ACT Association for Competitive Technology

May 20, 2026

The Honorable Chuck Grassley
Chairman
U.S. Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, District of Columbia 20510

The Honorable Dick Durbin
Ranking Member
U.S. Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, District of Columbia 20510

The Honorable Marsha Blackburn
Chair
U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology,
and the Law
224 Dirksen Senate Office Building
Washington, District of Columbia 20510

The Honorable Amy Klobuchar
Ranking Member
U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology,
and the Law
224 Dirksen Senate Office Building
Washington, District of Columbia 20510

RE: ***From the Courtroom to Congress: Why Landmark Social Media Verdicts Demand Federal Action to Protect Kids Online***

Dear Chairman Grassley, Ranking Member Durbin, Chair Blackburn, and Ranking Member Klobuchar:

Thank you for the opportunity to submit testimony for the record on your hearing titled, *From the Courtroom to Congress: Why Landmark Social Media Verdicts Demand Federal Action to Protect Kids Online*.[1]

The Association for Competitive Technology (ACT) represents small business innovators and startups in the software development and high-tech space in the United States and around the world. As the world embraces mobile technologies, our members create the innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping consumers lead healthier lives. Today, the

[1] "From the Courtroom to Congress: Why Landmark Social Media Verdicts Demand Federal Action to Protect Kids Online: United States Senate Committee on the Judiciary." *From the Courtroom to Congress: Why Land... | United States Senate Committee on the Judiciary*, 13 May 2026, www.judiciary.senate.gov/committee-activity/hearings/from-the-courtroom-to-congress-why-landmark-social-media-verdicts-demand-federal-action-to-protect-kids-online.

1401 K Street, NW, Suite 501
Washington, D.C. 20005

+1 (202) 331 - 2130 www.ACTonline.org /US-ACT @ACTonline

domestic app economy is worth more than $1.8 trillion and provides over 6.1 million American jobs.[2]

ACT welcomes the Committee's continued focus on protecting children online. As the Committee considers legislative responses to advance online safety, we urge that efforts remain focused on the platforms where the risks to children are highest. To the extent the Committee considers online safety within the app ecosystem, the Parents Over Platforms Act (POPA) offers a well-targeted approach that will empower parents with meaningful tools to protect their children online. In contrast, the App Store Accountability Act (ASAA), actively championed by Meta, would shift responsibility away from the companies whose platforms pose significant online safety risks.[3] Policymakers should reject Meta's approach and pursue legislation that places responsibility and accountability with those directly responsible for known harms.

The ASAA Misaligns Accountability and Creates New Risks for Developers and Consumers
The ASAA would require app stores to verify their users' ages and transmit that information to developers every time a user initiates an app download. By transmitting these age signals, the bill assigns developers "actual knowledge" of users' ages, which can trigger legal obligations under the Children's Online Privacy Protection Act (COPPA), regardless of whether an app is directed or marketed to children.

The ASAA would redistribute responsibility and accountability for online safety in a manner that benefits large social media companies while exposing others to increased risks and liability. For example, Meta has a long and well-documented history of failing to adequately address online safety harms on its platforms, including knowingly hosting users under the age of 13. A 2023 complaint filed by 33 state attorneys general stated that Meta received more than 1.1 million reports of Instagram users under the age of 13 since 2019 and closed only a small fraction of those accounts.[4] Under current law, Meta faces significant exposure under COPPA if it is found to have actual knowledge that children under 13 are using its services.

However, by requiring app stores to conduct age verification and pass along age signals, the ASAA would allow Meta to argue that it is merely relying on third-party information rather than independently determining users' ages. This effectively creates a legal buffer: Meta can remove flagged underage users while maintaining that it did not itself generate the knowledge that would trigger liability for years of past conduct.[5] In effect, the bill lets Meta externalize both the responsibility and legal consequences of its online safety malfeasance.

For other developers, however, the requirement to receive age signals under the ASAA would create significant legal and operational risks. Because developers would receive age information

---

[2] "State of the App Economy." *ACT | The App Association*, ACT | The App Association, actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf. Accessed 13 Jan. 2026.
[3] *Zuckerberg's Enlisting the GOP against Tech Rivals Apple and Google - Politico*, www.politico.com/news/2025/04/20/zuckerbergs-enlisting-the-gop-against-tech-rivals-apple-and-google-00295945. Accessed 14 May 2026.
[4] Singer, Natasha. "At Meta, Millions of Underage Users Were an 'Open Secret,' States Say." *The New York Times*, 25 Nov. 2023, https://www.nytimes.com/2023/11/25/technology/instagram-meta-children-privacy.html. Accessed 14 May 2026.
[5] Dufault, Graham. "Into the Metaverse: The Money and Motivations behind Meta's App Store Gambit." *ACT*, 4 June 2025, actonline.org/2025/05/23/into-the-metaverse-the-money-and-motivations-behind-metas-app-store-gambit/.

at the point of download, they are deemed to have actual knowledge of users' ages. In turn, this triggers COPPA obligations, such as verifiable parental consent, data retention obligations, and targeted advertising restrictions. These requirements would apply uniformly, regardless of whether an app poses any meaningful risk to children. As a result, flashlight apps, stargazing platforms, and back-office farm management tools would all face the same obligations as social media platforms.

