakis, Ranking Member Schakowsky, Chairman Guthrie, and Ranking Member Pallone:

Thank you for the opportunity to submit testimony for the record on your hearing titled *Legislative Solutions to Protect Children and Teens Online*. 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. 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. No matter the industry in which our member companies innovate, they all agree that keeping children safe online is essential. Well-crafted legislation with clear guidelines can strengthen the tools available to parents and enable developers to efficiently build safe and secure digital experiences.

ACT has maintained a strong commitment to privacy protection and online safety throughout its history. We frequently provide testimony and expert guidance on the subject, including in a 2023 U.S. House of Representatives Committee on Energy and Commerce hearing, *Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information*.[1] Over the years, we have sought to ensure small businesses can comply with kids' safety and privacy laws, bridging the gap between enforcers and entrepreneurs. These efforts sought to translate the Children's Online Privacy Protection Act's (COPPA's) mandates for small business app companies and included Moms with Apps and Know What's Inside. Whether through formal designations like these or in our day-to-day advocacy, we focus on children's online safety and privacy and on strengthening the role of parents in the safety discussion. We will continue to champion strong privacy protections for all consumers, including

[1] https://www.congress.gov/118/meeting/house/115819/witnesses/HMTG-118-IF17-Wstate-ReedM-20230427.pdf.

children, and support thoughtful, privacy-protective solutions that promote safety, trust, and accountability in digital environments.

Our members have a vested interest in policy discussions about privacy and online safety. As they build new products in industries ranging from agriculture to hospitality to cybersecurity, they must carefully consider their users' expectations and ensure designs reflect appropriate privacy and safety protections. This work includes designing accessible, user-friendly tools and tailoring product designs, features, and specifications for the intended audience. Many of our members already include privacy-focused features and work to ensure their products are age-appropriate.

Safety Features Need to Keep Kids Safe

As the Committee deliberates options to advance online safety, it may be helpful to consider the protections already in place across the mobile ecosystem. First, mobile device manufacturers, established app store providers, and developers have implemented a range of tools to help parents keep children safe online. For example, Apple's App Store and the Google Play store assign age ratings to apps, and both platforms offer robust controls that parents or guardians can use to monitor the content their children access on their devices.[2] These features include requiring approval for app downloads, limiting accessible content or features, and restricting changes to privacy settings.

Further, app makers can evaluate the content and features of their apps and assign an age category that aligns with its intended use. This type of age categorization works in tandem with other protections on devices to help parents understand what content their children may access through that app. Companies can then independently monitor their apps to ensure content remains appropriate for the age category they have selected for the app.

Finally, minimizing data collection is a fundamental component of keeping kids safe online, and can significantly reduce the amount of data at risk of misuse. For example, apps that perform limited or targeted functions, such as flashlight or cooking apps, should not need access to precise location data or stored passwords. Limiting unnecessary collection is a key step toward decreasing the amount of available data bad actors might be able to access. Unfortunately, many current proposals for online safety do not appropriately incorporate data minimization as a safeguard.

Concerns with the App Store Accountability Act

Among the proposals under consideration is the App Store Accountability Act (H.R. 3149). While ACT shares the Committee's goals of empowering parents, protecting children, and

[2] *See* https://support.google.com/googleplay/answer/1075738?hl=en; https://www.apple.com/families/.

providing developers with clear guidelines on online safety, the bill introduces several privacy, security, and usability complications that will ultimately undermine these objectives.

In a bid to stop children from accessing potentially unsuitable content, the bill would require all app developers to receive an age signal from a device's app store when a user initiates a download. This age signal would give developers "actual knowledge," as defined under COPPA, and trigger extensive compliance obligations, including requirements to obtain verifiable parental consent (VPC) for users under 13, regardless of the nature of their app or the risks it poses to children. Many companies in local communities create apps that are appropriate for users of all ages, including pizza places, barber shops, and tax preparation firms. The App Store Accountability Act (ASAA) would effectively require these developers to redesign their apps to meet COPPA obligations without meaningfully improving children's online safety.

Moreover, age verification, the process of ascertaining beyond any doubt the age of a user, is an inherently privacy-invasive process. Although the bill requires the app store to "[limit] its [data] collection, processing, and storage to what is strictly necessary to verify a user's age, obtain verifiable parental consent, or maintain compliance records," app stores will need to collect sensitive information to verify users' ages beyond a reasonable doubt and determine the parent-child relationship.[3] By devolving definitive knowledge of age category to all developers distributing through the stores, ASAA further saddles any business with an app with accompanying obligations. Although the bill would allow developers to delete some of this data, by carving all businesses with an app into COPPA compliance, ASAA mandates the additional record-keeping necessary to associate kids with guardians in order to accommodate revocation of consent, among other COPPA-related obligations. One estimate puts the initial cost for small businesses to comply with app store age verification mandates at up to $280 billion, not counting the ongoing expense of complying with COPPA and the additional risk of handling sensitive personal data many companies never expected, or wanted, to collect.[4]

The bill's approach to age verification also places onerous requirements on parents and legal guardians. Experience has shown that unnecessary additional friction, including the kinds associated with superfluous age verification and excessive instances of verifiable parental consent, tend to dissuade families from making use of the protections and prompt them to circumvent the available tools. A more effective system would minimize friction so that parents make use of the protections available on their children's devices.