The costs of this approach would be substantial. In a 2025 report, Trusted Future estimated that the total costs to small businesses could reach $280 billion under the ASAA.[6] If the ASAA is enacted, small businesses, which often do not have legal or compliance teams, would have to divert limited resources towards interpreting complex legal obligations and reconfiguring their products to comply.

Finally, age verification increases privacy and security risks for consumers. Sharing age information necessarily creates an entirely new data collection infrastructure that embeds privacy and security risks by design. Indeed, in March 2026, researchers at Cybernews, a cybersecurity outlet, found that IDMerit, a global identity verification provider, left more than 203 million sensitive records from U.S. consumers exposed.[7] This incident underscores how requiring the collection and storage of age-related data at scale creates high-value targets for bad actors and places consumers at risk.

POPA Provides a Better Approach to Online Safety

In contrast to the ASAA, the Parents Over Platforms Act takes a more targeted, risk-based approach by focusing obligations on the apps and platforms that pose the greatest risks to online safety. Instead of sweeping in the entire app ecosystem, POPA applies to services intended only for adults or those that provide materially different experiences based on age, such as social media platforms. For covered services, POPA requires parental consent before minors can access unsuitable content, mandates centralizing privacy and safety information, and limits the collection and use of age-related information. This approach focuses safeguards where there are foreseeable harms rather than in low-risk contexts.

By concentrating obligations where the risks actually exist, POPA avoids the unintended consequences of broad app store age verification mandates. Social media platforms and similar services that curate, recommend, and host risky content are best positioned to implement meaningful safeguards and should bear the corresponding responsibility. Extending the same obligations to general audience apps that pose no comparable risk to children would not meaningfully improve online safety but would impose significant compliance costs and increase liability exposure for developers.

Importantly, POPA also builds on existing parental controls and gives families more effective tools to manage their children's digital experiences. It preserves parental choice by allowing

---

[6] Staff, NP. "The Huge Costs for Small Businesses of App Store Age Verification Bills." *TRUSTED FUTURE*, 6 June 2025, trustedfuture.org/the-huge-costs-for-small-businesses-of-app-store-age-verification-bills/.

[7] Kurt Knutsson, CyberGuy Report, and Fox News. "1 Billion Identity Records Exposed in ID Verification Data Leak." *Fox News*, FOX News Network, www.foxnews.com/tech/1-billion-identity-records-exposed-id-verification-data-leak. Accessed 14 May 2026.

families to decide whether a child's age information is shared with a developer. It also requires covered platforms to provide easy access to privacy and safety settings. This approach recognizes that parents are in the best position to make decisions about their children's online experiences and ensures they have the information and control needed to do so effectively.

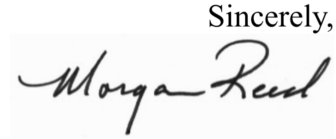
Congress Should Preserve Encryption and Privacy Protections

Further, effective online safety measures should not require that companies compromise encryption or other privacy-preserving tools. After the verdict in *State of New Mexico v. Meta Platforms, Inc.*, the New Mexico Department of Justice announced its intent to seek relief that would require Meta to weaken its encryption.[8] However, proposals that undermine encryption may create broader privacy and cybersecurity risks for consumers. Strong encryption and the ability to communicate anonymously remain important safeguards for consumers, as well as journalists, political dissidents, domestic violence survivors, and many more. Congress should carefully tailor online safety legislation to avoid undermining encryption and ensure that consumers can continue to realize its benefits.

Conclusion

We appreciate the Committee's attention to online safety and urge the consideration of legislation that focuses on known harms, empowers parents, and safeguards privacy. Broad mandates, such as the ASAA, will shift liability away from the platforms best positioned to address online safety harms while simultaneously introducing new risks to consumer privacy and security. In contrast, POPA's targeted approach will meaningfully improve online safety, preserve access to useful digital tools, and avoid unintended consequences for privacy and innovation. We welcome the opportunity to work with you to advance effective legislation, protect consumer privacy, and support small business innovators.

Sincerely,



Morgan Reed
President
Association for Competitive Technology

[8] "New Mexico Department of Justice Wins Landmark Verdict Against Meta." *New Mexico Department of Justice*, 24 Mar. 2026, https://nmdoj.gov/press-release/new-mexico-department-of-justice-wins-landmark-verdict-against-meta/. Accessed 14 Apr. 2026.