Thoughtful Designs for New Legislation

Online safety legislation should empower parents to safeguard their children online and provide developers with guidelines to design safe, age-appropriate digital experiences. As discussed above, parents already have access to tools that support safer online experiences, such as age ratings, restrictions on downloading new apps, and features that allow developers to embed

[3] See Sec. 3(a)(6)(A) of H.R. 3149, the App Store Accountability Act.
[4] https://trustedfuture.org/the-huge-costs-for-small-businesses-of-app-store-age-verification-bills/

content filters into apps with messaging functions. When policymakers impose additional compliance requirements through broad, untailored mandates, they risk shifting these controls away from parents and toward the government and forcing developers to prioritize legal compliance over parent-centered product development. Moreover, mandating age checks at a single layer of the stack—on a device, in an app store, or on each individual app—can leave other layers without protections and offer only an illusion of safety.

A more effective approach focuses compliance obligations on businesses that intentionally direct content to children, rather than imposing broad requirements on services that are not designed for them. For example, an age signal system in which app stores provide age information only to developers of child-directed apps or to apps with content that poses age-related risks would avoid extending COPPA obligations to all developers, including local restaurants and tax preparation tools. By limiting obligations to apps actually designed for children or adults, this approach would concentrate safety resources where they are most needed while minimizing burdens imposed on other developers.

Beyond legal burdens, such an approach would also reduce the volume of age information shared across the ecosystem and, in turn, lessen the risks posed if such data were ever exposed in a breach. Any age-checking system introduces privacy risks, and applying those requirements universally would increase data exposure without meaningfully improving safety. More intrusive age verification methods, such as the processing of biometric data or government-issued identification, create significant security concerns, while even less intrusive approaches introduce additional points of vulnerability across the ecosystem. For these reasons, if the Committee pursues an approach that relies on age verification, it should adopt a targeted, privacy-protective model that limits data collection and applies compliance obligations only to developers of child-directed content.

The *Parents Over Platforms Act*, draft legislation on the Committee's docket for this hearing, strikes a better balance on these points. The bill would require that app stores prompt users setting up an app store account to indicate the age of the device's primary user, allowing for additional information to be shared to authenticate the person's age, subject to the parent or guardian's discretion. The stores would only be required to make flags available to the kinds of developers that would potentially need to know the age of a user—those that provide different experiences for minors than for adults or that provide content only suitable for adults. Although legislation to rework kids' safety tools on the app stores is probably not necessary and creates some risks, this framework fits far better between existing kids' privacy laws and the tools currently available and evolving to better fit the needs of parents, guardians, and families.

Finally, moving forward, any online safety legislation should include a data minimization standard as a foundational safeguard. An effective version can be found in the California Consumer Privacy Act, which limits collection, use, retention, and sharing of data to what is

reasonably necessary and proportionate for a given purpose or for another compatible purpose.[5] Such a provision would protect consumer data from unnecessary collection or overuse while still providing businesses with reasonable flexibility to innovate and serve their customers.

The Children and Teens' Online Privacy Protection Act (CTOPPA)

A few aspects of this legislation stand out as welcome efforts to update the law. Ideally, these updates should help developers better understand their obligations and parents and teens better exercise control over personal information. For example, the legislation would codify some of the FTC's existing guidance on the applicability of verifiable consent obligations to entities contracting with educational institutions. The Family Educational Rights and Privacy Act (FERPA), a separate federal privacy silo focused on the services provided by independent companies to students as part of school curricula. The FTC currently handles the awkward handoff between COPPA, which applies outside the school context, and FERPA—which applies within a school's scope of activities—by guidance, but statutory clarity would help significantly. We may seek changes to these provisions, but at a high level, providing more statutory clarity as to where FERPA ends and where COPPA begins is a concept we support.

The legislation would also update the applicability of COPPA's overarching protection to teens ages 13 to 17. The bill would appropriately vest "verifiable consent" with the teens themselves rather than parents. The provision would also enabling parents some visibility into how and which kinds of data are collected about their teen children, which may help parents protect their teen children, but carries some risks as well to teens' autonomy in certain situations. In any case, simply applying parental controls as they appear now under COPPA to ages 13 to 17 would fit poorly with teens' experiences and relative independence within their families, and the scaled approach of CTOPPA attempts to respect the inherent differences between teens and children under 13.

Lastly, the bill's provision expanding allowable forms of verifiable consent are welcome additions to the statutory framework. Although the updates the FTC recently made via rulemaking appropriately sought to allow for the use of newer technologies to accomplish VPC, the legislation would provide a much-needed statutory basis for further updates, via a "feasibility assessment" of common verifiable consent mechanisms. We applaud the sponsors of the legislation for allowing the FTC to try and keep pace with further technology developments that can put parents in better, more meaningful control of their children's digital experience and look forward to providing more detailed input on how best to accomplish this.

Conclusion

Small businesses want to help keep kids safe on the internet. They need a way to contribute to that safety without being forced to collect, process, and store large amounts of sensitive

[5] https://cppa.ca.gov/pdf/enfadvisory202401.pdf

information on their users. Proposals like the App Store Accountability Act shift the burden of child safety onto individual app makers and the app stores, rather than recognizing that it takes coordination from every level to ensure children can safely use online tools. We urge the Committee to consider proposals that strike a better balance, such as the *Parents Over Platforms Act*, and look at options to inform parents of existing tools in the stores (which developers are already familiar with and know how to leverage) before adding additional onerous regulatory burdens that only shift certain social media platforms' responsibilities to small businesses.

Sincerely,

Morgan Reed
President
ACT | The App Association